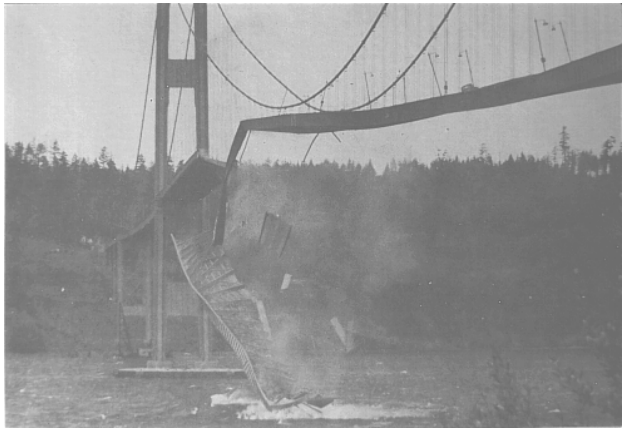
Diversity and Defense-in-Depth for Digital Systems

NRC Regulatory Information Conference
Session Th5D: Digital Instrumentation and Control
March 9, 2006

Allen G. Howe, Chief
Instrumentation and Controls Branch
Division of Engineering

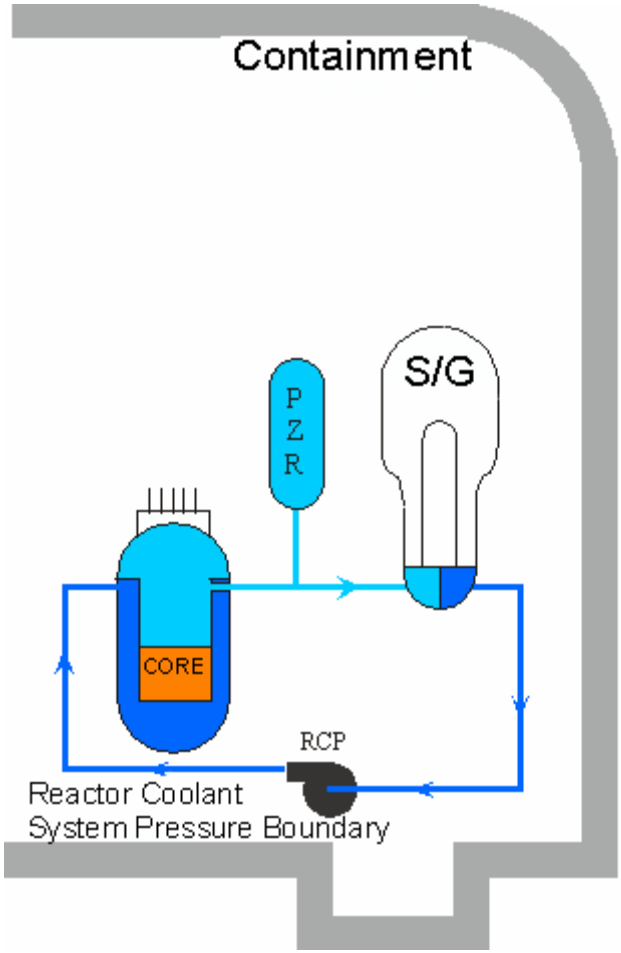
Why is diversity and defense-in-depth important?

- **Unexpected events arise that challenge safety**



- **Robust designs can meet those unexpected challenges**

What is defense-in-depth?



- **Multiple protective barriers or means, usually layered**
- **All barriers must be breached to have an adverse effect on human beings or the environment**
- **EXAMPLE: The classic three physical barriers to radiation release in a reactor:**
  - **Fuel cladding**
  - **Reactor coolant system pressure boundary**
  - **Containment**

What is diversity?

- **Diverse instrumentation systems provide several ways to detect and respond to significant events:**
  - Sense different parameters,
  - Use different technologies,
  - Use different logic or algorithms, or
  - Use different actuation means

  – Defenses at different levels of depth may also be diverse from each other

What are the concerns with digital systems?

- **Vulnerable to common-mode failures caused by software errors**
  - Defeats the redundancy achieved by hardware architecture
- **This concern applies to both new reactors and retrofits in existing reactors**
- **Complex systems with unique configurations possible**
- **Software cannot be proven to be error free**

Operating Experience

- **Digital systems at Nuclear Power Plants have caused:**
  - Reactor trips
  - Transients
  - Systems inoperable

- **Problems caused by:**
  - software design errors
  - inadequate control of modifications
  - personnel errors

U.S. Nuclear Regulatory Commission Position

- **SRM to SECY-93-087**
  - Applicants shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.

- **SRP Branch Technical Position HICB-19:**
  - Guidance for assessment of defense-in-depth and diversity.

What is the path forward?

- **Ongoing research to address digital systems**
  - Identify sets of NUREG/CR-6303 CMF coping strategies
  - Identify configuration-specific CMF vulnerabilities in currently approved COTS digital system configurations
  - Develop and validate a fault injection tool and methodology to identify diversity requirements
- **Work by the industry**
  - EPRI initiative use risk insights for defense-in-depth and diversity evaluations