Chapter 3 Safety Criteria

3.1 Introduction

3.1.1 Chapter Content based on [SNE86]

This chapter explores the roots and practice of setting the safety criteria by which reactor designs are judged.

The criteria are, in the final analysis, somewhat subjective in that there are no truly absolute definition of what is safe or even what is safe enough.

Rather, as pointed out in the introduction, we rely on the context sensitive philosophy of setting safety criteria with respect to alternative means of achieving the same technical goal (alternative technologies).

But, as we shall see, even this route is modified by the interplay of the designers, operators, the public and the regulators.

3.1.2 Learning Outcomes

The overall objectives for this chapter are as follows:

Objective 3.1	The student should be able to explain the various approaches to setting safety goals and discuss their relative merits.					
Condition	Open book written examination.					
Standard	100% on key terms and symbols, use of equations and diagrams as appropriate.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a	a		a		

Objective 3.2	The student should be able to apply C6 and the R documents to a specific case such as a research reactor.					
Condition	Workshop based project.					
Standard	An explanation of deviations from the regulatory documents is expected.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a	a	a	a	a	a

3.1.3 The Chapter Layout

The historical basis and the evolution of the criteria are explored, leading up to the current practice.

3.2 Safety Goals

In 1959 Ernest Siddall derived a safety goal of 0.2 deaths per year per plant.

These deaths (or loss of person-years in a population) is a function of the dose uptake by the workers and general population.

This uptake is in turn a function of the radiation released by the accident event.

The event sequence is termed LEVEL 1 and is the focus of this course.

The dose calculation is LEVEL 2 and the conversion to deaths is LEVEL 3.

Functionally, then:

$$\text{Safety Goal} \leq 0.2 \text{ deaths / year} = \sum_{\text{i=all events}} \text{Death (Dose (Risk}_i \text{)))} \quad (1)$$

where Risk is defined as

$$Risk = \sum_i expected\ frequency\ of\ event_i\ X\ expected\ consequence_i \quad (2)$$

This approach was used in the seminal WASH 1400 report [WAS75].

In this way, total risk is related to individual event risk.

In these terms, event risk is related to core damage since the core is the only source of radiation sufficient to cause severe injury or death.

The core can be damaged in a number of ways, each with its own circumstance and frequency.

Hence the above approach tracks each event to its conclusion and the total effect (loss of life) can be properly summed.

But this is not the only approach taken.

The nuclear industry uses two general types of acceptance criteria:

Binning and Averaging,

presumably as more expedient methodologies than the comprehensive summation of equation 2.

3.2.1 Binning

Binning techniques are based on limiting the consequences for any event based on frequency. Examples are the ASME code and C-6. Binning simply lumps all events, j, of a particular class, ostensibly those that fit with a given frequency range, into one bin or CLASS:

$$\text{Frequency}_{\text{lower bound}} < \lambda_j < \text{Frequency}_{\text{upper bound}} \tag{3}$$

Dose limits are set for each CLASS. The events are often <u>not</u> summed within each CLASS. This is the approach used in C-6, the limitations of which are discussed later in this chapter.

Summing can be performed within the bins, however, to give the criterion for each CLASS:

$$\left[\sum_{\substack{j=\text{all events} \\ \in \text{ bin } i}} \lambda_j \text{ x dose}_j \right] < (\text{dose limit})_{\text{bin } i} \tag{4}$$

IOWG and ACNS-4, discussed later in this chapter, are of the "summed binned" type.

3.2.2 Averaging

Averaging techniques are based on setting a limit on the frequency of a given outcome, which we will call a "safety goal".

The safety goal methodology requires the summation of the frequency of all events that exceed the stated criteria (set a few orders of magnitude below the desired limit).

As an example of a frequency based goal, for severe accidents, the goal may be set such that the expected frequency of the release of a dose between x and y is less than some value, ie

$$\lambda_i < \text{frequency target}, \tag{5}$$

where i represents events giving a dose between some defined limits.

"Core damage frequency" is sometimes estimated as the sum of the damage for all events weighted by some measure of the dose or amount of release, eg:

$$\text{Core Damage Frequency} = \sum_{i=\text{all events}} \text{frequency}_i \times \text{probability of release}_i \qquad (6)$$

This damage estimate is then used in a Level 2 calculation of the core damage dose.

This approach, although expedient, loses some fidelity.

An even simpler goal is to require that the core damage frequency be less than, say, 10^{-5} events/year.

3.3 Deterministic approach and definitions

3.3.1 Single and Dual Mode Failures

The probabilistic approach discussed above involves setting the safety criteria based on event frequency.

In contrast, the deterministic approach uses a predetermined acceptance criteria for each event, irrespective of the event frequency. For instance, for Canadian reactors, the failure of reactor control systems must not result in any addition fuel failure [R8]. This failure is an example of a "single mode failure".

Single and dual mode failures are deterministic criteria. In Canada, they are defined as:

1. Single mode failures: the failure of any one process system
2. Dual mode failures: the failure of any one process system plus either of the SD, ECC or containment systems.

Dose limits are given later in this chapter and the events which comprise single and dual failures are discussed in the next chapter.

The US NUREG Part 50 definition of a single failure is different than the Canadian definition:

> "A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions."

The IEEE Class 1E definition is:

> "The system shall be capable of performing the protective actions required to accomplish a protective function in the presence of any detectable failure within the system concurrent with all identifiable, but non-detectable failures, all failures occurring as a result of the single failure, and all failures which would be caused by the design basis event requiring the protective function."

3.3.2 Other criteria

The ANSI B31.1 binning criteria is given in table 3.1.

Table 3.1 ANSI B31.1 Criteria

Frequency		Criteria
high	$> 10^{-2}$	Events must be handled by normal process systems (ie, stay within safety limits).
medium	10^{-6} - 10^{-2}	Varies. Allows plastic deformation for the more infrequent events.
low	$< 10^{-6}$	No analysis required.

The ASME category definitions are given in table 3.2.

Table 3.2 ASME Category definitions

Category	Definition
A	Normal operation
B	Normal operation
C	Emergency operation - Large deformations permitted
D	Faulted conditions - Gross distortions permitted

3.4 NRX Accident

[Description given in appendix 1]

30 MW reactor, 12 shutoff rods driven by air pressure, 7 sufficient for shutdown.

Bank 1 = maximum # in any other bank + 1 = safeguard bank. This bank is interlocked so it must be withdrawn first ("poised" philosophy) but the interlock was not functioning and was known to be not functioning.

Button 1: raise Bank 1
Button 2: raise remainder of rods
Button 3: seat air supply valve
Button 4: air supply charger

Operation in progress: compare reactivity if irradiated fuel vs fresh fuel.

Error: Operator opened 3 out of 4 air supply bypass valves.

Supervisor in control room saw red lights, phoned the operator and went to look.

Error caused 3 or more rods to rise when the reactor was shutdown.

Fixed error and assumed rods would drop back in (rods were off their seat and hence there was no indication that they weren't in. In fact the rods were not in.)

Supervisor called control room to press Button 4 then Button 1. (Error: should have been 4 and 3)

This would normally have been safe if all the rods were in as assumed.

Assistant couldn't be recalled since he put the phone down. The buttons were spaced far apart by design. The operation was not meant to be done over the phone.

Button 1 raised the rods -> $\rho > 0$ which was a surprise.

Button 4 ineffective since Button 3 not pushed.

Pushed moderator dump to terminate the reaction. Peak power ~ 20 MW.

In the basement, the operator saw water gushing.

Operator in the control room heard a rumble and saw a spurt of water up through the top of the reactor.

Air activity noted.

Apparently some channels had a reduced cooling rate and boiled during the power pulse.

+ve void-reactivity coefficient -> second excursion (peak power = 60 to 90 MW)

Partial core disassembly.

Considerable gas evolution (H_2??).

Lessons: Separate control from shutdown
KISS

3.5 Canadian Safety Goals

Prompted by the NRX accident, the Canadian nuclear industry took a in-depth look at nuclear safety.

In 1959, Siddall suggested that a target of 0.2 deaths / year / plant be set, about 5 times lower than the coal fired power plant experience. This included the full fuel mining and production aspects of nuclear and coal based stations and was based on a comparison of prompt deaths.

He produced a set of event frequencies and unavailability targets as given in table 3.3.

Table 3.3 Event targets [SNE86]

EVENT	TARGET
Loss of Coolant	1 / 50 years
Loss of Power Control	1 / 16 to 1 / 160 years
Shutdown System Unavailability	1 in 500 tries

Note the implied sequence:

An event ---> radiation release ---> human dose.

This course focusses on the event. Event targets and event analysis form the bulk of the effort in PSAs.

From this, the amount and kind of radiation released can be calculated and from there a dose uptake can be derived.

The industry has, in effect, worked backwards from a dose limit to infer event target limits.

These event limits, then, become the targets that engineers work to on a daily basis.

From time to time, as new data appears on radiation dispersion and effects on radiation on humans, the event frequency targets are reassessed. As well, event targets are altered as more is learned about where the real risks lie and as safety philosophy evolves.

The industry used (as still uses) good design practice to achieve its targets.

The NRX accident showed the importance of
system independence (functional and physical group separation),
multiple barriers (defence in depth),
and the use of standards and procedures.

This led to good performance but quantifying the situation proved elusive.

This led to an increased focus on quantifying the probability and consequence of accident events.

This move to an increased emphasis on formal PSAs have proven successful on at least 2 accounts:

1. The relative merits of alternative designs could be demonstrated. Absolute quantification has not been always successful, however.
2. The systematic review and assessment of designs and procedures have successfully ferreted out weaknesses.

In 1961, the targets were revised downward by Laurence to 10^{-2} deaths per year.

If a disaster is assumed to lead to 1000 deaths, then the frequency targets must be 10^{-5} events per year.

Given that it is very difficult to engineer any complex system to a high reliability, the 'defence in depth' approach naturally arose.

The process system is placed in tandem with a protective system and a containment system.

Thus, a disaster could only occur if the process system failed AND the protective system failed AND the containment system failed.

Realistic targets were set at 1 event / 10 years for the process system and 1 in 100 demands each for the protective and containment systems, giving a combined probability of $10^{-1} \times 10^{-2} \times 10^{-2} = 10^{-5}$ events per year.

Note that process systems are continuously operating systems and the process failures are related to events / year.

In contrast, safety systems are 'on-demand' systems and their failure is related to events / demand. Care must be taken, however, for safety systems like ECCS are initially operate on demand but are required to operate continuously once they are demanded (more on this in Chapter 7).

One of the benefits of the defence in depth approach is that the failure rates of each of the systems is high enough for reliable data to be gathered on failure modes and frequencies.

Thus risk coverage can be demonstrated.

Further, to meet the system event targets, redundancy in equipment is required. Triplication is commonplace.

This permits on-power testing of all equipment, proving to be a boon to assuring compliance.

This approach was used for NPD to a large extent.

For Douglas Point, the event target was lowered to 10^{-6} per year.

A safety report was written that was comprised of a systematic listing of all identifiable events, an evaluation of the event frequencies and of the consequences (expressed as a dose).

This new low target, although admirable, was now so low that costs of implementation rose out of proportion to the benefits compared to coal fired plants.

This is not to say that nuclear is more expensive than the alternatives, rather, it means that money spent on increasing nuclear safety would be more effectively spent elsewhere.

3.6 Single / Dual Mode Failures

In 1967, Boyd collapsed the spectrum of events into 2 categories:

1. Single mode failures: the failure of any one process system
2. Dual mode failures: the failure of any one process system plus either of the SD, ECC or containment systems.

Targets were set as shown in table 3.4. These guidelines were finalized in 1972 [HUR72].

We note here a substantial risk aversion to events that are less frequent but have a larger consequence.

The acceptable risk (frequency x dose) for a less frequent but more disastrous dual mode failure is some 10 times lower than for the more frequent but less harmful single mode failure.

This is human nature.

Table 3.4 Reference Dose Limits

REFERENCE DOSE LIMITS FOR ACCIDENT CONDITIONS			
Situation	Assumed Maximum Combined Frequency	Maximum Individual Dose Limits (1 Sv = 100 rem)	Maximum Total Population Dose Limits
Serious Process Equipment Fault (Single Failure)	1 per 3 years	0.5 rem/yr = 5 mSv/yr whole body 3 rem/yr = 30 mSv/yr to thyroid	10^4 rem/yr = 100 Sv/yr whole body 10^4 rem/yr = 100 Sv/yr to thyroid
Process Equipment Failure plus Failure of any Safety System (Dual Failure)	1 per 3 x 10^3 years	25 rem/yr = 250 mSv/yr whole body 250 rem/yr = 2500 mSv/yr to thyroid	10^6 rem/yr = 10^4 Sv/yr whole body 10^6 rem/yr = 10^4 Sv/yr to thyroid

There are some noted problems with the single / dual mode failure approach.

1. What about multiple failures? It is possible for some of them to be more probable than the S/D events.
2. There is no way to put events in perspective for risk analysis or assessment of design alternatives. Indeed, a systematic review based on the PSA approach revealed that the failure of support systems can adversely affect plant safety through their effect on many systems.
3. The conservative nature of the event sequences and analysis tended to mislead operations as to what to expect in the event of a real emergency.
4. Complex systems were treated too simplistically.
5. There was no framework for post event sequence analysis.

Hence, the PSA approach was adopted for Bruce A and B, Pickering A and B, and CANDU 600.

The target was further reduced to 10^{-7} events / year for individual events.

Early PSAs that were conducted on support systems were called Safety Design Matrices or SDMs.

3.7 Frequency-based Targets

Largely driven by a need to assess whether design changes were warranted, the S/D targets were plotted as shown in figure 3.1 as a reference guide.

A line was draw between the single and dual mode points and extrapolated to serve as a guide for events of higher and lower doses and frequencies.

If an event fell to the right of the line, then a redesign or some other form of mitigation was required. This proved useful in ferreting out design weaknesses.

However, as Snell points out, the very fact of conducting a systematic assessment leads to finding faults (and fixing them before a final PSA is done).

The actual position of the line is probably of secondary importance since high frequency events are too uneconomical to allow and because the basic design of CANDU (employing group separation, defence in depth, etc) is basically sound (figure 3.2).

3.8 The Evolution Continues

In 1977, the AECB formed the Inter-Organizational Working Group (IOWG) to identify, clarify and document the Canadian safety principles. Six levels of dose were defined as shown in table 3.5 and figure 3.2. An individual event cutoff at 10^{-7} was retained. This led to C-6, an AECB document.

Table 3.5 IOWG Proposed Dose/ Frequency Guidelines

	Sum of frequencies of all events in dose interval must be less then (per year)	Reference Individual Whole Body Dose Interval (rem)	Reference Individual Thyroid Dose Interval (rem)
1	10^{-1}	0.00 - 0.05	0.00 - 0.5
2	10^{-2}	0.05 - 0.5	0.5 - 5
3	10^{-3}	0.5 - 5	5 - 50
4	10^{-4}	5 - 10	50 - 100
5	10^{-5}	10 - 30	100 - 300
6	10^{-6}	30 - 100	300 - 1000

In 1980, the AECB issued C-6 for consultation purposes. Five event classes were defined, (discussed in more detail in the next chapter) each with its own frequency and dose limits (see table 3.6).

The AECB has never acknowledged these frequencies; they are simply implied by the industry.

The main problem with this approach was that specific events, such as LOCA or feedwater failure, were assigned **a priori** to a frequency class. This gave a distorted view of the actual safety picture.

Also it removed some of the incentive for the designer to improve the design. The event frequencies are design specific and such an approach impacts on new and novel designs.

In addition, an upper limit on whole body individual dose (25 rem) was set, even for events less frequent than dual failures. In total, this approach seems to be a step backward from even the S/D approach but its requirement for a systematic plant review is good. C-6 was used on a trial basis on Darlington although Ontario Hydro has done a full PSA in parallel. Currently, a deterministic approach is used to design the safety systems and a PSA is conducted for the purposes of a systematic plant review, in the spirit of C-6.

Table 3.6 C6 Proposed Dose Guidelines

	Derived Frequency of Occurrence (events per reactor year) [Assumed but not defined in C6]	Reference Individual Whole Body Dose Interval (Sv) [1 Sv = 100 rem]	Reference Individual Thyroid Dose Interval (Sv)
CLASS 1	$>10^{-2}$	0.0005	0.005
CLASS 2	10^{-2} - 10^{-3}	0.005	0.05
CLASS 3	10^{-3} - 10^{-4}	.03	0.3
CLASS 4	10^{-4} - 10^{-5}	0.1	1
CLASS 5	$<10^{-5}$	0.25	2.5

The Advisory Committee on Nuclear Safety advises the AECB.

In 1983 it issued a report, ACNS-4, which set an upper limit on whole body dose at 100 rem, permitted the use of realistic event frequencies and accident consequence models and retained the cutoff frequency of 10^{-7}.

The limits are very risk adverse and the dose criteria appear to be too restrictive.

It has not been adopted for use.

3.9 Current Canadian Practice

[NAT85a] notes:

> "In Canada, the AECB does not set detailed design requirements for nuclear power plants. Following the long-established principle, in Canadian safety philosophy, that the primary and ultimate responsibility for the safety of a nuclear reactor installation rests with the licensee, the AECB establishes only the general safety criteria and targets."

Currently, the AECB regulatory documents such as C6, R7, R8, R9 and R10 that govern nuclear safety in Canada are essentially deterministic and are based on (but not limited to) prescribed single and dual mode failures, forming the Design Basis Accidents that must be considered.

Dose limits are as per table 3.4. These dose limits are supplemented by general safety principles and subsidiary criteria as discussed in Chapter 8.

Moreover, C6 calls for a systematic plant review to identify those events which pose a risk to the public.

The inclusion of dual failures forces one to look systematically at the design of mitigating systems - in effect, don't put all your eggs into one basket.

Overall, this combined deterministic / probabilistic approach provides two generically different views of safety - another form of defence in depth.

According to[TIN90], AECL conducted such a review and categorized the events as per table 3.7.

Table 3.7 Safety Analysis Event Categories

Category	Type of analysis required	Evaluation objectives	Evaluation methodology
A	Deterministic analysis	Assess the performance of the special safety systems	Pessimistic assumptions
B	Probabilistic analysis	Assess the most probable plant responses; identify the dependence on operator action; demonstrate independence between initiating event and mitigating systems	Realistic assumptions
C	Common cause analysis	Assess plant's ability for safe shutdown, decay heat removal and containment of radioactivity for common-cause events such as earthquakes	Qualitative assessment
D	Risk arguments	Assessment of the features of the plant design or operation which reduce the probability of certain postulated events to such an extremely low level that failure consequences need not be considered	Qualitative assessment

Category A events are further broken down into:

- A.1 Single / dual mode failure analysis
- A.2 Trip coverage
- A.3 LOCA with Loss of Class IV Power
- A.4 Special Containment Impairments

Appendix 2 provides more details on the categories as follows:

Table 2 to table5 (extracted from [TIN90] further defines the events to be analyzed. Tables 6, 7 and 8 define the events for categories B, C and D, respectively.

Category A events are subject to the dose limits of [HUR72], given in table 3.4.

In addition, the R-docs (R-7, R-8, R-9, etc.) require no new fuel failures or channel failures or other restrictions, depending on the event.

These are summarized in tables 9 - 11 of appendix 2.

Category B events are subject to the C-6 dose limits as given in table 3.6.

Although C-6 does not refer to event frequencies, the events have been binned according to the expected frequencies for typical CANDU designs.

It is tacitly assumed that, following the PSA approach, events found by a systematic station review to be below the "incredible" cutoff (10^{-6} events / yr.) do not require a consequence analysis.

To illustrate:

Category A LOCA - evaluate the performance of SDS, ECC, and containment.

Category B LOCA - evaluate realistic frequencies. Some combinations in category A are not credible (eg, large LOCA + failure of ECC).

Category C LOCA - ensure that an earthquake won't fail the HTS or damage the ECCS.

Category D LOCA - design so that the failure of a vessel such as the pressurizer is incredible by using codes and standards.

3.10 Safety Limits

Although the focus so far has been on the probabilistic assessment of risk, we should not lose sight of the role that good design practice plays in overall plant safety. This is discussed in some detail in Chapter 8.

Of note in the context of safety criteria is the notion of safety limits. One example of a safety limit is the dryout limit.

Design targets are used during the process and safety system design phase to provide a defined margin to the onset of dryout, centreline fuel melting and other indications of the beginning of a failure limit.

Neither dryout nor centreline melting constitutes a failure per se but are considered prudent limits for design purposes.

This practice adds considerable conservatism and robustness to the overall design.

Codes and standards that are typically used are listed in the appendix 3 [from TIN90 and NAT85a]

3.11 Safety Evaluation Process

Overview diagrams of the safety evaluation process as per CANDU 9 LBD as shown in the appendix 4 [TIN90 and LBD94].

3.12 Exercises

1. Summarize this chapter on a one page concept diagram.

2. Establish safety goals for a small research reactor such as the MNR.

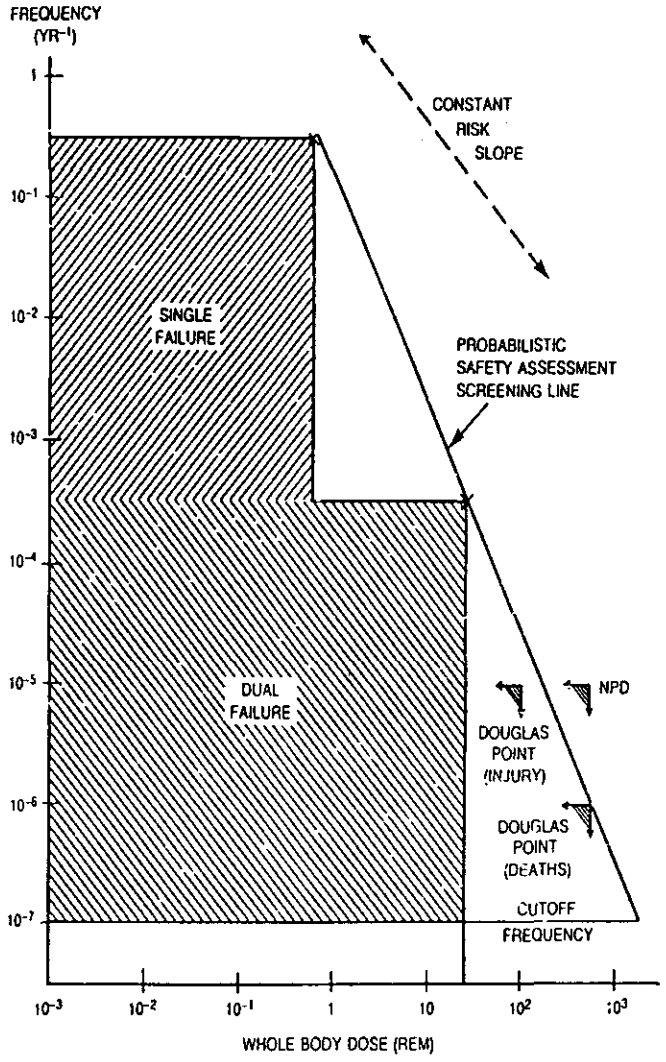

Figure 3.1 Probabilistic Safety Assessment (SDM) Screening Line [Source: SNE86]

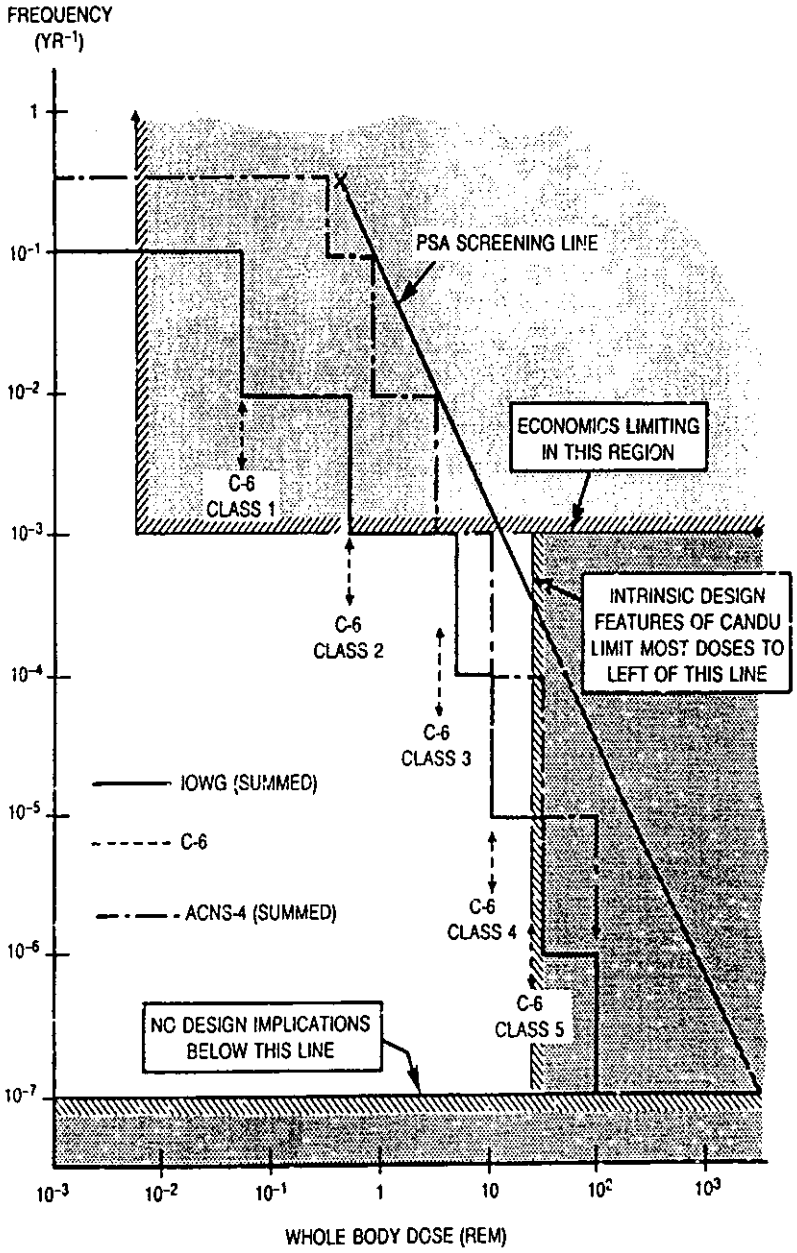

Figure 3.2 Comparison of Safety Goals and "Natural" Restrictions [Source: SNE86]