EECE499-01: Computers and Nuclear Energy

Charles Kim

Fall 2011

Defense in Depth

- Military Strategy
  - Front Line
  - Forward Defense
  - Defense-in-depth
- Industrial Use
  - Computing
  - Security
  - Nuclear Power
  - Aircraft
  - etc

Defense-in-Depth as Military Strategy

- Military Defense
  - Forward Defense --- Roman army
    - Garrison posts in Barbarian territory
    - Battle Fields – out of Roman territory
    - Expensive
  - Front Line
    - Everything at the border line
    - Win or Lose
  - Defense-in-Depth
    - Thin Presence in the border line – just to delay the advance of enemy
    - Strong defense line behind
    - Modestly expensive

Defense-in-Depth in Information Assurance

- an information assurance (IA) concept
  - conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security
  - multiple layers of security defense are placed throughout an information technology (IT) system
  - provides redundancy in the event a security defense fails or a vulnerability is exploited
- Examples
  - Physical security (e.g. deadbolt locks)
  - Authentication and password security
  - Hashing passwords
  - Anti virus software
  - Firewalls (hardware or software)
  - IDS (intrusion detection systems)
  - VPN (virtual private networks)
  - Logging and auditing
  - Biometrics
  - Timed access control
  - Software/hardware not available to the public (but see also security through obscurity)

Defense-in-Depth in Safety-Critical Industry

- Fire Fighting:
  - Instead of focusing on fire prevention only;
  - It also requires the deployment of fire alarms, extinguishers, evacuation plans, mobile rescue and fire-fighting equipment and even nation-wide plans for deploying massive resources to a major blaze.
- Aircraft:
  - emphasizes redundancy - a system that keeps working when a component fails - over attempts to design components that will not fail in the first place.
  - an aircraft with four engines will be less likely to suffer total engine failure than a single-engined aircraft no matter how much effort goes into making the single engine reliable.
- Nuclear engineering and nuclear safety:
  - practice of having multiple, redundant, and independent layers of safety systems for the single, critical point of failure – reactor safety system.
  - Reactor Safety System: reduce the risk that a single failure of a critical system could cause a core meltdown or a catastrophic failure of reactor containment.

Defense-in-Depth in NPP

- Defense-in-depth is the requirement that nuclear reactors should have
  - multiple, independent barriers in place to prevent injuries to the public and damage to the environment.
  - The presence of a pressure-resistant, leak-tight containment
  - the maintenance of comprehensive emergency planning
  - mitigate the impact of a severe accident with core damage.
- The presence of multiple barriers is a hedge against uncertainty and an acknowledgement that the understanding of the performance of any one barrier is incomplete.

Defense-in-Depth in NPP and DI&C

- Safety System must reliably satisfy the functional requirements
  - Single-failure proof (no single failure is to prevent safety system actuation if needed, nor shall a single failure cause a spurious activation)
  - How to achieve this goal?
    - By Redundancy
    - Achieve the functional goals in the presence of component failures
    - Active redundancy and Standby redundancy

Redundancy

- Active Redundancy
  - Multiple identical components operating in parallel
  - The multiple outputs are compared or selected in some way to determine which outputs will be used
  - (ex) Boolean Logic; 2-out-of-3
- Standby (or backup) Redundancy
  - Make spares available to replace failed components
    - (ex)Backup generator
- Component duplication – Same function and identical component
  - Protection against independent failures caused by physical degradation (wear-out)

Common Cause Failure

- The benefit of component duplication can be defeated by common-cause or common-mode failures
  - CCF: multiple components fail by the same cause
  - CMF: multiple components fail the same way (ex) stuck open.
- CCF and CMF occur
  - because the assumption of independence of the failures of the components is invalid
  - Common external or internal influences
  - Design error

Protection against CMF - **Diversity**

- Design Diversity:
  - components with different internal design (but performing the same function) are used.
  - (ex) Multiple versions of software written from the equivalent requirements specifications – same function by different algorithms →(ex) two different ways of determining of two number are the same
  - (ex) Multiple different components differently achieving the design requirement

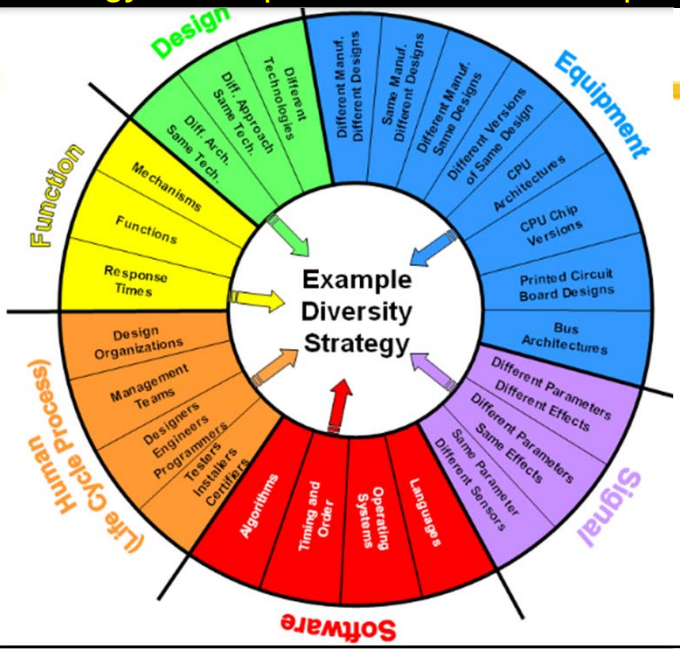
DIVERSITY

- Functional Diversity
  - Components made by **different requirements** perform **different functions at the component level** while satisfying **the upper level system requirements**
  - Different Principle of operation or physical principles to satisfy the same or different system-level requirements
  - (ex) one program checks if two numbers are equal; another program selects the larger of 2 numbers
  - (ex) One uses control rods to trip a reactor (based on the ratio of reactor power and flow); another uses Boron concentration to trip a reactor (based on coolant temperature)
- Most important issue: Independence

Diversity and Defense-in-Depth (D3) in NRC

- Diversity and Defense-in-Depth (D3) established in 1990's.
- Adding diverse systems and/or defense-in-depth features can mitigate the effect of common cause failure (CCF)
- Difference between Defense-in-Depth and Diversity

D3 Strategy development – Research Topics



D3 simulator

- U. S. Patent Application

(19) **United States**
(12) **Patent Application Publication**
Yu et al.
(10) **Pub. No.: US 2011/0060582 A1**
(43) **Pub. Date: Mar. 10, 2011**

(54) **DIVERSITY AND DEFENSE-IN-DEPTH SIMULATION APPARATUS**

(75) Inventors: **Yuan-Chang Yu**, Longtan Shiang (TW); **Mao-Sheng Tseng**, Longtan Shiang (TW); **Hui-Wen Huang**, Longtan Shiang (TW); **Tsung-Chieh Cheng**, Longtan Shiang (TW)

(73) Assignee: **ATOMIC ENERGY COUNCIL-INSTITUTE OF NUCLEAR ENERGY RESEARCH**, Taoyuan (TW)

(22) Filed: **Sep. 9, 2009**

Publication Classification

(51) **Int. Cl.**
G06G 7/54 (2006.01)
G06G 7/66 (2006.01)

(52) **U.S. Cl.** **703/18**; 700/292

(57) **ABSTRACT**

A simulator system transfers parameters between a power plant simulator and a safety control simulator. Problems concerning software common mode failure, interface interactions errors, software failure complexity, and so on, are evalu-

Guidelines in Nuclear Industry

- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," December 1994.
- NUREG-0800, Standard Review Plan, BTP 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," March 2007.
- U.S. Code of Federal Regulations, Title 10, Energy, Part 50, Section 62, "Requirements for Reduction of Risk from Anticipated Transient Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants."
- Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," April 16, 1985 (Accession No. ML031140390).
- IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,"
- NUREG/CR-6463, "Review Guidelines on Software Languages for Use in Nuclear Power Plant Safety Systems", June 1996

Guidelines in Other Industries

- FAA: RTCA (Radio Technical Commission for Aeronautics) DO-178B Software Considerations in Airborne Systems and Equipment Certification
- DOD: MIL-STD-882C System Safety Program Requirements
- FDA: Review Guidance for Computer Controlled Medical Devices Undergoing 510(k) Review

Homework #5

- Find Diversity examples in the real life and describe it and classify if it is functional diversity or design diversity, and in what sense?“
- 1-page with same format and instruction as usual
- Due: October 13

Diversity Practice

- Kit