Chapter 9a - Whither Safety? - IAEA

Introduction

In this chapter we shall cover two apparently disparate but related topics: the role of the International Atomic Energy Agency (IAEA), particularly in setting international safety standards, and the direction future designs appear to be taking with respect to safety.

IAEA

Figure 9-1 - Atoms for Peace

At the end of World War II, the U.S. was the only country to possess the atomic bomb. It was joined in short succession by the United Kingdom, the USSR, France and later China. It became clear that once the secret of the bomb was out - the secret being that one could build one - there was little to stop almost any determined government from developing its own nuclear weapons programme. The IAEA was born to administer a "deal" proposed by President Eisenhower in his "Atoms for Peace" speech to the United Nations (Figure 9-1): if nations would eschew the path of nuclear weapons development, those countries which already had nuclear weapons would assist them in developing a civilian nuclear power programme. In other words, the IAEA had two initial objectives: *safeguards*, aimed at prevention of the proliferation of nuclear weapons, and *promotion*, aimed at assisting non-nuclear-weapons states.

Despite countries which either have developed and declared nuclear weapons since then (India, Pakistan, North Korea), or which started on a nuclear weapons path and then stopped (Argentina, South Africa), or which were forcibly stopped (Iraq, Syria), or which are ambiguous (Israel, Iran), the 'deal' has held remarkably well.

The promotion side of the IAEA has been increasingly focussed on safety, especially since the Chernobyl accident. In the early days, the IAEA developed a series of Safety Guides, which declared good safety practices in all areas of the nuclear fuel cycle, from design to waste management. These Guides were prepared in a collaborative and consensus manner by IAEA members, with of course the nations which had a nuclear power programme having a predominant role. Because of this, they tended to reflect a "lowest common denominator" approach, containing useful advice, but they were not specific enough to affect design and operation in a fundamental way. They were generally adopted by both purchaser and vendor nations. Since safety remains the responsibility of each country, the Guides have no legal force

internationally, but tend to be incorporated informally or adopted formally (e.g. China) as part of the country's safety regulations.

How then could Chernobyl have happened? As we have discussed earlier, the Chernobyl accident was a combination of an unforgiving design which was vulnerable to operation outside an approved envelope, and operators who took the machine well outside that envelope without apparently realizing the risk they were running. It has been claimed that Chernobyl met **all** the IAEA Safety Guides. In the author's opinion, this is disingenuous; however there is no question that Chernobyl caused a fundamental rethinking of the effectiveness of the guidance the IAEA was offering.

INSAG

The first action taken was by an international group of independent experts, who provided advice to the Director-General of the IAEA - the International Safety Advisory Group, or INSAG. They produced a number of key documents, three of which we shall summarize here. They gained widespread international acceptance and have strongly influenced the development of safety since then.

Fundamental Safety Principles

The first document[1] (recently revised[2])[a] tried to set down in one place what its title implied: what were the underlying and fundamental safety principles of nuclear power plants. Five levels of safety principles were defined, in a hierarchy going from the general and all-encompassing to the specific technical practices. The document was written in the present tense, as if all reactors followed the safety principles - a clear message that if they did not, they should be modifying at least their operating practices. The levels were:

1. Objectives
2. Fundamental Management Principles
3. Defence-in-Depth Principles
4. General Technical Principles
5. Specific Principles

Three general safety objectives were defined.

[a] We shall follow INSAG-3, the original report, unless otherwise stated

1. GENERAL NUCLEAR SAFETY OBJECTIVE

To protect individuals, society and the environment by establishing and maintaining in nuclear power plants an effective defence against radiological hazard.

In the commentary following this objective, INSAG noted that if it were achieved, the level of risk due to nuclear power plants does not exceed, and is generally lower than, that of competing energy technologies. No allowance could be taken for offsetting these risks by the benefit from nuclear plants.

We covered this approach in Chapters 1 and 2. Note however the inclusion of environmental protection - which is not however further explained or quantified in INSAG-3. However the CNSC legislative mandate has been expanded to include the effects of civilian nuclear activities on the environment - clearly a growth field in the regulatory arena!

2. RADIATION PROTECTION OBJECTIVE

To ensure in normal operation that radiation exposure within the plant and due to any release of radioactive material from the plant is kept as low as reasonably achievable and below prescribed limits, and to ensure mitigation of the extent of radiation exposure due to accidents.

This objective restated the existing requirements of the International Commission on Radiological Protection (ICRP). There are two broad elements to radiation protection: you must first meet dose limits, which are set to protect public and workers from undue health risks; and once you have achieved that, you are obliged to see if you can reduce the dose further in a cost-effective fashion. INSAG-3 omitted the qualifier used by ICRP: ALARA (As Low As Reasonably Achievable) is to be applied with "economic and social factors taken into account". Thus doses must be optimized, not minimized, recognizing that at some point the cost of further dose reduction exceeds the benefit of such reduction. In such optimization, it is common to assign a "benefit" of $100,000 per Sievert averted[3] - i.e., if the cost of averting a Sievert is below this amount, the dose reduction measures should be considered; and conversely. The qualifier was restored in the revision of INSAG-12.

3. TECHNICAL SAFETY OBJECTIVE

To prevent with high confidence accidents in nuclear plants; to ensure that, for all accidents taken into account in the design of the plant, even those of very low probability, radiological consequences, if any, would be minor; and to ensure that the likelihood of severe accidents with serious radiological consequences is extremely small.

This partly restates the defence-in-depth principle: prevent accidents, stop them if they occur

(protection) and mitigate their consequences. However a special emphasis is placed on severe accidents: ensuring they are low likelihood and providing accident management procedures to attempt to control their progress.

In the commentary INSAG recommends a quantitative safety goal: that the severe core damage frequency for existing plants should be below 10^{-4} events per year; and that for future plants it should be reduced to 10^{-5} events per reactor-year. This safety goal has been widely adopted as an minimum requirement by most national regulatory agencies, including the CNSC. INSAG-3 also comments that severe accident management and mitigation procedures should reduce the risk of a large prompt offsite release by at least a factor of 10; that is, the probability of a large off-site release should be less than 10^{-5} per year for existing plants and 10^{-6} per year for future ones (INSAG-12 gives no number but says that such sequences can be 'practically eliminated', which probably means the same thing). Another way of viewing this is that the conditional containment failure probability after a severe accident should be less than 0.1. Similar targets have been set by the US Electric Power Research Institute (EPRI), an industry-funded group, for new plants.

Safety Culture

INSAG 3 introduced one concept that altered thinking about safety across the world (safety culture) and gave a complex explanation of another (defence-in depth). We shall not summarize the rest of INSAG-3 here - it is available in most specialty libraries - but we will describe these two areas.

Safety culture was defined as one of the three fundamental management principles: the other two were defence-in-depth, and provision of regulatory control and verification. The safety culture principle was stated as follows:

"An established safety culture governs the actions and interactions of all individuals and organizations engaged in activities related to nuclear power".

It was defined as "the personal dedication and accountability of all individuals engaged in any activity which has a bearing on the safety of nuclear power plants".

In the author's view, it provides a hint of what went wrong at Chernobyl. No design is so safe that it cannot be disabled by incompetent operation - that is why plant safety is fundamentally the responsibility of the plant operator, not the designer and not the regulator, as we discussed in an earlier chapter. It is particularly important that an unforgiving design requires cautious operation which in case of uncertainty always opts for the prudent course of action. In retrospect, Chernobyl was an unforgiving design run by an organization deficient in safety culture. We saw an example of safety culture on our case study on the Point Lepreau spurious douse. The report stressed the capsule management philosophy which operators were trained to: in case of the unexpected - S.T.A.R. - Stop - Think - Act - Review.

The difficulty with safety culture was that it was hard to 'get hold of' - like personal character, one could sense when it was deficient but it was hard to measure. INSAG therefore hastened to try to define the term, in a subsequent report[4] entitled "Safety Culture". The term was redefined as:

"Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance".

The three concepts were that Safety Culture is attitudinal as well as structural; relates both to organizations and individuals; and matches all safety requirements with appropriate perceptions and action.

In simpler terms, the best design and the most carefully-written procedures will not help if the staff do not place safety first in their thoughts and actions.

The report goes on at length to describe the attributes of safety culture. Figure 9-2 summarizes the elements that are addressed.

Other organizations have used different definitions. The US Nuclear Regulatory Commission has stated that "A good safety culture in a nuclear installation is a reflection of the values, which are shared throughout all levels of the organization and which are based on the belief that safety is important and that it is everyone's responsibility."

More basic definitions are "*Safety culture is what you do when the boss isn't looking*", and "*Safety culture is the way we do things around here*".

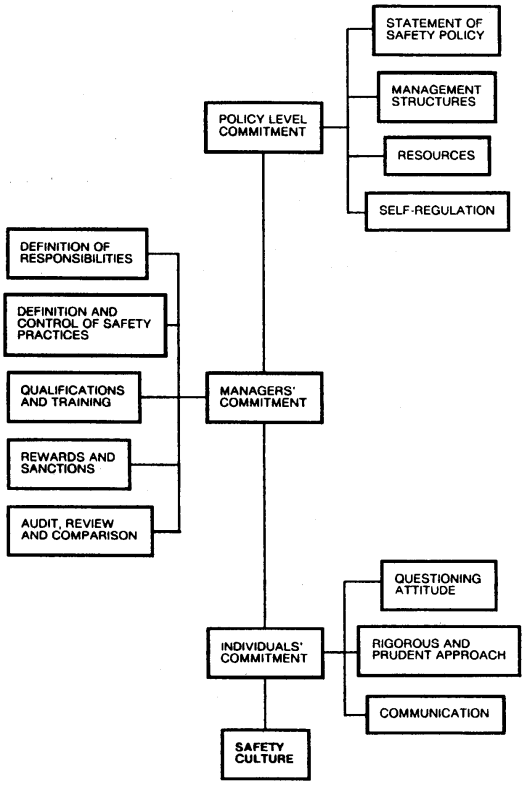

FIG. 1. Illustration of the presentation of safety culture.

Figure 9-2 - Elements of Safety Culture

In the end, according to D. Meneley[b], safety culture is like a sharp-edged tool: a useful device if wielded carefully, and dangerous in the hands of fools.

Although the term is new, the concept is not. E. I. Dupont starting manufacturing explosives in the early 1800s. He developed the concept of separation distances for the powder mills and designed buildings so that explosions would go upwards or away from occupied buildings. He built his house inside the plant and insisted managers also live inside the plant. He also developed plant rules and procedures. These ideas would fit well with modern ideas of safety culture.

On the negative sense, the IAEA[5] has defined the stages of organizational decline:

Stage	*Name of stage*	*Characteristic of stage*
1	Over-confidence	Good past performance leading to self-satisfaction
2	Complacency	Occurrence of minor events that are subjected to minimum self-assessment, and delay in improvement programmes
3	Denial	Number of minor events increases, with possibly a more significant event. These are treated as isolated events. Findings from audits are considered invalid. Root cause analysis not used.
4	Danger	Several potentially serious events occur but management and employees reject criticism from audits or regulator, by considering their views biased. The oversight function is afraid to confront management.
5	Collapse	Regulator intervenes to implement special evaluations. Management is overwhelmed and may need to be replaced. Major and very costly improvement needs to be implemented.

[b] Personal communication

Audits by organizations such as INPO[c] (an association of operating organizations) have distilled - through auditing utilities which were subsequently forced into extended plant outages due to management deficiencies - a list of symptoms of a poor safety culture (Figure 9-3). It is the rare organization which does not recognize at least part of itself in the list.

[c] Institute of Nuclear Power Plant operators

Figure 9-3 - Safety Culture Warning Flags from INPO

DRAFT - 11/5/98

INPO

THEMES ("WARNING FLAGS") FROM RECENT EXTENDED SHUTDOWNS

Overconfidence
- The "numbers" are good and the nuclear staff is living off past successes.

Isolationism
- There are few interactions with other utilities, INPO, and other industry groups.
- Benchmarking is seldom done or is limited to "tourism" without implementation.
- As a result, the plant is "behind the industry and doesn't know it."

Managing Relationships
- Mindset toward NRC/INPO is defensiveness or "do the minimum" - no bank account.
- Employees are not involved, not listened to, and raising problems is not valued.

Operations and Engineering
- Operations standards, formality, and discipline are lacking.
- Plant operational focus is overshadowed by other issues, initiatives, or special projects.
- Engineering is weak (loss of talent) or lacks alignment with operational priorities.
- Design basis is not a priority and design margins erode over time.

Production Priorities
- Important equipment problems linger, and repairs are postponed while the plant stays on line.
- Nuclear safety is "assumed" but not emphasized in staff interactions and site communications.

Managing Change
- Organizational changes, staff reductions, retirement programs, or relocations are initiated before fully considering impact - recruiting or training is not used to compensate.
- Processes and procedures don't support strong performance after management changes.

Plant Events
- Event significance is unrecognized or underplayed and reaction to events is not aggressive.
- Organizational causes of events are not explored.

Nuclear Leaders
- Managers are defensive, lack team skills, or are weak communicators.
- Managers lack integrated plant knowledge or operational experience.
- Senior managers are not involved in operations and do not exercise accountability or follow-up.

Self-Critical
- Oversight organizations lack an unbiased outside view or deliver only good news.
- Self-assessment processes do not find problems or do not address them.

Defence In Depth

INSAG-3 took great pains to develop the concept of 'defence in depth'. We covered this in simple terms in earlier chapters:

1. Prevent an accident from occurring (**prevention** - e.g., good quality piping and in-service inspection help prevent a pipe break)
2. Stop it if it occurs (**protection** - e.g., shut down the reactor and make up leaks through a make-up system)
3. Limit the damage to the fuel (**mitigation** - e.g., use ECC to refill the core)
4. Limit the release of fission products (**accommodation** - e.g., contain consequences within containment and stop them getting worse through severe accident management and emergency procedures)

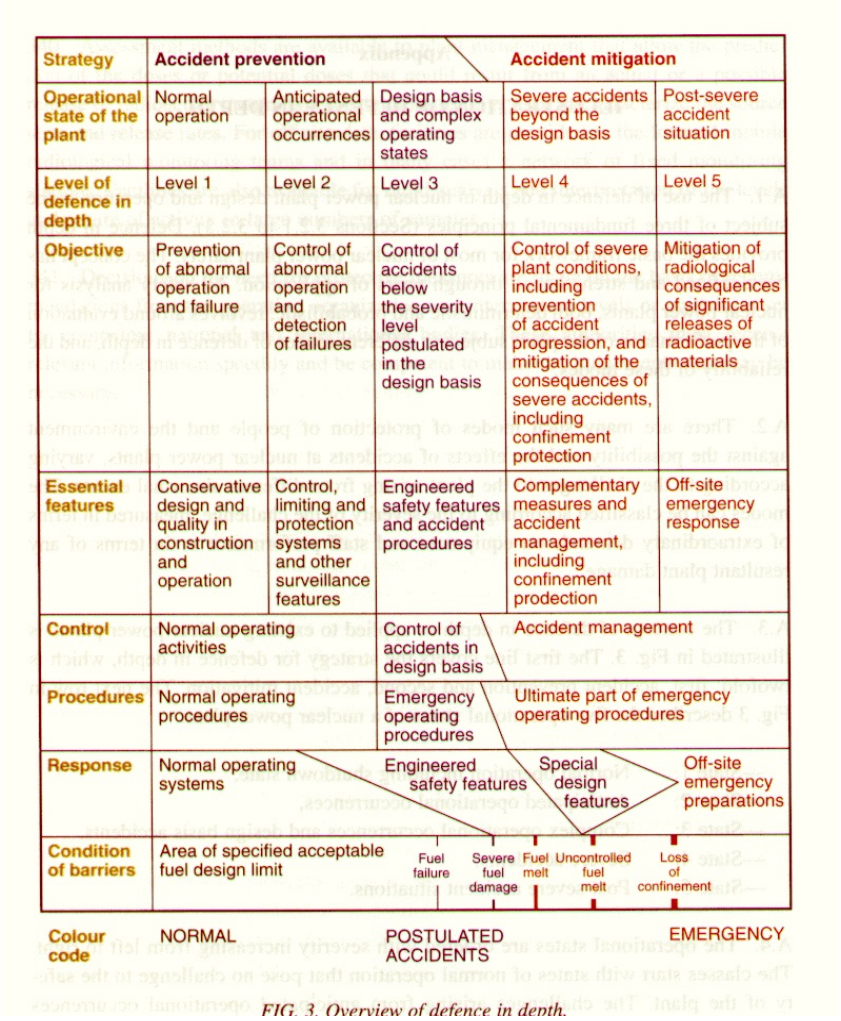

FIG. 3. Overview of defence in depth.

Figure 9-4 - Defence in Depth - Concepts

Figure 9-4 from INSAG-12 indicates the structure and level of detail in their model, going well beyond our simple one. Figure 9-5 shows defence-in-depth when viewed as a series of physical or procedural barriers. To the author, this formalism seems unnecessarily complex, but it is included here in case it resonates with the reader.

IAEA Safety Guides are now being rewritten to make them more detailed, so that they state the increased safety expectations of the 21st. Century. "Requirements" on both design[6] and operations[7] are becoming the de facto minimum standard for nuclear power plants. Indeed, the IAEA design "requirements" report, NSR-1 is the basis of the current Canadian top-level design requirements for new build, in CNSC report RD-337.

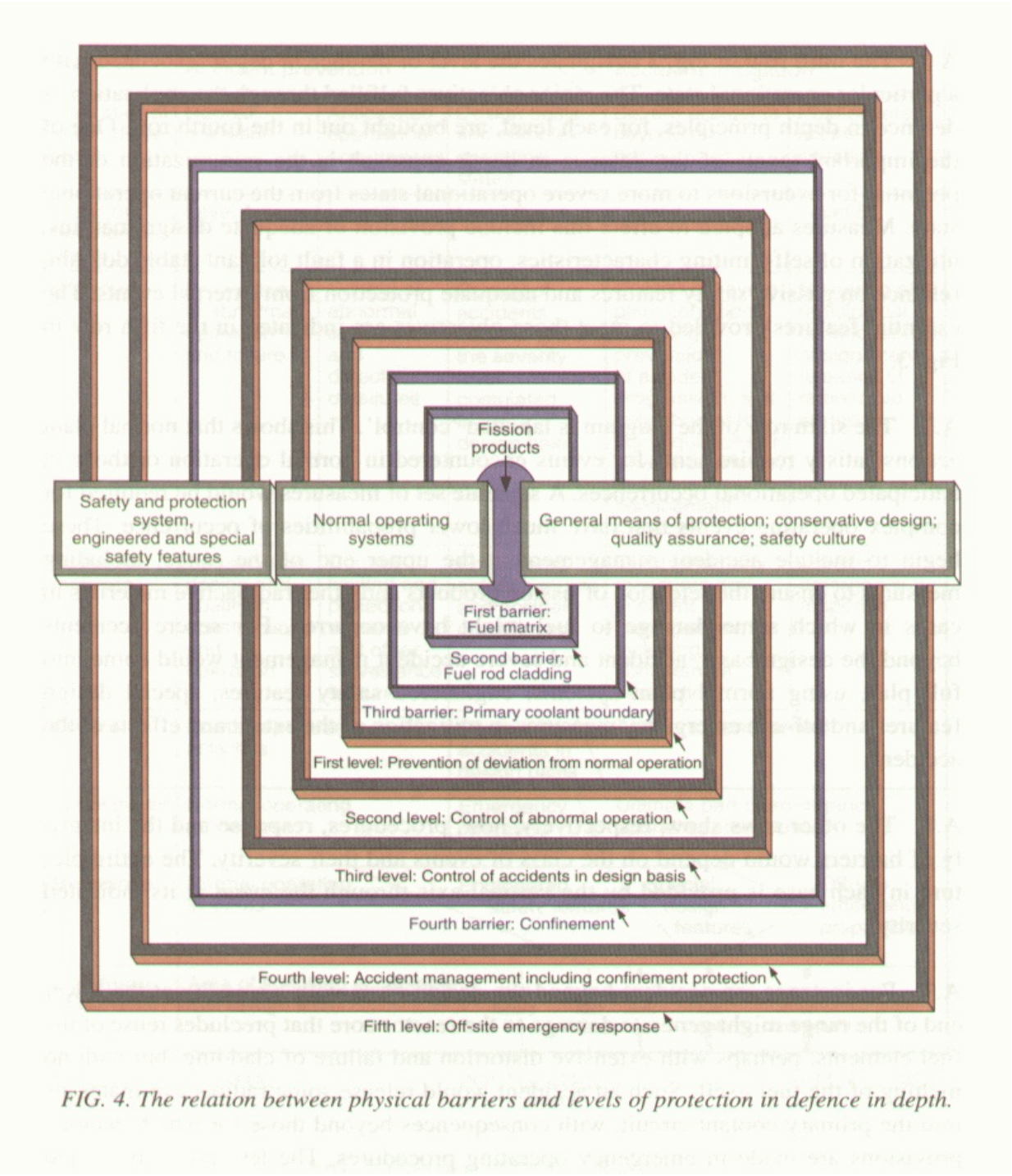

FIG. 4. The relation between physical barriers and levels of protection in defence in depth.

Figure 9-5 - Defence-in-Depth - Barriers

INPRO

For the last few years, IAEA has been reviewing the requirements for reactors 50 years from now - an activity called INPRO, short for "International Project on Innovative Nuclear Reactors and Fuel Cycles". A significant part of INPRO is trying to define where safety will be going. It seems likely that the following will be much more important in assuring the safety of plants in the future:

- **Passive safety**. Passive systems perform their job without the use of external electrical or mechanical power, etc.

- **Inherent safety characteristics**. A plant has an inherently safe characteristic[8] against a potential hazard if the hazard is rendered physically impossible. An inherent safety characteristic is achieved through choice of the fundamental physics, physical and chemical properties of nuclear fuel, coolant and other components. The term inherent safety is normally used with respect to a particular characteristic, not to the plant as a whole; for example an area is inherently safe against internal fire if it contains no combustible material; a reactor is partially inherently safe against reactivity insertion if the physically available amount of excess reactivity is small and overall reactivity feedback is negative so that no large power excursions can occur[d]; a reactor is inherently safe against loss of the heat sink if decay heat can be removed by conduction, thermal radiation and natural convection to the environment without fuel damage; a fuel cycle facility is inherently safe against criticality if it cannot contain a critical configuration of material etc.

We shall cover these in the second part of this chapter.

International Nuclear Event Scale

No discussion of safety would be complete without a summary of the International Nuclear Event Scale[8]. This is a ranking of accidents so that the safety significance of events in nuclear power plants could be reported in a consistent way all over the world. The seven levels in the scale are reproduced in Figure 9-6.

[d]Partially, since the heat still has to be removed

GENERAL DESCRIPTION OF INES LEVELS

INES Level	People and Environment	Radiological Barriers and Control	Defence-in-Depth
Major Accident Level 7	• Major release of radioactive material with widespread health and environmental effects requiring implementation of planned and extended countermeasures.		
Serious Accident Level 6	• Significant release of radioactive material likely to require implementation of planned countermeasures.		
Accident with Wider Consequences Level 5	• Limited release of radioactive material likely to require implementation of some planned countermeasures. • Several deaths from radiation.	• Severe damage to reactor core. • Release of large quantities of radioactive material within an installation with a high probability of significant public exposure. This could arise from a major criticality accident or fire.	
Accident with Local Consequences Level 4	• Minor release of radioactive material unlikely to result in implementation of planned countermeasures other than local food controls. • At least one death from radiation.	• Fuel melt or damage to fuel resulting in more than 0.1% release of core inventory. • Release of significant quantities of radioactive material within an installation with a high probability of significant public exposure.	
Serious Incident Level 3	• Exposure in excess of ten times the statutory annual limit for workers. • Non-lethal deterministic health effect (e.g., burns) from radiation.	• Exposure rates of more than 1 Sv/h in an operating area. • Severe contamination in an area not expected by design, with a low probability of significant public exposure.	• Near accident at a nuclear power plant with no safety provisions remaining. • Lost or stolen highly radioactive sealed source. • Misdelivered highly radioactive sealed source without adequate procedures in place to handle it.
Incident Level 2	• Exposure of a member of the public in excess of 10 mSv. • Exposure of a worker in excess of the statutory annual limits.	• Radiation levels in an operating area of more than 50 mSv/h. • Significant contamination within the facility into an area not expected by design.	• Significant failures in safety provisions but with no actual consequences. • Found highly radioactive sealed orphan source, device or transport package with safety provisions intact. • Inadequate packaging of a highly radioactive sealed source.
Anomaly Level 1			• Overexposure of a member of the public in excess of statutory annual limits. • Minor problems with safety components with significant defence-in-depth remaining. • Low activity lost or stolen radioactive source, device or transport package.
NO SAFETY SIGNIFICANCE *(Below Scale/Level 0)*			

Figure 9-6 - INES scale

Exercises

1. Place the following accidents on the International Nuclear Event Scale, with brief reasons for your choice:
    1. NRX accident, 1952
    2. SL-1 accident
    3. Pressure-tube failure in Pickering A (G-16)
    4. Feeder crack in Point Lepreau (S-08)
    5. Spurious douse in Point Lepreau (as discussed under our 'Case studies')
    6. Fire in Narora plant in India
    7. Chernobyl accident (power run away)
    8. Three Mile Island accident (core melt)
    9. Erosion/corrosion of Davis-Besse vessel head

2. Possible project: If you work for a Nuclear Power Plant, evaluate either its design or its operation against NSR-1 or NSR-2 respectively.

3. If you work for a design organization or a regulator or a Nuclear Power Plant, evaluate its safety culture in terms of either the INPO criteria in Figure 9-3 or the IAEA stages listed above it. Give reasons and evidence, not just opinion.

References

1. “Basic Safety Principles for Nuclear Power Plants”, International Safety Advisory Group report 75-INSAG-3, IAEA, 1988.
2. “Basic Safety Principles for Nuclear Power Plants”, International Safety Advisory Group report 75-INSAG-3 Rev. 1, INSAG-12 IAEA, 1999.
3. US 10CFR50, “Appendix I to Part 50--Numerical Guides for Design Objectives and Limiting Conditions for Operation to Meet the Criterion "As Low as is Reasonably Achievable" for Radioactive Material in Light-Water-Cooled Nuclear Power Reactor Effluents; Sec. IID.
4. “Safety Culture”, International Safety Advisory Group report 75-INSAG-4, IAEA, 1991.
5. “Safety Culture in Nuclear Installations”, IAEA-TECDOC-1329, December 2002.
6. “Safety of Nuclear Power Plants: Design”, IAEA report NS-R-1, September 2000.
7. “Safety of Nuclear Power Plants: Operation”, IAEA Report NS-R-2, September 2000.
8. For a good definition of terms such as inherent safety characteristic or passive system, see “Safety Related Terms for Advanced Nuclear Power Plants”, IAEA TECDOC-626, September 1991.
8. “INES - The International Nuclear Event Scale” International Atomic Energy Agency brochure, 08-26941 / E.