Risk-Informed Design Guidance for Gen IV Reactors

22.39 Elements of Reactor Design, Operations, and Safety

Lecture 25

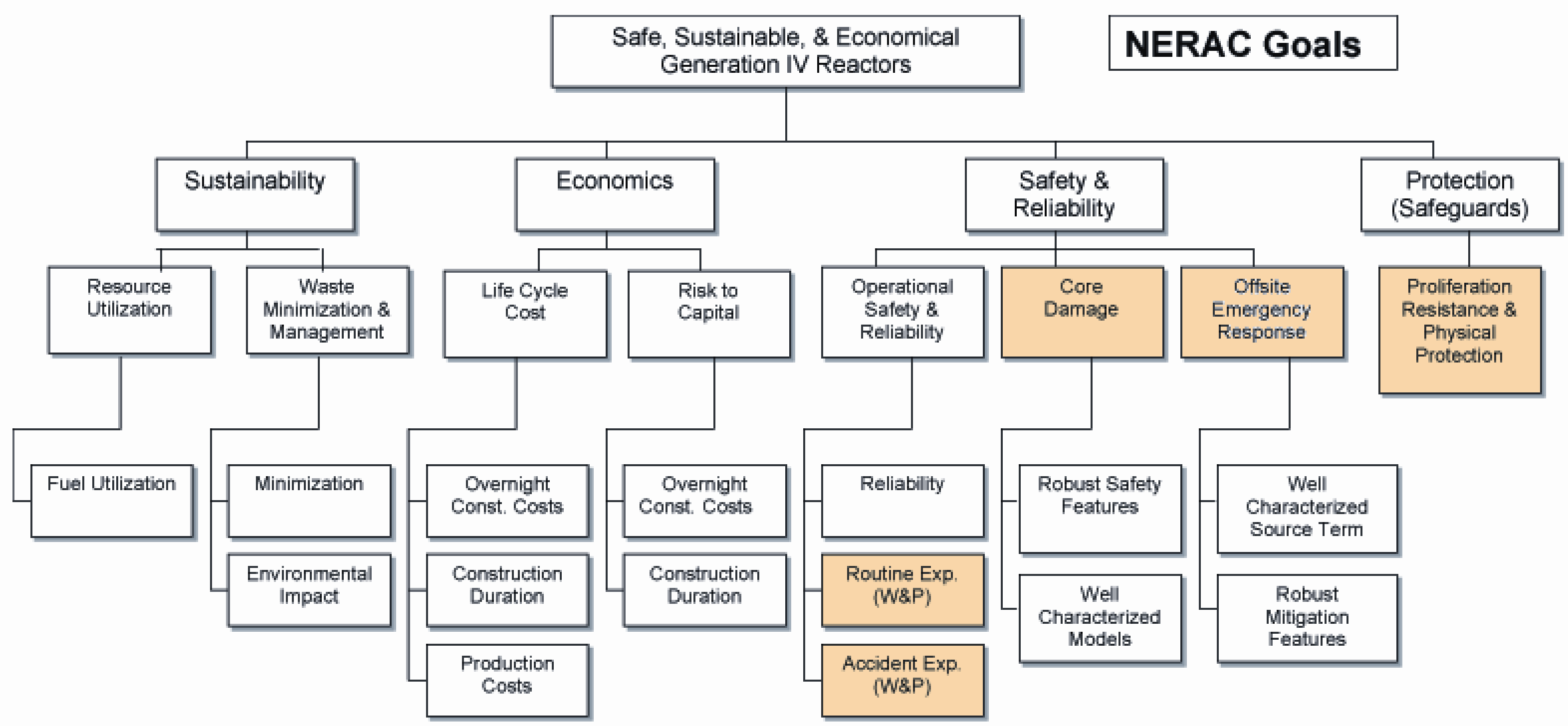
Fall 2006

George E. Apostolakis
Massachusetts Institute of Technology

Why Risk-Informed Design?

- The NRC is preparing a new risk-informed licensing process for future reactors.
- DOE (NERAC) goals refer to "reliable" reactivity control and decay heat removal.
- Important uncertainties are identified early.
- The combination of the *structuralist* (i.e., defense in depth) and the *rationalist* (i.e., risk-based) safety philosophies could be addressed early in the process.
- Design options can be compared.
- PRA methodological needs are identified early so that improvements can be made.

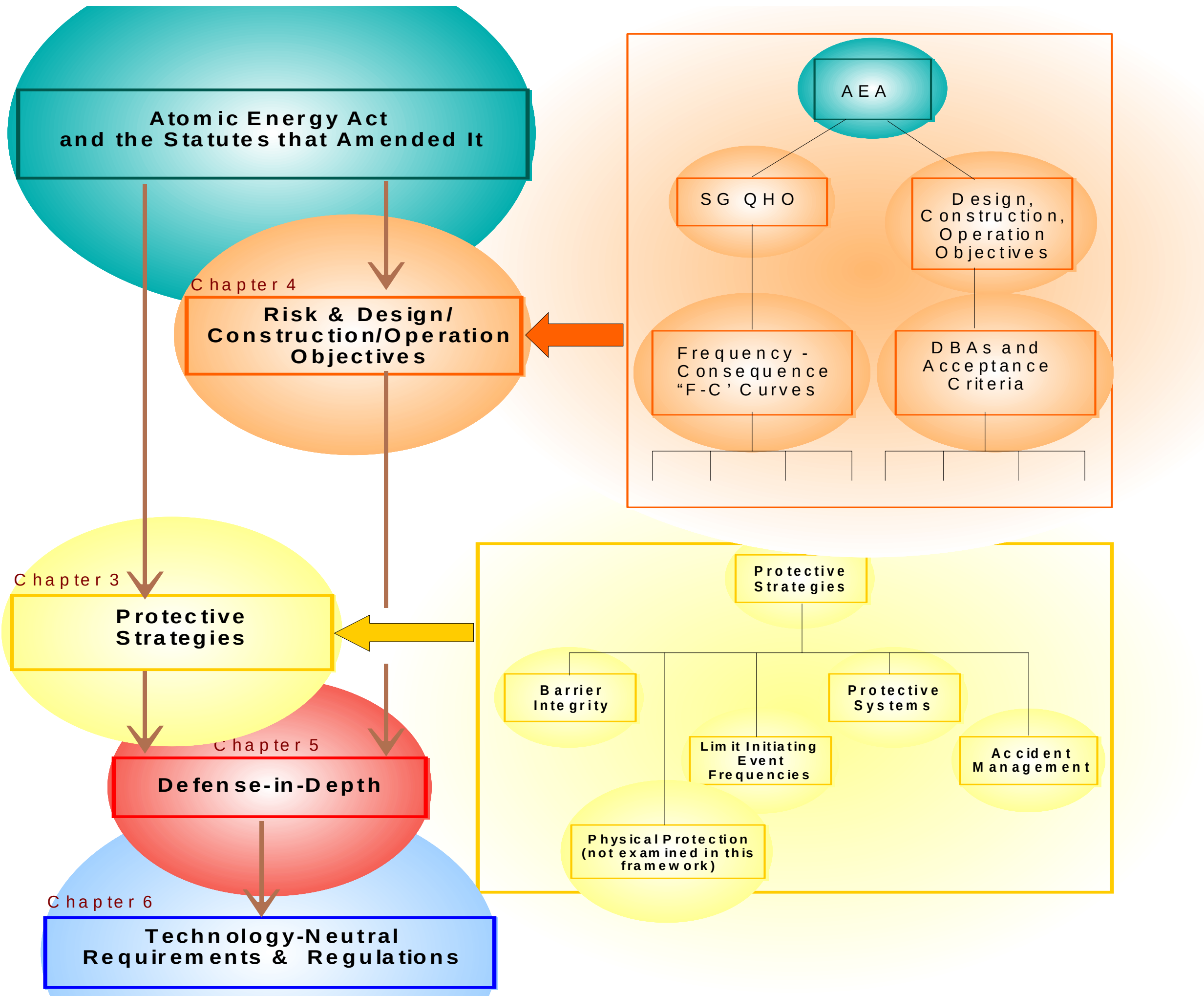
Sorensen, J. N., Apostolakis, G. E., Kress, T. S., and Powers, D. A., "On the Role of Defense in Depth in Risk-Informed Regulation," *Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment*, pp. 408-413, Washington, DC, August 22 - 26, 1999, American Nuclear Society, La Grange Park, Illinois.


Safe, Sustainable, & Economical Generation IV Reactors
NERAC Goals
Sustainability
Economics
Safety & Reliability
Protection (Safeguards)
Resource Utilization
Waste Minimization & Management
Life Cycle Cost
Risk to Capital
Operational Safety & Reliability
Core Damage
Offsite Emergency Response
Proliferation Resistance & Physical Protection
Fuel Utilization
Minimization
Environmental Impact
Overnight Const. Costs
Construction Duration
Production Costs
Overnight Const. Costs
Construction Duration
Reliability
Routine Exp. (W&P)
Accident Exp. (W&P)
Robust Safety Features
Well Characterized Models
Well Characterized Source Term
Robust Mitigation Features

Technology-Neutral Regulatory Framework (NUREG-1860)

- This alternative to 10 CFR 50 would have the following advantages:
  - It would require a broader use of design-specific risk information in establishing the licensing basis, thus better focusing the licensing basis, its safety analysis and regulatory oversight on those items most important to safety for that design.
  - It would stress the use of performance as the metrics for acceptability, thus providing more flexibility to designers to decide on the design factors most appropriate for their design.
  - It would be written to be applicable to any reactor technology, thus avoiding the time consuming and less predictable process of reviewing non-LWR designs against the LWR oriented 10 CFR 50 regulations, which requires case-by-case decisions (and possible litigation) on what 10 CFR 50 regulations are applicable and not applicable and where new requirements are needed.
  - It would provide the foundation for technology-specific implementation, through the use of technology-specific implementing guidance in those areas unique to a specific technology.

Technology-Neutral Regulatory Framework (USNRC)



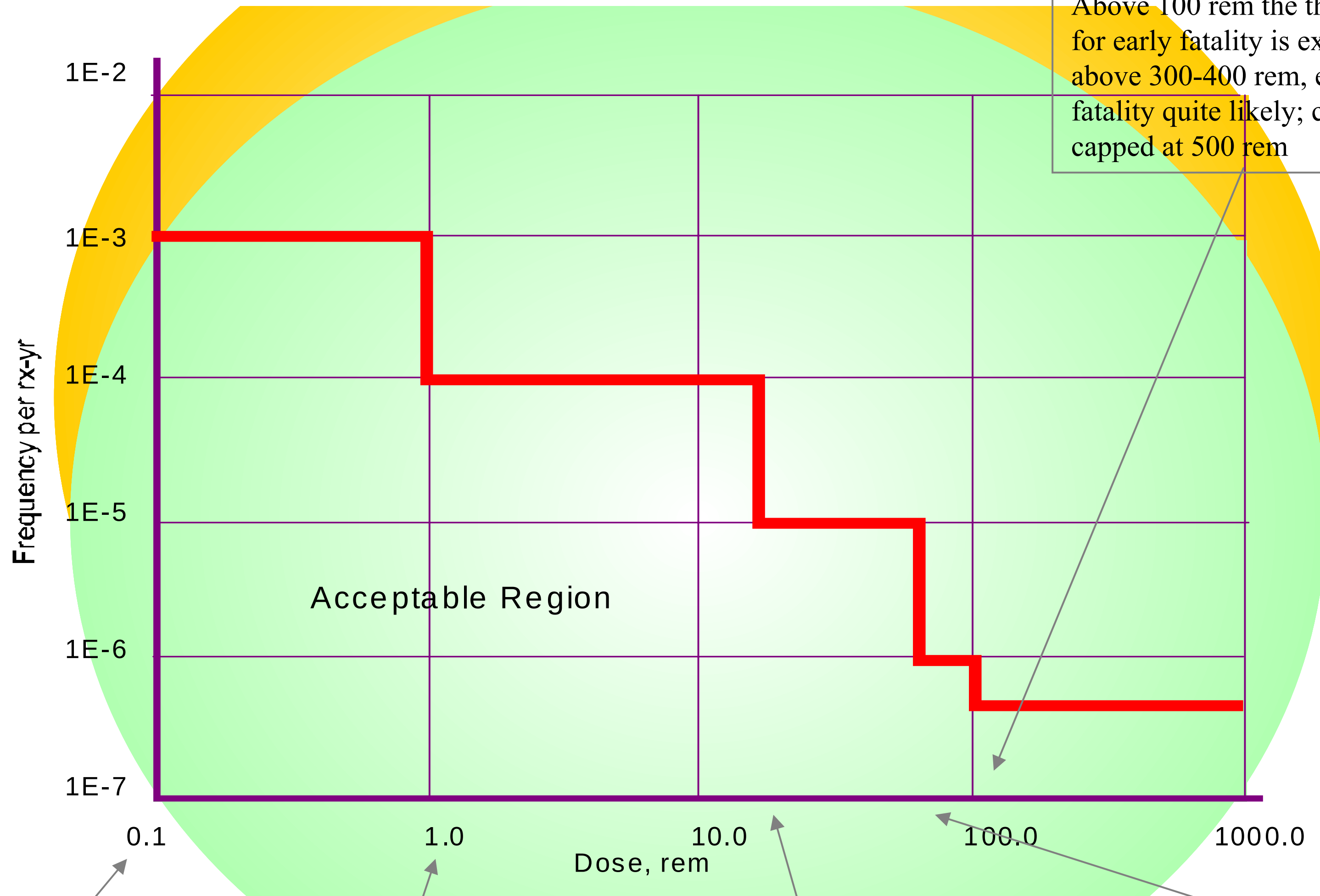
Defense in Depth

- The defense-in-depth principles address the various types of uncertainty (i.e., parameter, modeling and completeness) and require designs to:
  - consider intentional as well as inadvertent events;
  - include accident prevention and mitigation capability;
  - ensure key safety functions are not dependent upon a single element of design, construction, maintenance or operation;
  - consider uncertainties in equipment and human performance and provide appropriate safety margin;
  - provide alternative capability to prevent unacceptable releases of radioactive material; and
  - be sited at locations that facilitate protection of public health and safety.

Protective Strategies

- The protective strategies address accident prevention and mitigation and consist of the following:
  - physical protection (provides protection against intentional acts);
  - maintaining stable operation (provides measures to reduce the likelihood of challenges to safety systems);
  - protective systems (provides highly reliable equipment to respond to challenges to safety);
  - maintaining barrier integrity (provides isolation features to prevent the release of radioactive material into the environment); and
  - protective actions (provides planned activities to mitigate any impacts due to failure of the other strategies).

Frequency-Consequence Curve



Above 100 rem the threshold for early fatality is exceeded; above 300-400 rem, early fatality quite likely; curve is capped at 500 rem

100 mrem/yr – public dose limit in 10CFR50 App I

1 rem/event – triggers EPA protective action guidelines

25 rem/event – triggers abnormal occurrence reporting; limit in 50.34a and Part 100 for siting

50 rem/event – triggers early health effects

Comments on the F-C Curve

- The PRA results must demonstrate that the total integrated risk from the PRA sequences satisfy both the latent cancer QHO and the early fatality QHO.
- The summation of the risk from all the PRA sequences is carried out using the mean value of each sequence dose and frequencies.
- Meeting the F-C curve imposes additional constraints in addition to satisfying the QHOs because specific dose limits are imposed at all frequencies.
- Both the individual risk of each new reactor and the integrated risk from all of the new reactors at one site, associated with a future combined license application, should not exceed the risk expressed by the QHOs.
- It is not required that the integrated risk from existing reactors, where there are multiple reactors at a single site, meet the risk expressed by the QHOs, even though the site may be considered for new reactors.

Licensing Basis Events (LBEs)

- Event sequences that must be considered in the safety analysis of the plant and must meet some deterministic criteria in addition to meeting the frequency-consequence curve.
- Purpose:
  - to provide assurance that the design meets the design criteria for various accident challenges with adequate defense-in-depth (including safety margin) to account for uncertainties, and
  - to evaluate the design from the standpoint of the dose guidelines in the siting criteria of 10 CFR Part 100.

LBE Selection using PRA

1. Drop all PRA sequences with point estimate frequency < 1.E-8/yr.
2. For sequences with point estimate frequencies equal to or greater than 1E-8, determine the mean and 95th percentile frequency.
3. Identify all PRA event sequences with a 95th percentile frequency > 1E-7 per year.
4. Group the PRA event sequences with a 95th percentile frequency > 1E-7 per year into event classes (similar initiating events and similar accident behavior in terms of system failures and/or phenomena; similar source terms).
5. Select an event sequence from the event class that represents the bounding consequence.
6. Establish the LBE's frequency for a given event class. The frequency of an event class is determined by setting the LBE's mean frequency to the highest mean frequency of the event sequences in the event class and its 95th percentile frequency to the highest 95th percentile frequency of the event sequences in the event class.
7. Verify that each LBE meets the acceptance criteria.

LBE Frequency Categories

Category	Frequency	Basis
frequent	**> 10^{-2} per year**	Capture all event sequences expected to occur at least once in lifetime of a plant, assume lifetime of 60 years
infrequent	**10^{-5} < to < 10^{-2} per year**	Capture all event sequences expected to occur at least once in lifetime of population of plants, assume population of 1000 reactors
rare	**10^{-7} < to < 10^{-5} per year**	Capture all event sequences not expected to occur in the lifetime of the plant population, but needed to assess Commission's safety goals

Deterministic Criteria for LBEs

- In the "frequent" range:
  - no impact on the safety analysis assumptions occurs
  - no barrier failure occurs
  - redundant means of reactor shutdown remain functional
  - redundant means of decay heat removal remain functional
  - the cumulative dose meets the 5 mrem dose specification of Appendix I of 10 CFR 50

- In the "infrequent" range:
  - a coolable geometry is maintained
  - at least one barrier remains
  - at least one means of reactor shutdown remains functional
  - at least one means of decay heat removal remains functional
    - ✓ the cumulative dose of LBEs with frequencies greater than or equal to 1E-3 per year, has to meet the 100 mrem specification of 10 CFR Part 20.
    - ✓ for LBEs with frequencies less than 1E-3 per year the worst (maximum based on meteorological conditions) two hour dose at the EAB (exclusion area boundary) meets the F-C curve

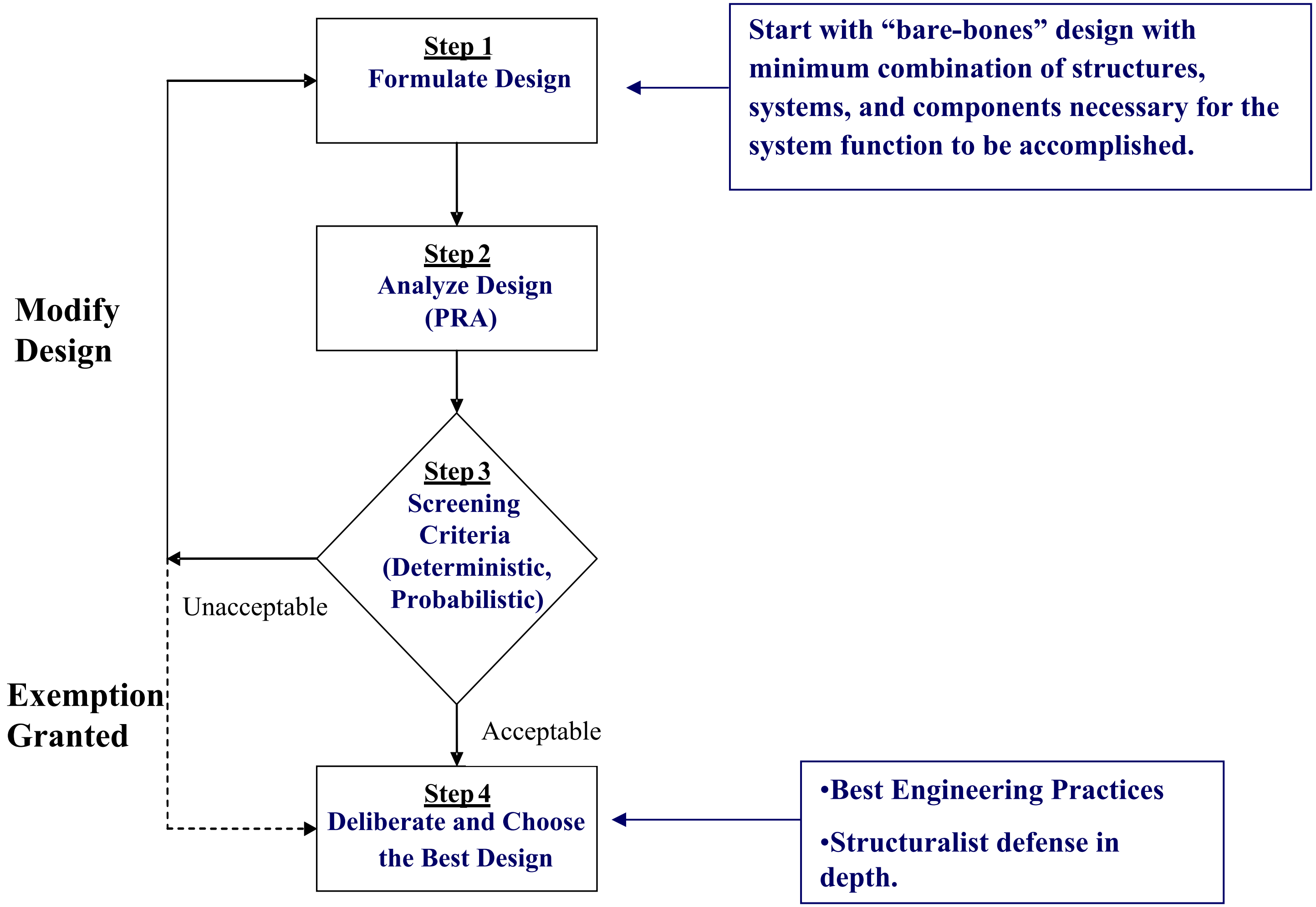
- For the "rare" range, no additional deterministic (DiD) criteria apply.
  - the 24 hour dose at one mile from the EAB meets the F-C curve

Category (Mean Event Frequency per reactor year)	PRA statistic for meeting F-C curve	LBE statistic for meeting F-C curve	Additional acceptance criteria for LBEs (demonstrated with calculations at the 95% probability value* with Success criteria that meet adequate Regulatory margin)
frequent (≥10-2)	mean	95th percentile*	no barrier failure; no impact on safety analysis assumptions; redundant means for reactor shutdown and decay heat removal remain functional; annual dose to a receptor at the EAB ≤5mrem TEDE
infrequent (< 10-2 to ≥10-5)	mean	95th percentile*	at least one barrier remains; a coolable geometry is maintained; at least one means of reactor shutdown and decay heat removal remains functional; for LBEs with frequency > 1E-3 annual dose to a receptor at the EAB ≤ 100mrem TEDE; for LBEs with frequency < 1E-3 the worst two-hour dose at the EAB meets the F-C curve
rare (<10-5 to ≥10-7)	mean	95th percentile*	24 hour dose at 1 mile from EAB meets the F-C curve

Notes

- With the exception of the source term, realistic calculations are carried out to obtain the mean and uncertainty distribution of the important parameters for estimating frequency and consequences.
- Source Term calculations use the 95% probability value of the amount of radionuclides released, obtained from a mechanistic calculation, and use RG 1.145 or the equivalent for calculating atmospheric dispersion.
- EAB - exclusion area boundary
- TEDE - total effective dose equivalent
- * The upper value of the 95% Bayesian probability interval.

The MIT Risk-Informed Design Process



Apostolakis, G.E., Golay, M.W., Camp, A.L., Durán, F.A., Finnicum, D., and Ritterbusch, S.E., "A New Risk-Informed Design and Regulatory Process," *Proceedings of the Advisory Committee on Reactor Safeguards Workshop on Future Reactors, June 4-5, 2001*, NUREG/CP-0175, US Nuclear Regulatory Commission, Washington, DC, 2001.

PRA as a Design Tool

- **Overall Objective: Eliminate Severe Accident Vulnerabilities**
- **PRA Provides a Systematic Means for Finding and Eliminating these Vulnerabilities**
- **Effectiveness May Be Limited by Information Availability Early in Design Phase**
- **Easier to Make Corrections Earlier in Design Phase**
- **Imperfect Tool is Better than None at All**

GE Presentation to the ACRS PRA Subcommittee, April 20, 2006.

Evolution of a Design and PRA

Conceptual Design	Design Base (DCD)	Detailed Design	Construction Design	Plant in Operation
Is Design Feasible?	Can Design be Licensed?	Will Design be Licensed?	Confirmation of Assumptions	Confirmation of Assumptions
Low Design Detail	Major Components Specified	All Components Specified	All Components Described	All Components Described
Qualitative Risk Assessment	Qualitative & Quantitative PRA	Quantitative PRA with Gaps	Quantitative PRA with Fewer Gaps	As-Built As-Operated PRA
Defense-in-Depth Concepts	Defense-in-Depth Analyzed	Defense-in-Depth Mostly Resolved	No Defense-in-Depth Issues	No Defense-in-Depth Issues
Past Vulnerabilities Addressed	Sequence Level Vulnerabilities Eliminated	System Level Vulnerabilities Eliminated	Component Level Vulnerabilities Eliminated	All Vulnerabilities Eliminated

GE Presentation to the ACRS PRA Subcommittee, April 20, 2006.

Applications

- **IRIS** (Y. Mizuno, H. Ninokata, and D. J. Finnicum, "Risk-informed design of IRIS using a level-1 probabilistic risk assessment from its conceptual design phase," *Reliability Engineering and System Safety*, 87:201–209, 2005)

- **GFR: Decay Heat Removal after a LOCA** (Delaney, M. J., Apostolakis, G. E., and Driscoll, M. J., "Risk-Informed Design Guidance for Future Reactor Systems," *Nuclear Engineering and Design*, 235:1537-1556, 2005)

- **GFR: Uncertainties in Passive Cooling Systems** (Pagani, L. P., Apostolakis, G. E., and Hejzlar, P., "The Impact of Uncertainties on the Performance of Passive Systems," *Nuclear Technology*, 149:129-140, 2005)

ECCS Designs 1-6 (LOCA)

Bare-bones system of MIT GFR concept (SCO_2 cooled, direct cycle)

Figure removed due to copyright restrictions.
See Delaney, M.J., Apostolakis, G.E., and Driscoll, M.J., "Risk-Informed Design Guidance for Future Reactor Systems." Nuclear Engineering and Design 235 (2005):1537-1556.

Designs 1- 6

1. **Bare-bones system**
2. **+Diesel (1x100%), DC battery (1x100%)**
3. **+Diesel (1x100%), DC battery (2x100%)**
4. **+Diesel (2x100%), DC battery (2x100%)**
5. **+Diesel (2x100%), DC battery (2x100%), DC transmission (2x100%)**
6. **+Diesel (3x100%), DC battery (2x100%), DC transmission (2x100%)**

Design 7: Secondary Onsite AC Power

Figure removed due to copyright restrictions.
See Delaney, M.J., Apostolakis, G.E., and Driscoll, M.J., "Risk-Informed Design Guidance for Future Reactor Systems." Nuclear Engineering and Design 235 (2005):1537-1556.

Design 7

- Diesel (3x100%)
- DC battery (2x100%)
- DC transmission (2x100%)
- Turbine (1x100%)
- Accumulator(1x100%)
- Electric valve (1x100%)
- Generator (1x100%)
- Secondary electric motor

Design 8: Microturbine (secondary onsite AC power)

Figure removed due to copyright restrictions.
See Delaney, M.J., Apostolakis, G.E., and Driscoll, M.J., "Risk-Informed Design Guidance for Future Reactor Systems." Nuclear Engineering and Design 235 (2005):1537-1556.

Design 8

- Diesel (3x100%)
- DC battery (2x100%)
- DC transmission (2x100%)
- Microturbine (1x100%)
- Natural gas accumulator(1x100%)
- Electric switch (1x100%)
- Generator (1x100%)
- Offsite natural gas connection (1x100%)
- Secondary electric motor

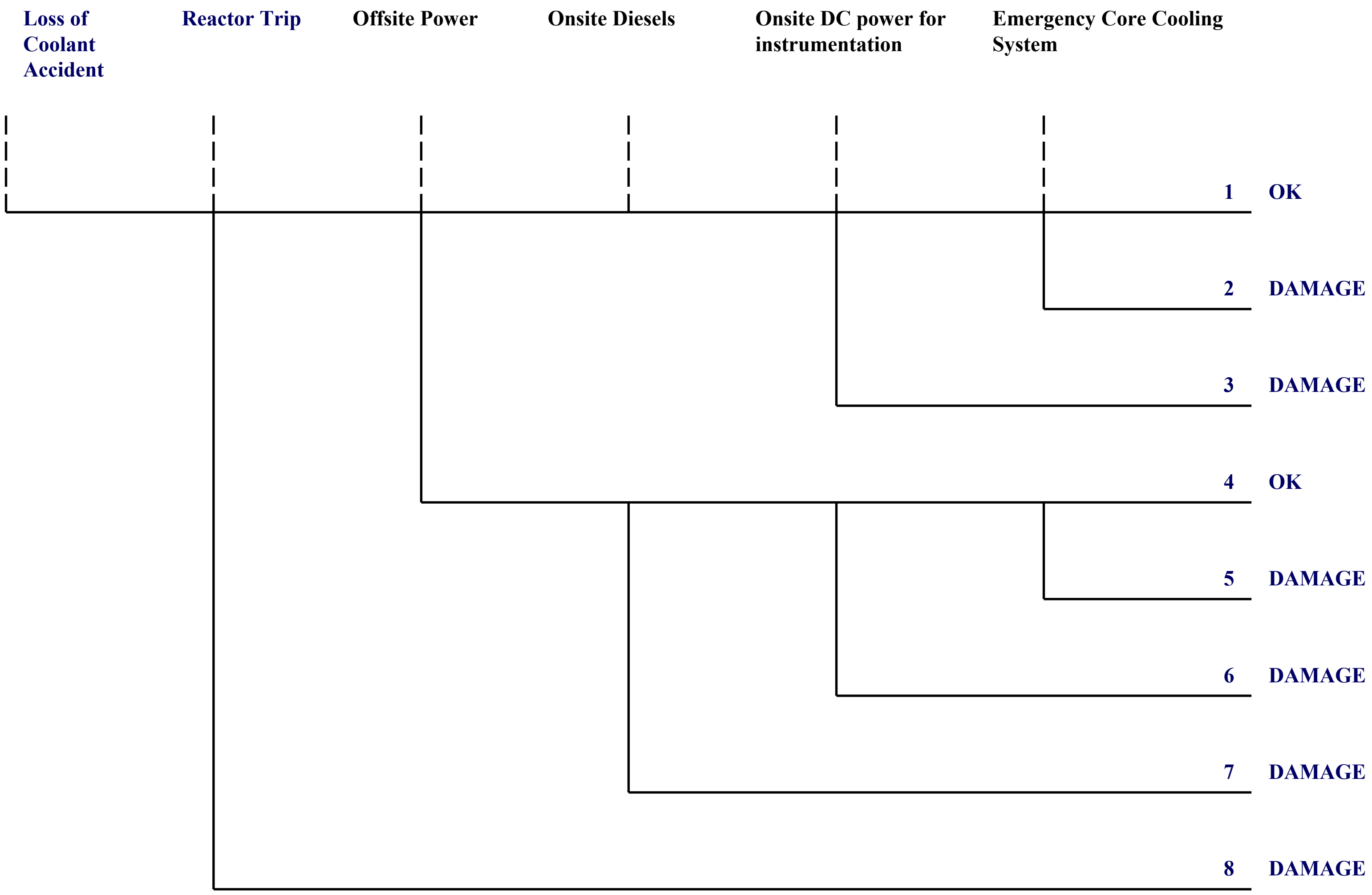
Design 9: Nitrogen Accumulator

Figure removed due to copyright restrictions.
See Delaney, M.J., Apostolakis, G.E., and Driscoll, M.J., "Risk-Informed Design Guidance for Future Reactor Systems." Nuclear Engineering and Design 235 (2005):1537-1556.

Design 9

- **Diesel (3x100%)**
- **DC battery (2x100%)**
- **DC transmission (2x100%)**
- **Nitrogen accumulator(1x100%)**
- **Electric valve**
- **Pressure valve**
- **Turbine**

Event Tree (Designs 1-6)



Results of the Iterative ECCS Design Guidance

Design	Configuration	CDF (3x100% ECCS Loops)	CDF reduction factor
1	No Diesels, 1x100% DC Battery	1.21×10^{-5}	1.00
2	1x100% Diesel, 1x100% DC Battery	1.29×10^{-6}	9.4
3	1x100% Diesel, 2x100% DC Battery	8.59×10^{-7}	14.1
4	2x100% Diesel, 2x100% Battery	3.11×10^{-7}	39.0
5	2x100% Diesel, 2x100% Battery, 2x100% Transmission	2.47×10^{-7}	49.0
6	3x100% Diesel, 2x100% Battery, 2x100% Transmission	1.64×10^{-7}	73.8
7	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Turbine	7.96×10^{-8}	152.0
8	3x100% Diesel, 2x100% Battery, 2x100% Transmission, 1x100% Secondary onsite Microturbine	7.58×10^{-8}	159.6
9	3x100% Diesel, 2x100% Battery, 2x100% Transmission, Nitrogen Accumulator	1.35×10^{-7}	89.6

PRA Insights

Design Number	Configuration	PRA Insights (3x100% ECCS Loops)
1	No Diesels, 1x100% DC Battery	•LOOP accounts for ~99% of risk
2	1x100% Diesel, 1x100% DC Battery	•Failure of diesel is largest contributor to risk (50.3%)
3	1x100% Diesel, 2x100% DC Battery	•1 Diesel account for 86.6% of risk
4	2x100% Diesel, 2x100% Battery	•LOOP + CCF of diesels accounts for 14.5% of risk •LOOP + random failure of diesels accounts for 27.1% of risk •1 DC Transmission loop accounts for 25.1% of risk
5	2x100% Diesel, 2x100% Battery, 2x100% Transmission	•LOOP + CCF of diesels accounts for 18.5% of risk •LOOP + random failure of diesels accounts for 35.5% of risk
6	3x100% Diesel, 2x100% Battery, 2x100% Transmission	•LOOP + CCF of diesels accounts for 2.84% of risk •LOOP + random failure of diesels accounts for 1.8% of risk
7	3x100% Diesel, 2x100% Battery, 2x100% Transmission , 1x100% Secondary onsite Turbine	•~99% of risk due to CCF of ECCS or DC components
8	3x100% Diesel, 2x100% Battery, 2x100% Transmission , 1x100% Secondary onsite Microturbine	•~99% of risk due to CCF of ECCS or DC components
9	3x100% Diesel, 2x100% Battery, 2x100% Transmission , Nitrogen Accumulator	•~99% of risk due to CCF of ECCS components
9	3x100% Diesel, 2x100% Battery, 2x100% Transmission , Nitrogen Accumulator	•~86.6% of risk due to CCF of ECCS components •12.1% of risk due to random failure of ECCS components

Criteria and Goals

- **Deterministic Criterion** (General Design Criterion 35)
  - An ECCS must be designed to withstand the following postulated LOCA: A double-ended break of the largest reactor coolant line, the concurrent loss of offsite power, and a single failure* of an active ECCS component in the worst possible place.

*Common-cause failures are not considered single failures.

- **Probabilistic Goal**
  - $f_{LOCA} = 5.45 \times 10^{-4}$ per reactor year → "infrequent initiator" →
    - ✓ Conditional Core Damage Probability (CCDP) $\leq 10^{-2}$

      AND
    - ✓ f_{LOCA} x CCDP $\leq$ 10% of the CDF goal of 10^{-4} per reactor year = 10^{-5}
  - CCDP $\leq 10^{-2}$ is the only goal in this case

Screening based on Probabilistic Goals (Designs 1-5)

Conditional Core Damage Probability given a LOCA						
	Number of ECCS Loops					
Design	1x100%	2x100%	3x50%	3x100%	4x50%	PRA Insights (3x100% ECCS Loops)
	Mean CCDP					
1	No	No	No	No	No	LOOP accounts for ~99% of risk
	2.51E-02	2.20E-02	2.20E-02	2.20E-02	2.20E-02	
2	Yes*	Yes*	Yes*	Yes*	Yes*	Failure of diesel is largest contributor to risk (50.3%)
	5.71E-03	2.32E-03	2.36E-03	2.31E-03	2.31E-03	
3	Yes*	Yes	Yes	Yes	Yes	1 Diesel accounts for 86.6% of risk
	4.86E-03	1.68E-03	1.72E-03	1.67E-03	1.67E-03	
4	Yes*	Yes	Yes	Yes	Yes	LOOP + CCF of diesels accounts for 14.5% of risk
	3.82E-03	5.97E-04	6.29E-04	5.81E-04	5.81E-04	LOOP + random failure of diesels accounts for 27.1% of risk
						1 DC Transmission loop accounts for 25.1% of risk
5	Yes*	Yes	Yes	Yes	Yes	LOOP + CCF of diesels accounts for 18.5% of risk
	3.75E-03	4.69E-04	5.02E-04	4.52E-04	4.52E-04	LOOP + random failure of diesels accounts for 35.5% of risk

*Did not meet deterministic criteria.

Insights

- Data appropriate for gas reactors are needed.
- PRA insights were used to
  - change the configuration of the design (Designs 5 and 6)
  - add a secondary onsite power source (Designs 7 and 8)
  - add a nitrogen accumulator system (Design 9)
- Several designs satisfied the probabilistic goals but not the deterministic criteria. Are the latter "unnecessary regulatory burden?"
- Design 8 (3x100% loops; microturbine; elimination of the failure-to-start mode for an onsite AC power supply) is best in terms of CDF (7.58×10^{-8} ry^{-1}).
- Mircoturbines have never been used in a NPP emergency power supply system. As such, they will be thoroughly scrutinized during the licensing process. Data are needed.
- Adding redundant ECCS loops beyond 2x100% capability does not result in significant improvement (Designs 1-8). This is due to the insensitivity of the CCF models.
  - No quantitative guidance exists as to how the values of the beta factor change when the design changes.
  - Causes: hardware (48.3%), maintenance (26.1%), operations (14.1%), environment (11.5%).
- Deliberation allows
  - The inclusion of best engineering practices
  - Comparison with other NERAC goals (sustainability, economics, reliability, proliferation resistance, and physical protection)