EECE499-01: Computers and Nuclear Energy

Defense-in-Depth & Diversity (D3)

Charles Kim

Electrical and Computer Engineering

Howard University

www.MWFTR.com

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

- 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
  - Delay the advance of enemy
  - Strong defense line behind
  - Modestly expensive

Defense-in-Depth in Information Assurance

- **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 lo
  - Authentication and password sec
  - Hashing passwords
  - Anti virus software
  - Firewalls (hardware or software)
  - IDS (intrusion detection systems)
  - VPN (virtual private networks)
  - Logging and auditing
  - Biometrics
  - Timed access control
  - Exclusive Software/hardware

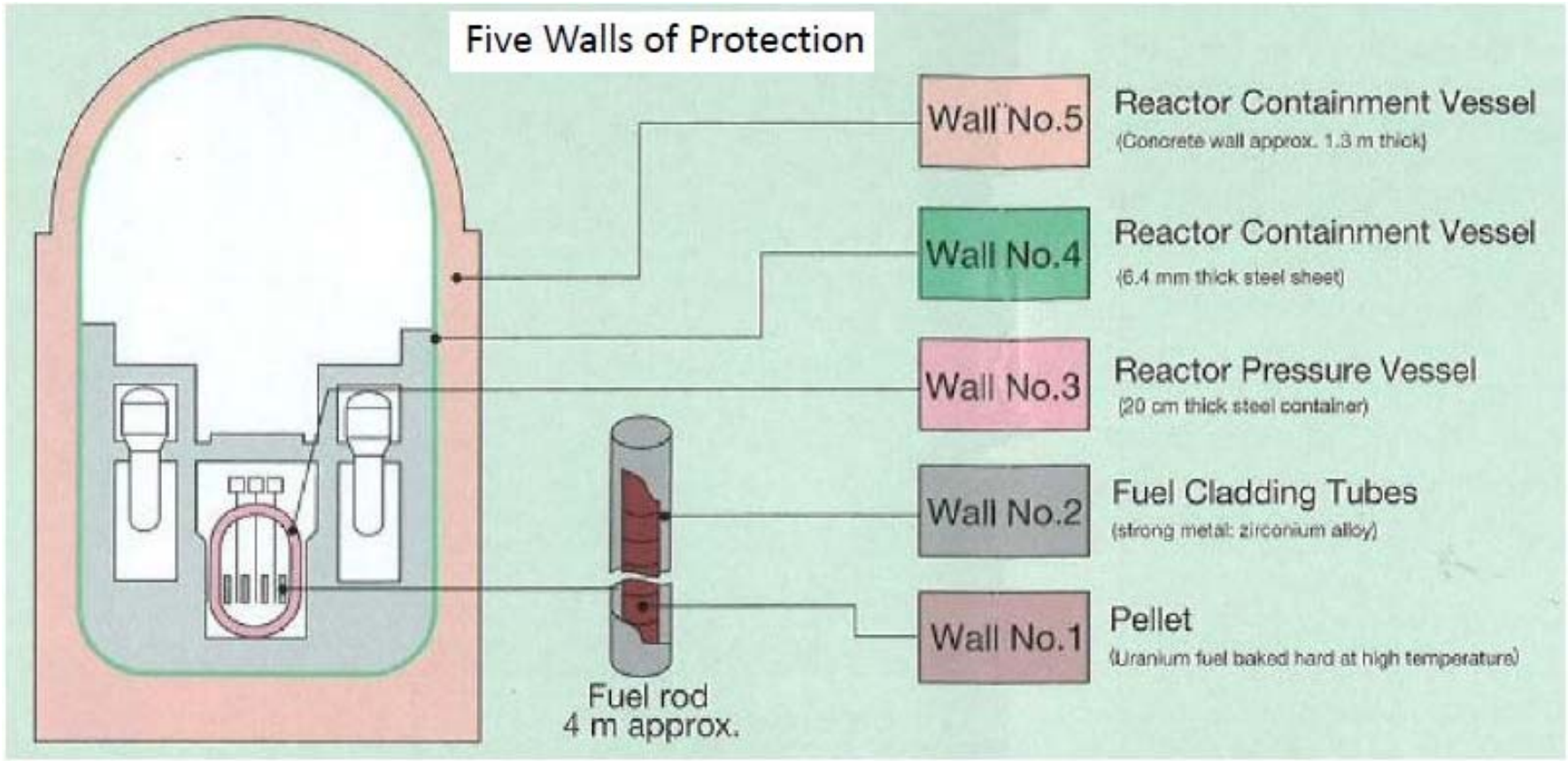
Defense-in-Depth Layers

Defense-in-Depth in Safety-Critical Industry

- 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 for Reactor Safety



Defense-in-Depth and Redundancy

- 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)

Redundancy in real life (Active? Standby?)

Problem in Redundancy

Vulnerability of Redundancy

Redundancy in the Cloud.

Common Cause Failure – Weakness of Redundancy

- 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
- 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

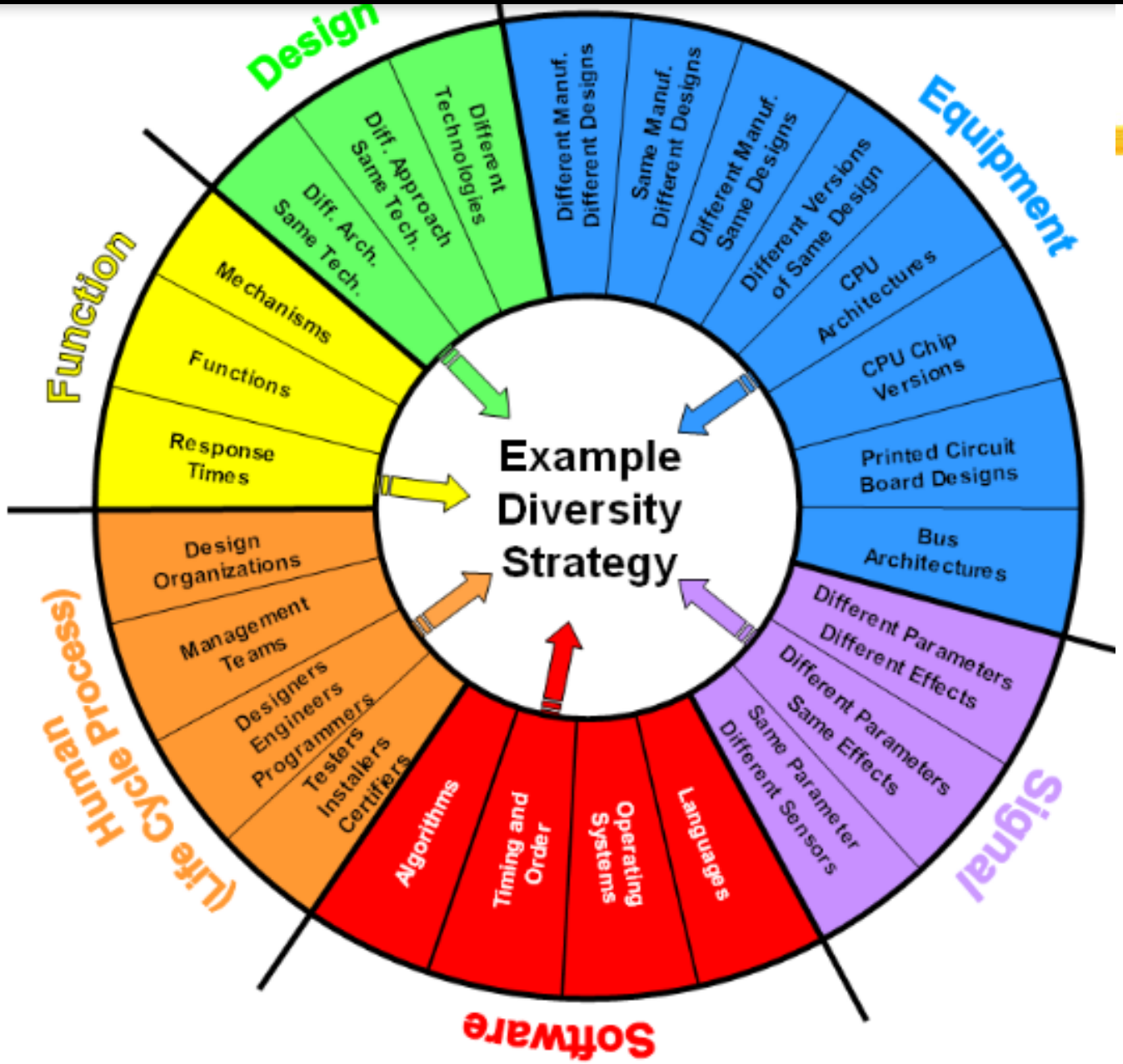
DIVERSITY

- 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 Everywhere

- GPRS: General Packet Radio Service – mobile data service on 2G and 3G Cellular Communication System

D3 Strategy development – Research Topics



D3 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

D3 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 #4

- Find Diversity Practices in the real life and describe it in a presentation form
- 1-5 slides
- Your_last_name_HW4.pptx
- Due: Nov 13, 2013 11:59pm
- Submission via email