Chapter 8 Good Design Principles & Practices

8.1 Introduction

This chapter provides a summary of good design principles and practices that should prove useful as a checklist and question generator when conducting design and analysis.

8.2 General

8.2.1 Keep It Simple Stupid (KISS)

8.2.2 Design so that safety systems are not needed

8.2.3 Reliability to avoid failure. Typically system reliability target is set to an unavailability of 10^{-3}.

8.2.4 Maintainability so that it is more likely that system will be operational

8.2.5 Passive systems are better than active systems

8.2.6 Group Separation

- 8.2.6.1 Physical: Process systems are independent of safety systems and safety systems are independent of each other.
- 8.2.6.2 Functional: Safety systems should be diverse in design, ie, they should use generically different principles and mechanisms and different manufacturers should be used.

8.2.7 Redundancy
- 8.2.7.1 Equipment
- 8.2.7.2 Instrumentation

8.2.8 Fail Safe
- 8.2.8.1 Equipment should fail in a safe manner

8.2.9 Environmentally Qualified
- 8.2.9.1 The safety systems must be able to withstand the fire, seismic, mechanical and other environmental loads placed on it.

8.2.10 Defence in Depth
- 8.2.10.1 Multiple barriers / safety mechanisms

8.2.11 Consider User Mental Models

8.2.12 [NAT85a] notes the following general safety principles and subsidiary criteria:
- 8.2.12.1 Prevention of fuel failure for loss of coolant events.
- 8.2.12.2 Prevention of channel failures for loss of coolant events.

8.3 CANDU Safety Principles from [HUR72]

8.3.1 Sequence

8.3.1.1 "In general, the design descriptions and supporting analysis of major reactor systems must be submitted well before these systems are installed."

8.3.2 Objectives

8.3.2.1 "...all criteria are directed (i) toward minimizing the chance of mechanical failure of the fuel and (ii) to preventing or minimizing the escape of fission products from the plant if fuel failure occurs. The chance of fuel failure depends on the ability to ensure that the power produced in the fuel and heat removal from the fuel are properly controlled. The escape of fission products can be prevented by ensuring that there are a number of high integrity barriers, the most important of which is the final containment."

8.3.3 Separate process and safety systems

8.3.3.1 "In specifying the requirements to be met by the designer and operator a very useful concept was developed in which the nuclear plant was considered to consist of three systems: the process system, the protective system, and the containment system. If these systems are independent of one another, and if each is of a reasonable reliability, the chance of a significant release of radioactive material to the public domain can be kept extremely small."

8.3.4 Failure measures and targets

8.3.4.1 "For the *process system* the aspect of most concern from a safety viewpoint is the frequency of occurrence of faults which could lead to fuel failure, whereas for each of the *protective* and *containment* systems the important parameter is the unreliability defined as the fraction of time during which the system would not perform its intended function."

8.3.4.2 "Progress was only possible in the application of this philosophy when it was made quantitative. The applicants were required to demonstrate that the frequency of occurrence of significant faults in the process system should be less than 1 per three years and that the unreliability of the protective devices and the containment divisions should be less than $10^{-2.5}$."

8.3.4.3 "Each safety system is expected to have an unreliability not exceeding 10^{-3}."

8.3.5 Radiation limits

8.3.5.1

"... individual members of the public should not be exposed to more than 0.5 rem / yr. To the whole body, not including exposure from natural background, medical procedures, ..."

8.3.5.2 "... a limiting population dose of 10^4 man-rem / yr per site ..."

8.3.6 Summary of Power Reactor Safety Criteria and Principles

8.3.6.1 Use standards, codes and practices for design and construction

8.3.6.2 Adhere to limits as per table

8.3.6.3 Safety systems shall be physically and functionally separate from the process systems and from each other.

8.3.6.4 Each safety system shall be testable and have a demonstrated unreliability of less than 10^{-3}.

8.3.6.5 Normal operation dose shall not exceed 1/10 of the allowable dose to Atomic Energy Workers.

Table 8.1 Reference Dose Limits

REFERENCE DOSE LIMITS FOR ACCIDENT CONDITIONS			
Situation	Assumed Maximum Frequency	Maximum Individual Dose Limits	Maximum Total Population Dose Limits
Serious Process Equipment Fault	1 per 3 years	0.5 rem/yr whole body 3 rem/yr to thyroid	10^4 rem/yr whole body 10^4 rem/yr to thyroid
Process Equipment Failure plus Failure of any Safety System	1 per 3x 10^3 years	25 rem/yr whole body 250 rem/yr to thyroid	10^6 rem/yr whole body 10^6 rem/yr to thyroid

8.4 General Reactor Safety Principles from [INS88]

8.4.1 Overview figure of approach to safety (page 24)

8.4.2 Management

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

8.4.2.2 The ultimate responsibility for the safety of a nuclear power plant rests with the operating organization.

8.4.2.3 The government establishes the legal framework for a nuclear industry and an independent regulatory organization.

8.4.3 Defence in depth

8.4.3.1 To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of barriers by averting damage to the plant and the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.

8.4.3.2 Principle emphasis is placed on accident prevention, particularly any which could cause core damage.

8.4.3.3 Mitigation measures are prepared and made available to reduce the effects of an accidental release of radioactive material.

8.4.4 General technical

8.4.4.1 Use engineering practices that are proven by testing and experience, and which are reflected in codes and standards.

8.4.4.2 Quality Assurance is applied throughout.

8.4.4.3 Personnel are trained and qualified. The possibility of human error is taken into account.

8.4.4.4 Safety assessment is made before construction and operation begin. The assessment is documented and independently reviewed. It is subsequently updated in light of new information.

8.4.4.5 A system of radiation protection practices, consistent with ICRP and IAEA is followed in the design, commissioning and operational phases.

8.4.4.6 Operating experience and research experience is shared and acted upon.

8.4.5 Siting

8.4.5.1 Siting takes local factors into account.

8.4.5.2 Sites are investigated from a radiological impact viewpoint.

8.4.5.3 A reliable ultimate heat sink is required.

8.4.6 Design process

8.4.6.1 The assignment and subdivision of responsibility for safety are kept well defined through the design phase.

8.4.6.2 Use proven technologies. New features are introduced only after thorough research and prototype testing at the component, system or plant level, as appropriate.

8.4.6.3 Design to cope with a set of events including normal, anticipated operational events, extreme external events and accident conditions. Conservative design requirements are established. Comprehensive analysis is carried out.

8.4.6.4 Operational occurrences are controlled to within operational limits. This reduces demand on safety systems.

8.4.6.5 Automatic safety systems are provided to shut down the reactor and maintain it in a cooled state if operating limits are exceeded.

8.4.6.6 Reliability targets are assigned to safety systems or functions. The targets are established on the basis of safety objectives. Provision for testing and inspection are made to ensure targets are met.

8.4.6.7 Design to prevent common mode failures.

8.4.6.8 Safety components and systems are to be environmentally qualified. The effects of ageing and abnormal functioning are considered.

8.4.6.9 Design to protect plant personnel from radiation exposure and to keep emissions within prescribed limits.

8.4.6.10 Reactivity induced accidents are protected against with a conservative margin of safety.

8.4.6.11 The reactor is designed to have mechanical stability to distortion and vibration.

8.4.6.12 Safety related shutdown systems are to be independent of process systems. The safety systems are to be available whenever a chain reaction is possible.

8.4.6.13 Normal process heat removal systems are highly reliable.

8.4.6.14 Alternate heat sinks are provided under accident conditions, even if the primary cooling system boundary integrity is lost.

8.4.6.15 Piping codes and standards are supplemented by additional measures to prevent pipe rupture.

8.4.6.16 The bulk of the radioactive material that might be released form the fuel is to be retained by containment.

8.4.6.17 If the containment structure could fail in a severe accident, special protection is provided to meet safety objectives.

8.4.6.18 Control room displays must be such that the operators have clear and unambiguous indications of safety related parameters, especially those for the purpose of identifying and diagnosing the automatic actuation and operation of a safety system or the degradation of defence in depth.

8.4.6.19 A secondary control room is provided in case the main control room is uninhabitable or damaged.

8.4.6.20 A loss of local power will not cause fuel damage.

8.4.6.21 Provisions are made at the design stage for the control of accidents within the design basis, including the specification of information and instrumentation needed by the plant staff for following and intervening in the course of accidents.

8.4.7 Manufacturing and construction

8.4.7.1 Construction is begun only after the operating and regulatory organizations have satisfied themselves that the main safety issues have been resolved and the remainder are amenable to solution before operations are scheduled to begin.

8.4.7.2 Manufacturers and constructors use proven and established techniques and procedures supported by quality assurance practices.

8.4.8 Commissioning

8.4.8.1 The commissioning procedure is established and followed to demonstrate that the entire plant, especially items important to safety and radiation protection, has been constructed and functions according to the design intent, and to ensure that weaknesses are detected and corrected.

8.4.8.2 Procedures for normal operation and for functional tests to be performed during the operating phase are validated as part of the commissioning programme.

8.4.8.3 During commissioning tests, detailed diagnostic data are collected on components having special safety significance and the initial operating parameters of the systems are recorded.

8.4.8.4 During the commissioning programme, the as-built characteristics of safety and process systems are determined and documented. Operating points are adjusted. Training procedures and limiting conditions are modified to reflect the as-built conditions.

8.4.9 Operation

8.4.9.1 The operating organization exerts full responsibility for safe operation through a strong organizational structure under the line authority of the plant manager. The plant manager ensures that all elements for safe operation are in place, including an adequate number of qualified and experienced personnel.

8.4.9.2 Safety review procedures are maintained to provide a continuing surveillance and audit of plant operational safety and to support the plant manager in his or her overall safety responsibilities.

8.4.9.3 Operation is conducted by authorized personnel according to administrative controls and procedures.

8.4.9.4 Programmes are established for training.

8.4.9.5 A set of operational limits and conditions is defined.

8.4.9.6 Normal operation is controlled by detailed, validated and formally

approved procedures.

8.4.9.7 Emergency operating procedures are established, documented and approved.

8.4.9.8 The radiation protection staff establish written procedures for the control, guidance and protection of staff.

8.4.9.9 Engineering and technical support are available.

8.4.9.10 Significant events are detected and evaluated in depth.

8.4.9.11 Safety related structures, components and systems are subject to regular preventive maintenance, testing and servicing.

8.4.9.12 A QA programme is established.

8.4.10 Accident management

8.4.10.1 The results of an analysis of the response of the plant to potential accidents beyond the design basis are used in preparing guidance on an accident management strategy.

8.4.10.2 Staff are trained in procedures for accidents that exceed the design basis of the plant.

8.4.10.3 Equipment, instrumentation and diagnostic aids are available for accidents beyond the design basis.

8.4.11 Emergency preparedness

8.4.11.1 Emergency plans are prepared before plant startup and are exercised periodically.

8.4.11.2 An emergency centre is available off-site and on-site with communication between the two.

8.4.11.3 Means are available for the assessment of releases and the need for protective measures.

8.4.12 Illustration of defence in depth (colour figures page 66 & 67)

8.4.12.1 physical barriers

fuel matrix
fuel cladding
coolant boundary
confinement

8.4.12.2 First level

conservative design
quality assurance
safety culture
normal operating systems
safety systems

8.4.12.3 Second level

detection of failures

control of abnormal operation

8.4.12.4 Third level

safety systems

8.4.12.5 Fourth level

accident management

confinement protection

8.4.12.6 Fifth level

off-site emergency response

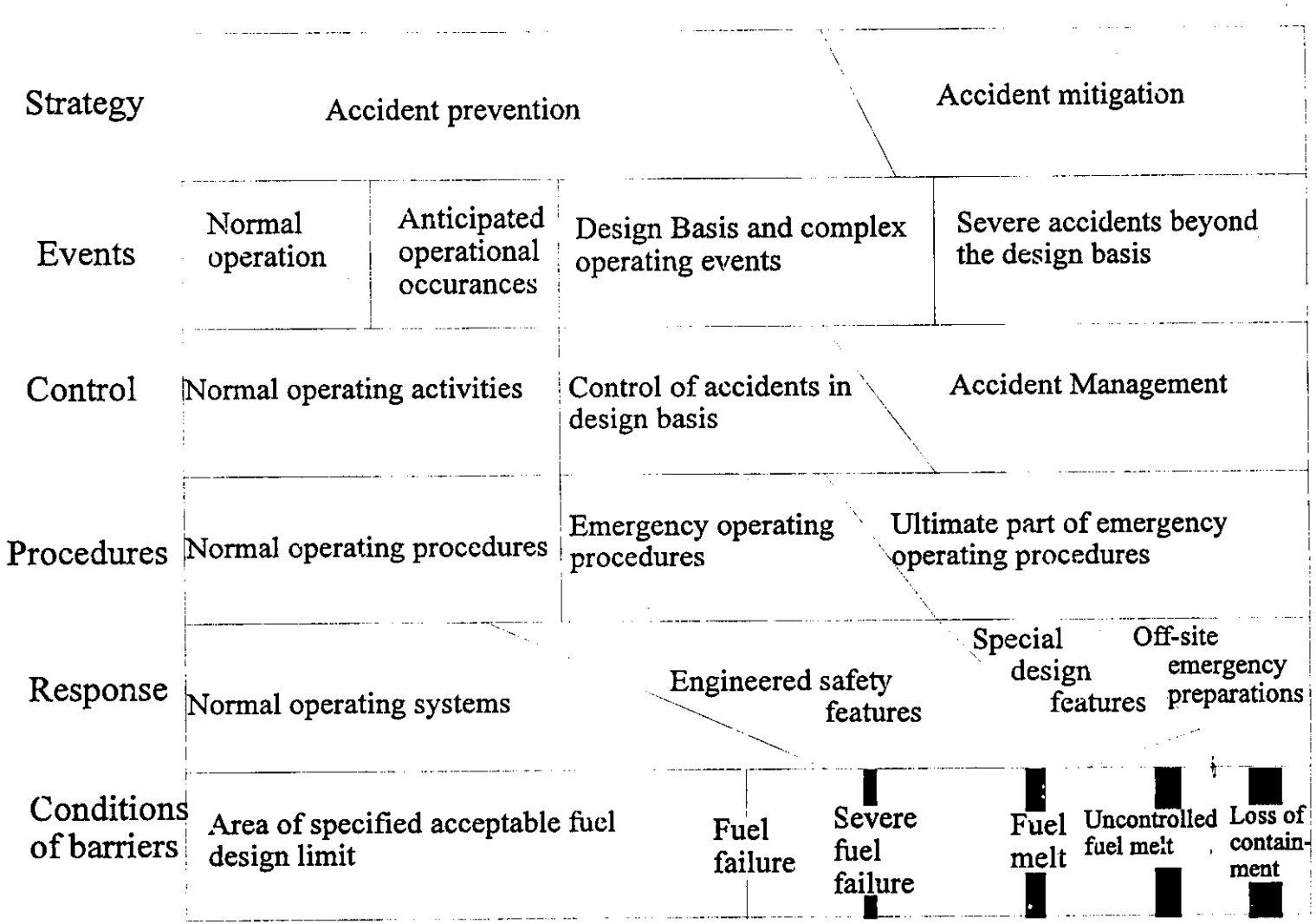

Figure 8.1 Overview of defence in depth.

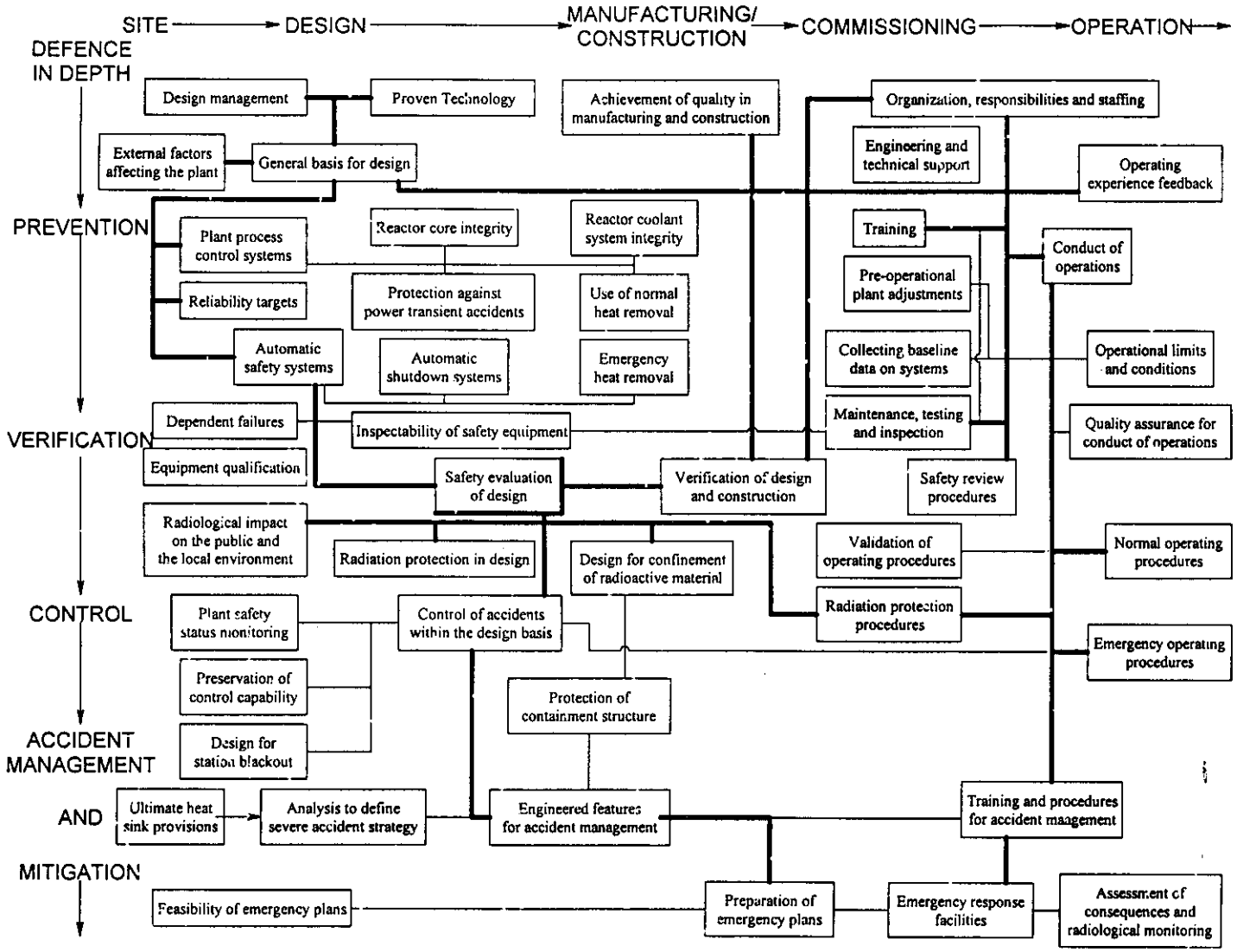

Figure 8.2 Schematic representation of the INSAG specific safety principles