NUCLEAR PLANT SAFETY COURSE

RISK-INFORMED REGULATORY APPROACH

Michael W. Golay
Professor of Nuclear Science and Engineering
Massachusetts Institute of Technology
Cambridge, MA 02139
June 23, 2005
TRADITIONAL NUCLEAR SAFETY REGULATION

- Rule Based
- Deterministic
- Focused Upon Satisfying Quantitative Criteria
  - Design basis accident (DBA) mitigation
  - Performance tests and inspections
  - Emergency drills
- Uncertainty Treated via
  - Conservative bias
  - Defense-in-depth redundancy
- Results Have Been Good Enough, But
  - Expensive
  - Unpredictable
  - Logically inconsistent
  - Undermining licensee responsibility for safety
OVERALL GOAL OF SAFETY-REGULATORY REFORM

• Create methods to assure consistency of nuclear power plant applicant and regulator in performance/goals for producing safe, economical power plants

**Major Elements:**
- Acceptance Criteria
- Comprehensive, consistent assessment methods
- Designers, operators

**Major Elements:**
- Acceptance Criteria
- Comprehensive, consistent assessment methods
- Regulators, designers, operators
RISK-INFORMED REGULATORY APPROACH – FUNDAMENTAL IDEAS

- Regulatory decisions are founded upon the informed beliefs of decision-makers.
- Any regulatory belief can and should be stated in a probabilistic format.

![Graph showing probability distribution](image)

\[ \text{Probability} \ (x < X < x+dx) = f(x)dx \]

- Regulatory acceptance criteria must reflect acceptable best-estimate performance expectations and uncertainties.
RISK-INFORMED REGULATORY APPROACH – FUNDAMENTAL IDEAS

• Regulatory questions and acceptance criteria should also be stated within a probabilistic framework.

• The probabilistic framework should be as comprehensive as possible:
  ■ utilize probabilistic and deterministic models and data where feasible - and use subjective treatments where not feasible,
  ■ state all subjective judgments probabilistically and incorporate into the PRA,
  ■ require both license applicant and regulatory staff to justify their decisions explicitly, and
  ■ initiate resolution process to resolve applicant-regulator disagreements.
Public Health & Safety as A Result of Civilian Reactor Operation

Evaluate Risk Against Safety Goals

Use PRA to Quantify Risk and Uncertainties

Limit Core Damage Frequency (Level 1 PRA)

Mitigate Releases of Radionuclides (Level 2 PRA)

Mitigate Consequences (Level 3 PRA)

Tactics

Identify Required Regulation based on Master Logic Diagram

Develop regulatory criteria for design, operation, inspection, maintenance, and testing of required elements.

Framework for Risk-Based Regulation and Design
COMPARISON OF NRC AND NERI RISK-INFORMED REGULATORY PROCESSES

Operating Plants (NRC/NEI)

Deterministic

Traditional (“Structuralist”) Approach

• Start with current designs and regulatory approvals.
• Justify risk-informed changes.
• Defense-in-depth remains as primary means of assuring safety.

Future Plants (NERI/New NEI Task Force)

Probabilistic

Risk-Based (“Rationalist”) Approach

• Develop new design and regulatory process.
• Use firm probabilistic criteria to assure safety.
• Use defense-in-depth and safety margins as needed.
RISK-INFORMED REGULATORY APPROACH . . .

- At all conceptual stages of development, nuclear power plant evaluation is performed probabilistically and is supported by deterministic analyses, tests, experience, and judgments.

- Safety results of defense-in-depth, performance margins, best-estimate performance, and subjective judgments are all incorporated into a comprehensive PRA
  - PRA is used as a vehicle for stating evaluator beliefs concerning system performance

- The level of detail of acceptance criteria becomes finer as the level of concept development increases
  - many LWR-based regulatory constructs (e.g., DBAs, GDCs) are not applicable to less mature design concepts.
## Stages of Nuclear Power Plant Concept Development

<table>
<thead>
<tr>
<th>Development Stage</th>
<th>Goals and Acceptance Criteria</th>
<th>Evaluation Tools</th>
<th>Relevant Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Concept</td>
<td>High level - qualitative</td>
<td>Qualitative, simple, deterministic</td>
<td>Experiences of other concepts, deterministic analyses</td>
</tr>
<tr>
<td>Initial detailed design</td>
<td>High level - quantitative</td>
<td>Quantitative – probabilistic, deterministic</td>
<td>Prior quantitative analyses</td>
</tr>
<tr>
<td>Final detailed design</td>
<td>Detailed – quantitative (design-specific subgoals)</td>
<td>Detailed – quantitative – probabilistic, deterministic</td>
<td>Prior quantitative analyses</td>
</tr>
<tr>
<td>N-th of a kind for a given plant type</td>
<td>Very detailed – quantitative (design specific criteria – DBAs, GDCs,....)</td>
<td>Very detailed – quantitative, probabilistic, deterministic, tests</td>
<td>Prior quantitative analyses, tests, field experience</td>
</tr>
</tbody>
</table>
NUCLEAR PLANT SAFETY COURSE

Public Health & Safety as a Result of Civilian Nuclear Reactor Operation

Reactor Safety

Radiation Safety

Safeguards

Public Radiation Safety
Occupational Radiation Safety
Physical Protection

Public Risk from Routine Operations
Worker Risk from Routine Operations

Initiating Events

Mitigating Systems

Barrier Integrity

Operational Modes

Full Power
Shut Down
Other

Internal Events

Frequent
Moderate
Rare

External Events

Frequent
Moderate
Rare

Core

Spent Fuel
Pool?

Waste?

Operational
Modes

Reactivity
Control

Coolant
Inventory

Pressure
Control

Containment

F-C
Curves

Emergency
Preparedness

CDF

CCFP or
LERF

F-LE

Public Risk from Accidents

Worker Risk
from Accidents

System
Model

Containment
Performance

Fission Product
Transport

Site
Model

Plant Damage

Accident
Progression
Bins

Release States

Public Health & Safety as a Result of Civilian Nuclear Reactor Operation

Radiation Safety

Safeguards

Public Radiation Safety
Occupational Radiation Safety
Physical Protection

Public Risk from Routine Operations
Worker Risk from Routine Operations

Initiating Events

Mitigating Systems

Barrier Integrity

Operational Modes

Full Power
Shut Down
Other

Internal Events

Frequent
Moderate
Rare

External Events

Frequent
Moderate
Rare

Core

Spent Fuel
Pool?

Waste?

Operational
Modes

Reactivity
Control

Coolant
Inventory

Pressure
Control

Containment

F-C
Curves

Emergency
Preparedness

CDF

CCFP or
LERF

F-LE

Public Risk from Accidents

Worker Risk
from Accidents

System
Model

Containment
Performance

Fission Product
Transport

Site
Model
NUCLEAR PLANT SAFETY COURSE

MASTER LOGIC DIAGRAM

Performance Goal Level

I
II
III
IV

GENERAL

CONCEPT SPECIFIC

V
VI
VII

Excessive Health Effects
Health-Effects

Offsite Release
Off-site-New

Release of Radioactive Material
Off-site

Failure to Contain Radionuclides
Containment-Fail

Release of Non-Core Material
Non-Core-Mat

Release of Core Material
Core-Mat

System Failure During Other Operational Modes
Other-Ops-Modes

System Failure During Shut-Down Mode
Shut-Down

System Failure During Full-Power Mode
Full-Power

Coolant Inventory Excursion
Cool-Inventor

Reactivity Excursion
Reactivity

Pressure Excursion
Pressure

Temperature Excursion
Temperature

Undesirable Coolant Inventory Decrease
Decrease-C

Undesirable Coolant Inventory Increase
Increase-C

Undesirable Reactivity Decrease
Decrease-R

Undesirable Reactivity Increase
Increase-R

Undesirable Pressure Decrease
Decrease-P

Undesirable Pressure Increase
Increase-P

Undesirable Temperature Decrease
Decrease-T

Undesirable Temperature Increase
Increase-T

Inadequate Exposure Mitigation
Exposure

Inadequate Emergency Response
ER

Inadequate Siting
Siting
NUCLEAR PLANT SAFETY COURSE

CONCEPT-SPECIFIC MASTER LOGIC DIAGRAM

Performance Goal Level
SPECIFIC FOR GAS
...COOLED RX

IV

V

VI

VII

VIII

Conditional Containment-Confinement Failure
Core-Rel - 1 Contain-Failure

Insufficient Isolation
Isolation

Filter Failure
Filter

Confinement Structural Failure
Structural

Excessive Fission Product Accumulation
Fission-Products

Other Initiators
Other-IE

Seismic Event
Seismic

Other Initiators
Other-IE

Seismic Event
Seismic

Other Initiators
Other-IE

Insufficient Radiative Heat Removal
Radiation-Heat

Cooling - 1

Radiation Transmission Retarded
Rad-Trans-Fail

Inadequate Radiative Heat Sink
Rad-Heat-Sink

Inadequate Material Temperature Limit
Temp-Excess

Insufficient Forced Coolant Flow
Cool-Flow

Inadequate Heat Sink
Con-Heat-Sink

Insufficient Coolant Inventory
Cool-Inventory

Other Initiators
Other-IE

Top Reflector Fails In the Core
Top-Reflector

Other Initiators
Other-IE

Top Reflector Fails In the Core
Top-Reflector

Other Initiators
Other-IE
FUNDAMENTAL INTERACTIONS BETWEEN LICENSE APPLICANT (OR LICENSEE) AND REGULATOR

- Should be formulated with probabilistic methods
- Acceptability negotiation for new license application or license revision
  - currently is deterministic
  - should be risk-based; completion of procedures, tools, and termination criteria is needed
- Plant construction oversight
  - can be deterministic, subject to risk-based oversight
- Plant operation oversight
  - can be deterministic, subject to risk-based oversight
BASIC DESIGN AND REGULATORY PROCESS – EMPLOYED TRADITIONALLY, REMAINS VALID TODAY

- Designer develops a plant design that both produces power reliably and operates safely
  - responsible for plant safety, using high level regulatory criteria and policies as inputs
- Regulator reviews the design
- Designer and regulator engage in a dialog
  - specific safety features, their performance criteria, and methods of design and analysis
- Documentation is developed throughout the process
  - designer documents the design basis
  - regulator documents the safety evaluation, policies established, and criteria for future reviews (e.g., Reg. Guides and Standard Review Plans, and possibly regulations)
PSA Modeling performed to determine the likelihood of specific outcomes:

- PSA provides the basis for design and regulatory compliance assessment
- PSA models include consideration of both aleatory and systemic uncertainties
- PSA is not totally risk based - margins are added to address uncertainties
SCHEMATIC DIAGRAM OF THE RISK-DRIVEN GENERIC DESIGN – BUILDS UPON A BARE-CONES DESIGN, USING AN ITERATIVE PROCESS

Bare-Bones Design

Deterministic analyses to identify failure modes

PRA to identify dominant failure modes

Add safety features for mitigation or prevention of dominant failure modes

Generic Risk-Driven Design must satisfy acceptability criteria
CLASSIFICATION OF EVENT SEQUENCES WITHIN THE RISK-INFORMED DBA APPROACH

Initial Sequences
- Very Small Leak
- Safety Relief Valve Stuck Open
- Small Pipe Break LOCA
- Pilot Operated Relief Valve Stuck Open
- RC Pump Seal Failure
- Medium Pipe Break LOCA
- Large Pipe Break LOCA

Shared Functional Challenges
- Insufficient RCS Inventory Control
- Insufficient RCS Pressure Control
- Insufficient RCS/Core Heat Removal

Classes
- **Very Small Leak**
  - SRV Stuck Open
- **Small Pipe Break LOCA**
  - PORV Stuck Open
  - RC Pump Seal Failure
- **Medium Pipe Break LOCA**
  - Large Pipe Break LOCA

Response Required
- Normal Coolant Make-Up
- Emergency High Pressure Coolant Injection
- Depressurization and Emergency Low Pressure Coolant Injection
APPORTIONMENT OF A PERFORMANCE GOAL INTO SUBGOALS

- Designer proposes apportionment - then negotiates with regulator
- Apportionment must reflect what is feasible in the design
- Example shows that the reliability/availability of mitigation systems reflects feasibility of the design

<table>
<thead>
<tr>
<th>Initiating Event</th>
<th>Initiating Event Frequency</th>
<th>Mitigation Unavailability</th>
<th>Core Damage Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Small LOCA</td>
<td>4E-3 /yr</td>
<td>1E-4</td>
<td>4E-7/yr</td>
</tr>
<tr>
<td>Small LOCA</td>
<td>2E-4 /yr</td>
<td>1E-3</td>
<td>2E-7/yr</td>
</tr>
<tr>
<td>Large LOCA</td>
<td>4E-5 /yr</td>
<td>1E-2</td>
<td>4E-7/yr</td>
</tr>
</tbody>
</table>

Example Acceptability Criterion: Achieved Total CDF due to LOCAs must be less than or equal to 2E-6 /yr

Achieved Total CDF due to LOCAs: 1E-6 /yr
EXAMPLE OF DESIGNER’S INITIAL RISK-INFORMED SUBMITTAL TO THE REGULATOR

- Two safety system divisions - each contains:
  - two active high-pressure injection trains
  - one active low-pressure injection train
  - cooling water (component cooling, service water, HVAC)
  - two diesel generators
  - DC (battery) power
- Shared support systems
  - chemical volume control system
  - off-site power
- PRA Includes:
  - deterministic analyses, data, models,
  - uncertainties, inter-dependencies, and common-cause failures
  - initiator data are from documented sources (NUREG/CR-5750)
  - component failure frequencies are estimated from existing PRA studies (for this LWR example problem)
NUCLEAR PLANT SAFETY COURSE

EXAMPLE OF NEGOTIATION BETWEEN APPLICANT AND REGULATOR

Design submittal - thought to be acceptable by applicant

Regulator disputes assumptions - requires new data

Result: Risk of failure to have adequate coolant levels too great

Cause: CDF due to high pressure LOCA is dominant contributor

Fix: Designer adds depressurization capability and revises PRA

Result: CDF due to LOCA still too high due to the high-pressure LOCA

Fix: Designer adds independent, redundant train of depressurization capability

Result: CDF remains too high due to support system common-cause failures (cooling water pump and diesel)
EXAMPLE OF NEGOTIATION BETWEEN APPLICANT AND REGULATOR . . .

Design is re-submitted to the regulator

**Evaluation-1:** Regulator reviews design and PRA with common-cause failure reduction. It is determined that further significant improvements in ensuring adequate core coolant levels cannot be accomplished at a reasonable cost or with an adequate degree of certainty - through use of a cost-benefit criterion.

**Evaluation-2:** The regulator compares the achieved level of function availability, including uncertainty, to a pre-determined standard to determine if the design is acceptable.

**Result:** Unavailability criteria have been met and risk metric has decreased by a factor greater than 3. The design is determined to be acceptable.
FOLLOWING THE EFFECTS OF DESIGN MODIFICATIONS UPON IMPORTANT RISK METRIC VALUES

<table>
<thead>
<tr>
<th>Plant Configuration</th>
<th>Median-CDF</th>
<th>5% Conf.</th>
<th>95% Conf.</th>
<th>Risk Metric*</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Depressurization</td>
<td>1.528E-06</td>
<td>3.093E-07</td>
<td>4.278E-06</td>
<td>2.216E-06</td>
</tr>
<tr>
<td>One Division of Depressurization</td>
<td>7.086E-07</td>
<td>1.226E-07</td>
<td>1.890E-06</td>
<td>1.004E-06</td>
</tr>
<tr>
<td>Two Divisions of Depressurization</td>
<td>7.055E-07</td>
<td>1.445E-07</td>
<td>1.980E-06</td>
<td>1.024E-06</td>
</tr>
<tr>
<td>Depressurization and reduced CW CC Failure**</td>
<td>4.970E-07</td>
<td>1.008E-07</td>
<td>1.432E-06</td>
<td>7.308E-07</td>
</tr>
<tr>
<td>Depressurization and reduced Diesel CC Failure</td>
<td>6.120E-07</td>
<td>1.211E-07</td>
<td>1.718E-06</td>
<td>8.885E-07</td>
</tr>
<tr>
<td>Depress with reduced CW and Diesel CC Failure</td>
<td>4.020E-07</td>
<td>7.960E-08</td>
<td>1.290E-06</td>
<td>6.24E-07</td>
</tr>
</tbody>
</table>

* Risk metric selected = (0.75 * Median CDF) + (0.25 * 95% confidence CDF)

** CW = Cooling Water; CC = Common Cause
EFFECTS OF DESIGN MODIFICATIONS ON CDF

Configuration

- Mean CDF
- 95% Confidence Level
- 5% Confidence Level
- Risk Metric
Concerns about common cause failures and large uncertainties would lead designers and regulators to conservative design approaches:

- defense-in-depth, safety margins

Guidelines are needed for consistently reflecting model weaknesses in the probabilistic database.

Consistent acceptance criteria are needed for negotiation guidance and termination.

Practical implementation requires more work:

- more trial examples
- standardized models, methods, databases
- methods for treatment of subjective judgments
- replacements for:
  - GDCs
  - DBAs (risk-dominant event sequences)
  - Standard Review Plan
SUMMARY

• The favored approach for a new design and regulatory process would:
  ■ use risk-based methods to the extent possible
  ■ use defense-in-depth when necessary to address model and data uncertainty

• A new risk-informed design and regulatory process would:
  ■ provide a rational method for both design activities and applicant-regulator negotiations
  ■ provide a method for an integrated assessment of uncertainties in design and regulation
  ■ provide a process that is applicable to non-LWR technologies

• Development of a new design and regulatory process should be continued to support new reactor license applications