Lecture 8 – Safety Goals

Dr. V.G. Snell*
Nuclear Reactor Safety Course
McMaster University

*Material on human error from R. Duffey gratefully acknowledged
Where We Are

Experience

Chapter 3

Safety Goals

Chapter 6

Deterministic Requirements

Design Basis Accidents

Chapter 2

Safety Analysis

Chapters 7 & 8

Mitigating Systems

Chapter 5

Probabilistic Requirements

Probabilistic Safety Analysis

Chapter 4

Credible Accidents

Plant safety as designed

Plant safety as operated

Safety Culture

Good Operating Practice

Chapter 9
Is this a useful safety goal?

European Pressurized Reactor:

“Accidents liable to lead to significant early radioactive releases, in particular accidents involving high-pressure core meltdown, must for their part be ‘practically eliminated’”
How Safe is Safe Enough?

- Require numerical, not qualitative goal, e.g.:

  "The annual risk of death to the most exposed member of the public due to accidents in a reactor should be small in comparison to his/her total risk of premature death."
Concepts

1. Compare like to like – risk of premature death

2. Compare risk from nuclear power to risk from all other sources – why?
   - Where are benefits compared?
   - How much of the fuel cycle is included?
   - What about global effects?
Concepts – cont’d

3. Limit risk to *individual*
   - Exclude (or assume bounded): population exposure, land contamination, effects on animals & plants, psychological effects

4. Goal refers to *public*, not workers
   - Acceptance of risk is ‘part of a job’
   - Industrial hazards dominate anyway

5. What is the risk of *not* having nuclear power?

   *Safety Goal is not unique; other models.*
Sub-Goals

- The annual risk of *prompt* death to the most exposed member of the public due to accidents in a reactor should be small in comparison to his/her total annual risk of prompt death due to all accidents.

- The annual risk of *fatal cancer* to the most exposed member of the public due to accidents in a reactor should be small in comparison to his/her total annual risk of fatal cancer due to all causes.
Risk of Dying in Canada

- Accidents fifth leading cause of death
- Rate of 27.6 deaths / 100,000 people /a
- Average person’s risk of death from an accident is $3 \times 10^{-4}$ per year, so e.g.:

  ‘The likelihood of a large release from a nuclear power plant in an accident should be less than 3 per $10^6$ reactor years’
Occupational Risk of Death in the U.S.

Number and rate of fatal occupational injuries, by industry sector, 2008*

- **Construction**: 969, 9.6
- **Transportation and warehousing**: 762, 14.2
- **Agriculture, forestry, fishing, and hunting**: 651, 2.3
- **Government**: 522, 2.5
- **Manufacturing**: 404, 2.7
- **Professional and business services**: 389, 2.7
- **Retail trade**: 290, 2.0
- **Leisure and hospitality**: 233, 2.2
- **Wholesale trade**: 175, 4.2
- **Mining**: 175, 18.0
- **Other services (exc. public admin.)**: 172, 2.5
- **Educational and health services**: 137, 0.7
- **Financial activities**: 103, 1.0
- **Information**: 45, 1.4
- **Utilities**: 36, 3.8

**Total fatalities** = 5,071

**All worker fatality rate** = 3.6

*Data for 2008 are preliminary.

NOTE: In 2008, CFOI implemented a new methodology, using hours worked for fatality rate calculations rather than employment. For additional information on the fatality rate methodology changes please see http://www.bls.gov/iif/oshnotice10.htm.

Table 6-2 - Cause of Death in Canada (Accident, non-Occupational)

<table>
<thead>
<tr>
<th>Cause of Death</th>
<th>Mortality rate (/100,000-year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motor vehicle accidents</td>
<td>8.7</td>
</tr>
<tr>
<td>Falls</td>
<td>5.4</td>
</tr>
<tr>
<td>Poisoning</td>
<td>2.8</td>
</tr>
<tr>
<td>Homicide</td>
<td>1.7</td>
</tr>
<tr>
<td>Drowning</td>
<td>0.8</td>
</tr>
<tr>
<td>Fire</td>
<td>0.7</td>
</tr>
</tbody>
</table>
Risk of Cancer in Canada

- Malignant neoplasm second leading cause of death
- Rate of 173 deaths per 100,000 people /a
- Average person’s risk of dying from cancer is $1.7 \times 10^{-3}$ per year (≈ 13% over 75-years)
  - 100 person-Sv $\Rightarrow$ ≈5 fatal cancers
  - “Averaged” risk of $5 \times 10^{-2}$ fatal cancers per Sv
  - Equivalent dose is 0.035 Sv per year per person
Possible Safety Sub-Goal for Delayed Fatalities

- Maximum time-averaged individual dose from accidents should be less than 0.35 mSv per year, averaged over a group of people
  - ~ 35% natural background radiation
  - Should nuclear power be ‘safer’ than background radiation?
- Requires summation of all accidents
Risk Acceptance

- Higher values accepted for:
  - Occupational risk
  - Voluntary risk
  - Familiar risk
  - Perceived direct benefit

- Lower values accepted for:
  - Involuntary risk
  - Unfamiliar risk
  - ‘Dread’
ACNS Again

- Requires PSA
- 6 dose bins
- In each bin, summed frequency of accidents must be < frequency limit
- $10^{-7}$/year cutoff
- Average dose of 2.5 mSv/year
International Goals

- Existing reactors:
  - The frequency of a core melt (severe core damage) accident must be less than $10^{-4}$ per reactor-year
  - The frequency of a large release must be less than $10^{-5}$ per reactor-year
  - i.e., CCF probability $< 0.1$
- New reactors: factor of 10 lower
# UK Safety Assessment Principles

<table>
<thead>
<tr>
<th>Maximum effective dose (mSv)</th>
<th>Total predicted frequency, per year</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Basic Safety Limit</td>
</tr>
<tr>
<td>0.1 - 1</td>
<td>1</td>
</tr>
<tr>
<td>1 - 10</td>
<td>10⁻¹</td>
</tr>
<tr>
<td>10 - 100</td>
<td>10⁻²</td>
</tr>
<tr>
<td>100 - 1000</td>
<td>10⁻³</td>
</tr>
<tr>
<td>&gt;1000</td>
<td>10⁻⁴</td>
</tr>
</tbody>
</table>
UK Safety Goals from Safety Assessment Principles

Dose Limit (mSv)

Frequency (/yr)

0.1 - 1

1 - 10

10 - 100

100 - 1000

> 1000

BSL

BSO

UK Safety Goals from Safety Assessment Principles
RD-337 - CNSC Safety Goals

Basis:

- Individuals should bear no significant additional risk to life and health.
- Societal risks to life and health shall be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.
**Numerical Values**

**Core Damage Frequency:** The sum of frequencies of all event sequences that can lead to significant core degradation is less than $10^{-5}$ per reactor year.

**Small Release Frequency:** The sum of frequencies of all event sequences that can lead to a release to the environment of more than $10^{15}$ becquerel of iodine-131 is less than $10^{-5}$ per reactor year. A greater release may require temporary evacuation of the local population.

**Large Release Frequency:** The sum of frequencies of all event sequences that can lead to a release to the environment of more than $10^{14}$ becquerel of cesium-137 is less than $10^{-6}$ per reactor year. A greater release may require long term relocation of the local population.
Limitations of Risk Approach

- All events have to be identified and summed
  - Hard to do early in design, no useful measure
- No risk aversion in simplest application
  - Is it necessary?
- Frequency must be cut-off
  - What does a frequency of $10^{-8}$ / year mean?
- Not all events can be quantified
  - Severe external events; sabotage, terrorism & war
- Innovative designs
  - Incomplete reliability database
Are We Kidding Ourselves?

- Safety goals aimed at design
  - Essential to give design a logical base
  - Not readily confirmed in practice
- Assume that technology continually improves, so safety goals get more and more stringent
- Ignores the learning/forgetting hypothesis
From R. Duffey…

- The major cause of accidents is human error
- The causes are always obvious and preventable – afterwards
- There is usually a confluence of factors as a cause
- There is/are no “Zero Defects”
Airlines

Airsafe.com fatal accident data 1970-2000
110 airlines 210 million flights

1 per 200,000 hours
Commercial Aircraft Near Miss Rates

Reported Near Miss Rates

- US NMAC
- Canada Airprox
- UK Airprox
- NMAC learning curve model

Data Sources: FAA, CAA and TSB

Accumulated Experience (MFhrs)

0 50 100 150 200 250 300

1 per 200,000 hours
Is 1 per 200,000 the Best One can Do?

Fatal Accident Rate

~1 per 200,000 hours at 0.1 MF
How To Learn From Mistakes

- Mistakes are necessary to learn
- Technology change is not enough
- Be careful when using safety goals outside design
- Comprehensive indicator sets are now in use which are risk and performance-based
- Wide sharing of industry near-misses