Distributed Control Systems

GE BWR/4 Technology Course
R-504B – 4.7

Objectives

1. Recognize the major advantages and vulnerabilities of Distributed Control Systems.
2. Identify the industry strategies for coping with the following:
   a. Common Cause Failures (hardware or software)
   b. Human performance issues
   c. Cyber Security
3. Identify the four echelons of defense described in the standard review plan (BTP 7-19) for diversity and defense-in-depth (D3) evaluations of Distributed Control Systems.

Distributed (Digital) Systems

- 5 reasons the Industry is moving to digital systems:
  - Obsolescence of current systems
  - Paucity of spare parts for existing systems
  - More readily modifiable than hardware systems
  - More reliable than current system designs
  - More precise than current systems

Advantages

1. Digital signals can be transmitted with no noise degradation
2. Digital systems are readily modified by software changes
3. Information is easily stored in a digital system
4. Use of fiber optics drastically cuts wire runs to the control room
5. Instrument failures are readily detectable and can auto switch to "good" inputs

Disadvantages

1. Lost data can corrupt the systems output, without being detected.
2. Viruses can corrupt the system without the operator being aware of the change
3. Digital inputs can be changed in areas remote from the sensor or control room.
4. OE shows that new failure mechanisms are introduced with digital systems

Analog versus Digital

- Analog has continuous signal, typically as a voltage or current (output proportional to parameter being monitored).
- Digital systems convert signals to a binary or discreet signal.
- Analog signals drive analog meters and are processed by hardware (switches, bi-stables, relays, filters, etc…)
- Digital signals are manipulated by software to generate output signal.

Distributed Control Systems

- Controller elements are not central in location (like the brain) but are distributed throughout the system with each component sub-system controlled by one or more controllers.
- Custom designed processors as controllers
- Uses both proprietary interconnections and communications protocol for communication.
- The processor receives information from input modules and sends information to output modules (I/O cards).

Distributed Control Systems

- The input modules receive information from input instruments in the process (or field) and transmit instructions to the output instruments/components in the field.
- Computer buses or electrical buses connect the processor and modules through multiplexer or demultiplexers.
- Buses also connect the distributed controllers with the central controller and finally to the human-machine interface (HMI) or control consoles.

History

- To ensure failures in a non-safety system does not impact safety related systems, control systems separate from safety systems. (GDC-24). Control functions typically controlled by separate systems (RFC, RMCS, FWC, EHC, etc…)
- System design criteria differ between reactor trip systems (RTS) and emergency safety features actuation systems (ESFAS) has historically led these I&C systems to be separate and independent (RPS, NSSSS, ECCS actuation).

History

- DCS can combine RTS and ESFAS into a single system (Oconee).
- DCS can be used as a stand-alone control system (Digital Feedwater Control, Digital EHC, etc…) or can be used as an integrated control system for multiple control functions (Susquehanna).
- Implementing digital design can introduce new failure modes and common cause failures (CCFs).

History

- IEEE standards for safety related system design (IEEE 279 and IEEE 603) did not specifically address digital systems.
- IEEE std 7-4.3.2 issued for digital systems, endorsed by RG 1.152 and included in SRP (NUREG 0800).
- NRC issued Interim Staff Guidance (ISGs) on review of digital modifications
- BTP 7-19, Guidance For Evaluation of Diversity and Defense-in-depth in Digital Computer-Based Instrumentation and Control Systems (part of SRP) to address CCF.

Common Cause Failures

- Failures of equipment or systems that occur as a consequence of the same cause.
- Usually used with reference to redundant equipment or systems; or to uses of identical equipment in redundant systems.
- CCFs can occur due to design, operational, environmental, or human factor initiators.
- DCS susceptible to both hardware and software CCF as well as HU CCFs.

NRC Branch Technical Position 7-19

- Design must include Diversity and Defense-in-Depth (D3) evaluation.
- BTP provides guidance for evaluating an applicant's D3 assessment, design, and the design of manual controls and displays to ensure conformance with the NRC requirements.
- Used for I&C systems incorporating digital, software-based or software-logic-based RTS or ESF, auxiliary supporting features, and other auxiliary features as appropriate.

NRC Branch Technical Position 7-19

- Verification design diversity meets the established NRC's requirements.
- Verification of adequate defense-in-depth in a design to meet the NRC's requirements.
- Verification that displays and manual controls initiated by operators for critical safety functions are diverse from the automatic computer systems.

BTP establishes 4 Echelons of Defense against CCFs

- **The Control System** - non-safety equipment that prevents reactor excursions toward unsafe regimes of operation during normal operations.
- **The Reactor Trip System (RTS)** - safety equipment designed to reduce reactivity rapidly.
- **The Engineered Safety Features Actuation System (ESFAS)** - safety equipment that removes heat or assists in maintaining the integrity of the cladding, vessel, or containment.
- **Monitoring and Indicators** - sensors, displays, data communication systems, and manual controls for operators to respond to reactor events.

NRC Branch Technical Position 7-19

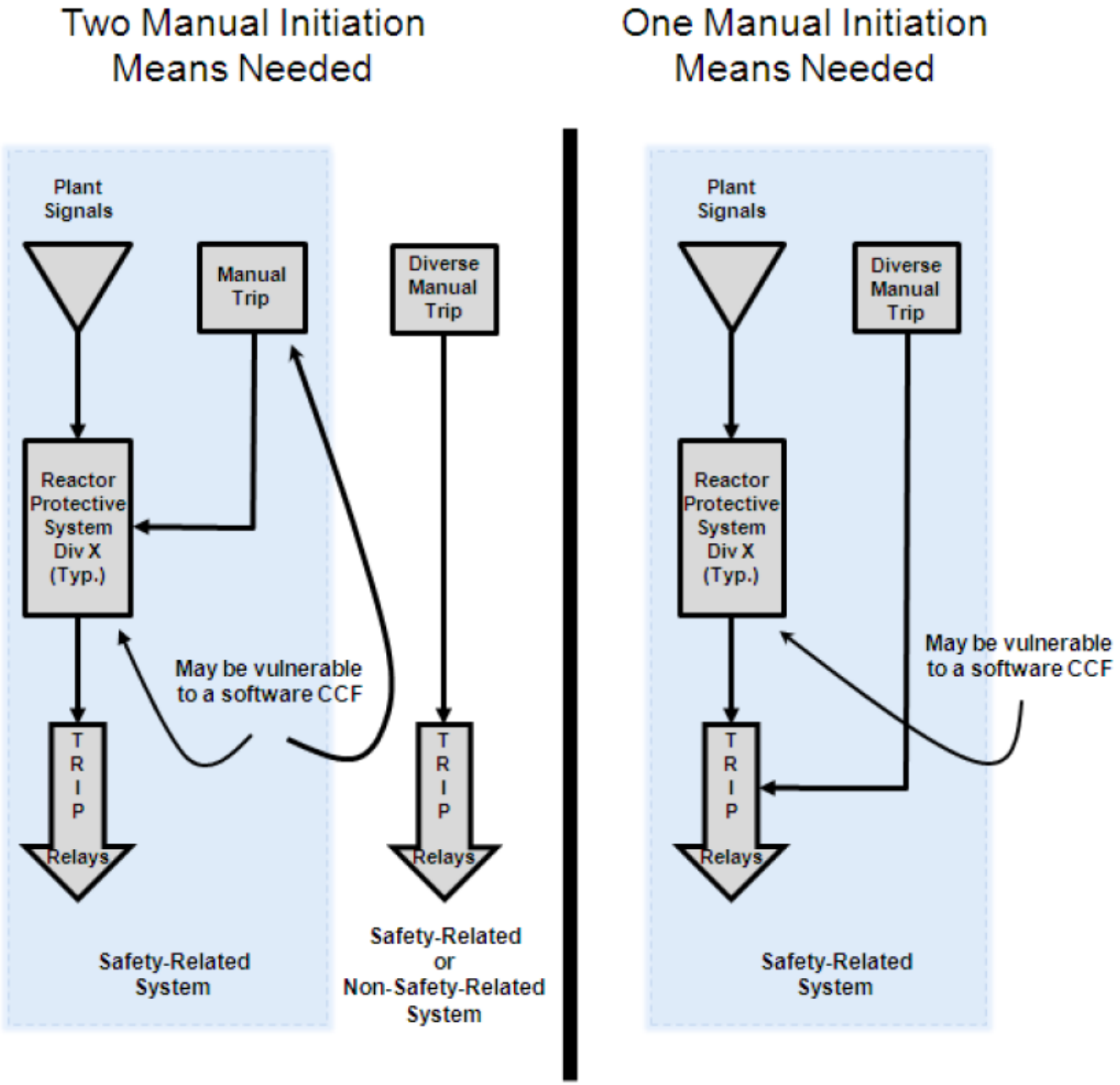
- Licensee completes a D3 evaluation as part of LAR
- Must include evaluating all credible software and hardware CCFs.
- If CCF prevents a safety function, there must be additional Diversity and/or Defense in Depth provisions added.
- **Diversity example**: design in which each safety function is implemented in two channels that use one type of digital system and another two channels that use a diverse digital system.

NRC Branch Technical Position 7-19

- DID examples:
  - Self-Testing features to detect failures
  - Watch dog timers
  - Specifications on limits on input signals and output values
  - Specifications on limits on input signals divergence
  - Error handling capabilities, system response when errors detected
  - External surveillances done by independent part of the system

NRC Branch Technical Position 7-19

- Design must include a set of displays and manual controls (safety or non-safety) in the main control room (MCR) that is diverse from any CCF vulnerability identified within the “safety computer system”
  - Retention of existing analog displays and controls in the MCR could satisfy this
  - If displays and controls serve as the diverse means, the displays and controls also should be able to function downstream of the lowest-level components subject to the CCF


Two Manual Initiation Means Needed
Plant Signals
Manual Trip
Diverse Manual Trip
Reactor Protective System Div X (Typ.)
May be vulnerable to a software CCF
T R I P
Relays
Safety-Related System
Safety-Related or Non-Safety-Related System
One Manual Initiation Means Needed
Plant Signals
Diverse Manual Trip
Reactor Protective System Div X (Typ.)
May be vulnerable to a software CCF
T R I P
Relays
Safety-Related System

Industry Strategies on CCF

- Validate the design's performance through testing or demonstration. Including a review of:
  - performance assumptions,
  - calculations,
  - extrapolations, and
  - models.
- Utility observance of critical pre-installation testing.
- Rigorous software validation and verification testing with oversight by plant personnel.
- Ensure unused software functions are isolated and will not adversely effect the operable software.

Industry Strategies on CCF

- Develop tests that verify and validate the software monitoring, control, and alarm functions in all conditions.
- Verify trip setpoint margins and key system control functions during this testing.
- Expand the scope of testing during anticipated operational modes and plant configurations to detect :
  - modification installation errors
  - unintended failure modes and effects
  - 100% testing of all input combinations

Industry Strategies on HU

- No different than with analog systems
- Two main categories of errors:
  - Human Machine Interface
  - Design and design implementation
- Human factor design: displays and controls
- Continued use of human performance error prevention tools.
  - Verification, Validation and/or peer checking
  - Self checking
  - Procedure development and use (design change process, maintenance, operation)

Cyber Security

- **10CFR 73.54 requires distributed systems to have cyber security protection for SSEPs:**
  - Safety related or important to safety functions
  - Security functions
  - Emergency preparedness functions,
    - including offsite communications
  - Support systems and equipment impacting safety, security, or emergency preparedness functions.
- **NEI 08-09 provides a template for cyber security plan to meet these requirements**

Cyber Security Plan

- Each utility develop a Cyber Security Plan
- Submit to NRC
- Incorporate into physical security plan
- Includes cyber attack assessment and mitigation
- First step is to identify Critical Digital Assets (CDAs) of which DCSs are a subset

Cyber Security Strategies

- Access Control
  - Limit physical locations to access programs
  - User IDs and passwords
  - Physical access control to HMI (MCR)
  - One-way (read only) access to data
  - Use of encryption
- Control use of removable media
- Host intrusion detection systems (HIDS)
- Virus and Malware detection systems
- Testing
- Personnel Training

Objectives

1. Recognize the major advantages and vulnerabilities of Distributed Control Systems.
2. Identify the industry strategies for coping with the following:
   a. Common Cause Failures (hardware or software)
   b. Human performance issues
   c. Cyber Security
3. Identify the four echelons of defense described in the standard review plan (BTP 7-19) for diversity and defense-in-depth (D3) evaluations of Distributed Control Systems.