



Systems Issues in Nuclear Reactor Safety

Commissioner George Apostolakis
U.S. Nuclear Regulatory Commission
CmrApostolakis@nrc.gov

MIT SDM Conference on
Systems Thinking for Contemporary Challenges
Cambridge, Massachusetts
21 October 2010

Overview

- **NRC mission**
- **Traditional regulations**
- **Probabilistic Risk Assessment**
- **Risk-informed decision making**
- **Human reliability**
- **Safety culture**

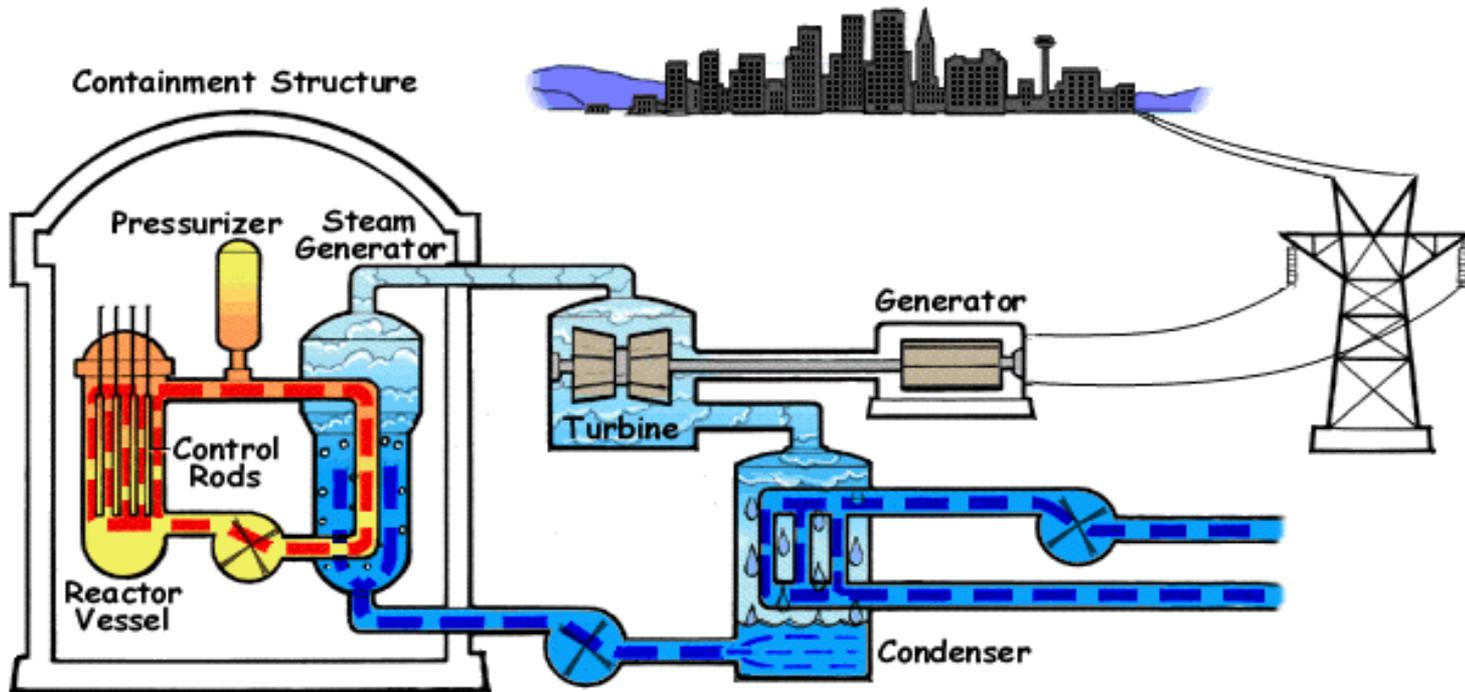
NRC Mission

- **To license and regulate the nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment.**

NRC Oversight



The Pressurized Water Reactor (PWR)



The Traditional Approach to Reactor Safety

- **Management of (unquantified at the time) uncertainty was always a concern.**
- **Defense-in-depth and safety margins became embedded in the regulations.**
- **“*Defense-in-Depth* is an element of the NRC’s safety philosophy that employs successive compensatory measures to prevent accidents or mitigate damage if a malfunction, accident, or naturally caused event occurs at a nuclear facility.” [Commission’s White Paper, February, 1999]**
- **Questions that defense in depth addresses:**
 - **What if we are wrong?**
 - **How can we protect ourselves from unknown unknowns?**
- **How much defense in depth is sufficient?**

The Single-Failure Criterion

- **“Fluid and electric systems are considered to be designed against an assumed single 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 intent is to achieve high reliability (probability of success) without quantifying it.**
- **Human errors are not considered to be single failures.**

Design Basis Accidents

- **A DBA is a postulated accident that a facility is designed and built to withstand without exceeding the offsite exposure guidelines of the NRC’s siting regulation.**
- **They are very unlikely events.**
- **They protect against “unknown unknowns.”**

Emergency Core Cooling System

- **An ECCS must be designed to withstand the following postulated Loss-of-Coolant Accident (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.**

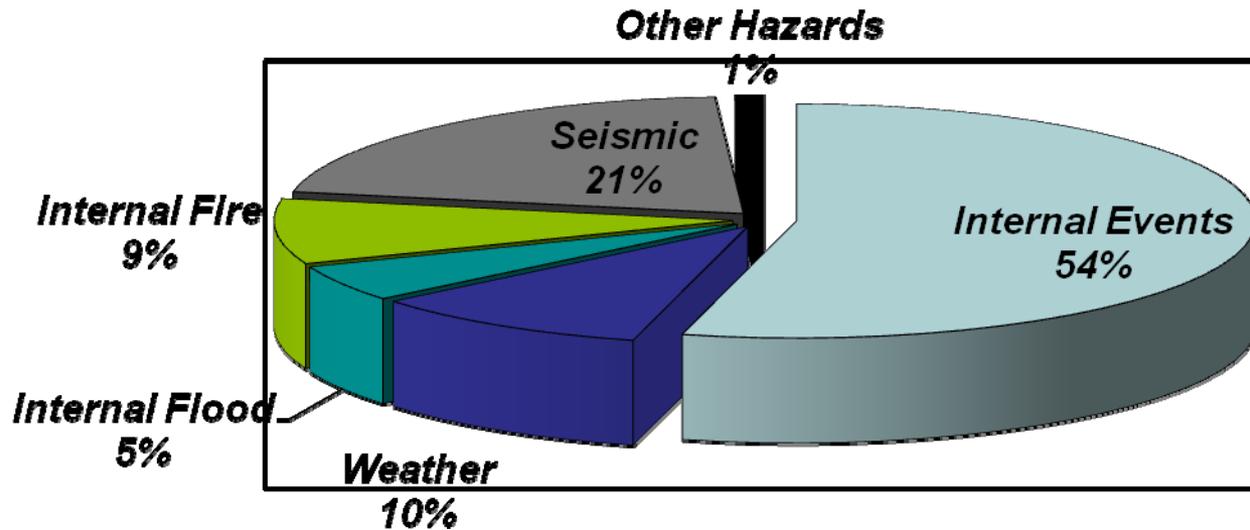
Technological Risk Assessment (Reactors)

- **Study the system as an integrated *socio-technical* system.**

Probabilistic Risk Assessment (PRA) supports Risk Management by answering the questions:

- **What can go wrong? (accident sequences or scenarios)**
- **How likely are these scenarios?**
- **What are their consequences?**
- **Which systems and components contribute the most to risk?**

Seabrook at Power PRA - Contribution of Initiators to Core Damage Frequency



CDF = 1.45E-5 / yr (mean value)



Risk Achievement Worth Ranking

Loss Of Offsite Power Initiating Event	51,940
Steam Generator Tube Rupture Initiating Event	41,200
Small Loss Of Coolant Accident Initiating Event	40,300
CONTROL ROD ASSEMBLIES FAIL TO INSERT	3,050
COMMON CAUSE FAILURE OF DIESEL GENERATORS	271
RPS BREAKERS FAIL TO OPEN	202

PRA Policy Statement (1995)

- **The use of PRA should be increased to the extent supported by the state of the art and data and in a manner that complements the defense-in-depth philosophy.**
- **PRA should be used to reduce unnecessary conservatisms associated with current regulatory requirements.**

How are decisions made?

- **Risk-informed decision making:**
 - **PRA results are one input to a subjective decision-making process that includes elements of traditional engineering approaches such as defense in depth.**

U. S. Nuclear Regulatory Commission, Regulatory Guide 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis,” Rev. 1, 2002.

- **The Analytic-Deliberative Process:**
 - *Analysis* uses rigorous, replicable methods, evaluated under the agreed protocols of an expert community - such as those of disciplines in the natural, social, or decision sciences, as well as mathematics, logic, and law - to arrive at answers to factual questions.
 - *Deliberation* is any formal or informal process for communication and collective consideration of issues.

National Research Council, *Understanding Risk*, Washington, DC, 1996.

Conflicts arise between Traditional and Risk-Informed Frameworks



Traditional “Deterministic” Approaches

- Unquantified Probabilities
- Design-Basis Accidents
 - Defense in Depth
- Can impose unnecessary regulatory burden
 - Incomplete

Risk-Informed Approach

- Combination of traditional and risk-based approaches

Risk-Based Approach

- Quantified Probabilities
 - Scenario Based
 - Realistic
 - Incomplete
- Quality is an issue

Progress over the years

- **Random hardware failures**
- **Common-cause failures**
- **Human errors (First Generation)**
- **Human errors (Second Generation)**
- **Safety culture**

Human Error Categorization (First Generation HRA)

- **Pre- and Post-Initiating Event**
- **Errors of Omission and Commission**

Pre-IE (“routine”) actions

	<u>Median</u>	<u>Error Factor</u>
Errors of commission	3×10^{-3}	3
Errors of omission	10^{-3}	5

A.D. Swain and H.E. Guttman, *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Report NUREG/CR-1278, US Nuclear Regulatory Commission, 1983.

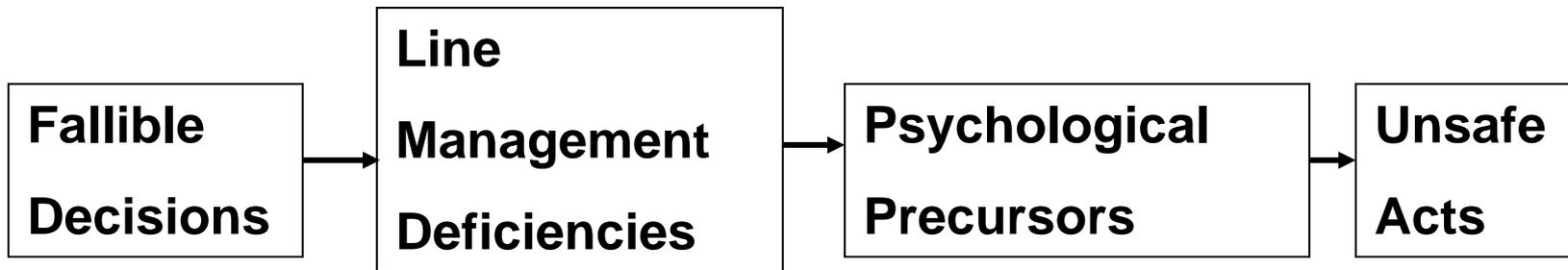
J. Rasmussen's categories of behavior

- ***Skill-based behavior:*** Performance during acts that, after a statement of intention, take place without conscious control as smooth, automated, and highly integrated patterns of behavior.
- ***Rule-based behavior:*** Performance is consciously controlled by a stored rule or procedure.
- ***Knowledge-based behavior:*** Performance during unfamiliar situations for which no rules for control are available.

Latent conditions

- **Weaknesses that exist within a system that create *contexts* for human error beyond the scope of individual psychology.**
- **They have been found to be significant contributors to incidents.**
- **Incidents are usually a combination of hardware failures and human errors (latent and active).**

Reason's model

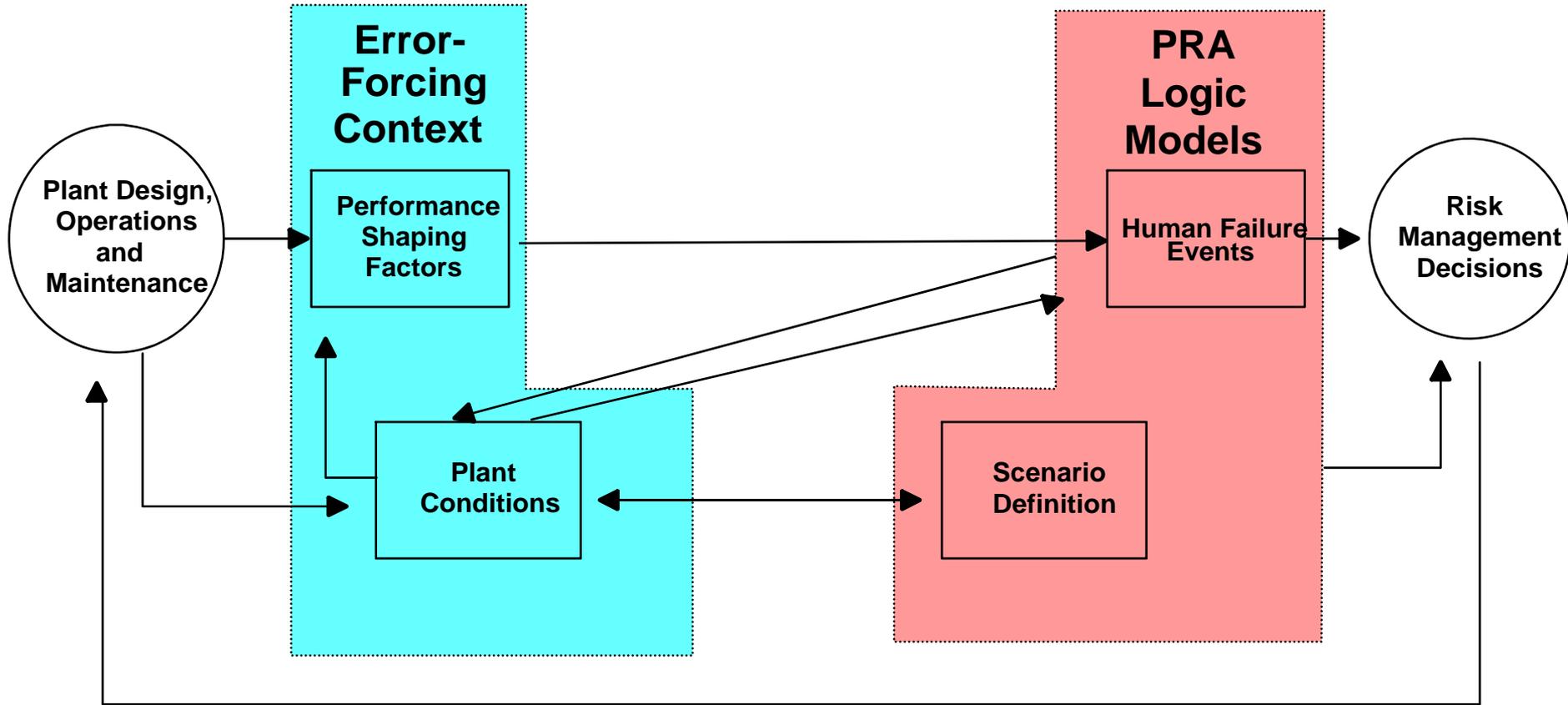


J. Reason, *Human Error*, Cambridge University Press, 1990

Post-IE errors

- **Models still being developed.**
- **Typically, they include detailed task analyses, identification of performance shaping factors (PSFs), and the subjective assessment of probabilities.**
- **PSFs: System design, facility culture, organizational factors, stress level, others.**

The ATHEANA Framework



NUREG/CR-6350, May 1996.

Draft Safety Culture Policy Statement (May 2009)

- **Draft definition of safety culture:**
 - **“That assembly of characteristics, attitudes, and behaviors in organizations and individuals which establishes that as an overriding priority, nuclear safety and security issues receive the attention warranted by their significance.”**
- **Safety and security are equally important in a positive safety culture**
- **Licensees and certificate holders are responsible for developing and maintaining a positive safety culture**

Commission Actions

- **Conduct of Operations (1989)**
 - **Control room operators were found sleeping on shift**
 - **Expectation of a positive safety culture at nuclear power plants**

- **Safety Conscious Work Environment (1996)**
 - **Environment in which employees feel free to raise safety concerns, both to their management and to the NRC, without fear of retaliation**

Roles

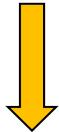
- **Licensee management has primary responsibility for establishing and maintaining a positive safety culture**
- **NRC has independent oversight role**

Important notes

- **The Reactor Oversight Process is risk informed and performance based**
- **There is no attempt to define a “good” safety culture**

Safety Culture Components (Cross Cutting Areas and Components)

Human Performance



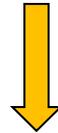
Decision-Making

Resources

Work Control

Work Practices

Problem Identification & Resolution

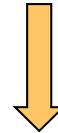


Corrective Action Program

Operating Experience

Self- and Independent Assessments

Safety Conscious Work Environment



Environment for Raising Concerns

Preventing, Detecting, & Mitigating Perceptions of Retaliation

Other Safety Culture Components

Decision Making

- **Licensee decisions demonstrate that nuclear safety is an overriding priority. Specifically (as applicable):**

H.1.a

H.1.b

H.1.c

H.1.a

- **The licensee makes safety-significant or risk-significant decisions using a systematic process, especially when faced with uncertain or unexpected plant conditions, to ensure safety is maintained. This includes formally defining the authority and roles for decisions affecting nuclear safety, communicating these roles to applicable personnel, and implementing these roles and authorities as designed and obtaining interdisciplinary input and reviews on safety-significant or risk-significant decisions.**

H.1.b

- **The licensee uses conservative assumptions in decision making and adopts a requirement to demonstrate that the proposed action is safe in order to proceed rather than a requirement to demonstrate that it is unsafe in order to disapprove the action. The licensee conducts effectiveness reviews of safety-significant decisions to verify the validity of the underlying assumptions, identify possible unintended consequences, and determine how to improve future decisions.**

H.1.c

- **The licensee communicates decisions and the basis for decisions to personnel who have a need to know the information in order to perform work safely, in a timely manner.**

Other Safety Culture Components

Accountability

Continuous
Learning
Environment

Organizational
Change
Management

Safety Policies

Accountability

- **Management defines the line of authority and responsibility for nuclear safety. Specifically (as applicable):**
 - **Accountability is maintained for important safety decisions in that the systems of rewards and sanctions is aligned with nuclear safety policies and reinforces behaviors and outcomes which reflect safety as an overriding priority.**
 - **Management Reinforces safety standards and displays behaviors that reflect safety as an overriding priority.**
 - **The workforce demonstrates a proper safety focus and reinforce safety principles among their peers.**

Continuous Learning Environment

- **The licensee ensures that a learning environment exists. Specifically (as applicable):**
 - **The licensee provides adequate training and knowledge transfer to all personnel on site to ensure technical competency.**
 - **Personnel continuously strive to improve their knowledge, skills, and safety performance through activities such as benchmarking, being receptive to feedback, and setting performance goals. The licensee effectively communicates information learned from internal and external sources about industry and plant issues.**

Safety Policies

- **Safety Policies and related training establish and reinforce that nuclear safety is an overriding priority in that:**
 - **These policies require and reinforce that individuals have the right and responsibility to raise nuclear safety issues through available means, including avenues outside their organizational chain of command and to external agencies, and obtain feedback on the resolution of such issues.**
 - **Personnel are effectively trained on these policies.**
 - **Organizational decisions and actions at all levels of the organization are consistent with the policies. Production, cost and schedule goals are developed, communicated, and implemented in a manner that reinforces the importance of nuclear safety.**
 - **Senior managers and corporate personnel periodically communicate and reinforce nuclear safety such that personnel understand that safety is of the highest priority.**
 - **Documentation and Follow-Up Actions**

Organizational Change Management

- **Management uses a systematic process for planning, coordinating, and evaluating the safety impacts of decisions related to major changes in organizational structures and functions, leadership, policies, programs, procedures, and resources. Management effectively communicates such changes to affected personnel.**

Example of Findings - Reactors

- In a 2008 regulatory inspection, it was discovered that during the replacement of a safety-related 125 VDC station battery breaker in 2004, electrical connection integrity was not adequate to ensure that the equipment would be able to perform its safety function (the condition existed for four years)
- The resources component in the *human performance area* was assessed to contribute to this performance deficiency because the licensee failed to establish adequate procedures and programs related to electrical connection integrity

Example of Findings – Nuclear Materials

- **A Medical Facility failed to report 97 medical errors out of 116 prostate cancer treatment procedures performed between 2002 and 2008**
- **Overall root cause included elements of safety culture**
 - **Inadequate management oversight**
 - **Poor decisions were not challenged and employees assumed the responsibility for a safe and adequate program belonged elsewhere**
 - **Failure to communicate concerns about the implants**
 - **Overall system did not demonstrate a commitment to safety**

2008 Commission Direction

- **Expand the Commission's policy of safety culture to address the unique aspects of security**
- **Ensure the resulting policy is applicable to all licensees and certificate holders**
- **Other issues to address:**
 - **Whether safety culture as applied to reactors needs to be strengthened**
 - **How to increase attention to safety culture in the materials area**
 - **Effective use of stakeholder involvement**
 - **One or two policy statements for safety and security?**

Next Steps

- **The NRC staff will respond to the public comments and develop the final policy statement**
- **The final policy statement will be submitted for Commission approval in March 2011**
- **Once approved, the focus will be on implementation**
 - **External – oversight programs**
 - **Internal – NRC’s own safety culture**

Open To The Public

- **The NRC places a high priority on keeping the public and stakeholders informed of its activities.**
- **At www.nrc.gov, you can:**
 - **Find public meeting dates and transcripts;**
 - **Read NRC testimony, speeches, press releases and policy decisions; and**
 - **Access the agency's Electronic Reading Room to find NRC publications and documents.**