# General Electric Advanced Technology Manual

# Chapter 4.7

# Distributed Control Systems

# TABLE OF CONTENTS



# LIST OF TABLES

## 4.7 DISTRIBUTED CONTROL SYSTEMS

**Learning 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.

### 4.7.1 Overview

The industry is shifting to more distributed (digital) systems for the control of safety and non-safety systems. A distributed control system (DCS) is one in which the controller elements are not in a central location, but distributed throughout the system, with each component subsystem controlled by one or more controllers. A DCS typically uses computers as controllers and uses both proprietary interconnections and protocols for communication. The entire system of controllers is connected by a network for communication and monitoring. Elements of a distributed control system may directly connect to physical equipment such as switches, pumps and valves or may work through an intermediate system such as a supervisory control and data acquisition (SCADA) system.

This movement to digital systems is being driven by multiple factors including obsolescence, reliability, and the precision of digital control systems. This makes the distributed control system failures a technical and regulatory issue for digital upgrades at operating plants and for the next generation of reactors. There is a potential for distributed system failures to disable multiple equipment trains or systems. These common cause failures (CCF) make systems that use software modifications a major design concern. As a regulator we need to ensure that plants have adequate protection against digital failures, along with adequate pre-design and post-design testing programs. As with most technologies, there are both advantages and disadvantages to digital systems some of which are discussed in the following section.

#### 4.7.1.1 Advantages

- Signals represented digitally can be transmitted without degradation due to noise. In a digital system, a more precise representation of a control or indication signal can be obtained. Digital systems do not tend to drift due to aging or temperature changes in an analog system.

- Computer-controlled digital systems can be controlled by software, allowing new functions to be added without changing hardware. This can often be done by updating the product's software, allowing the product's design errors to be corrected after the product is in a customer's hands.
- Information storage can be easier in digital systems than in analog ones. The noise-immunity of digital systems permits data to be stored and retrieved without degradation, thus allowing improved trending of data.
- Digital signal processing replaces a large volume of hard copper wiring between the field and control room with ethernet or fiber optic connections
- Instrumentation input failures can be readily detected, with automatic swapping to redundant inputs. This seamless transfer prevents transients

#### 4.7.1.2 Disadvantages

- If a single piece of digital data is lost or misinterpreted, the meaning of the related data can completely change. Because of this effect, it can be difficult for users to tell if data is valid or corrupted. Analog signal failures tend to be more obvious by failing completely in one direction or another.
- Digital systems are also susceptible to software viruses either changing the processing of a signal or the input from a digital sensor. If a virus reaches the system from either an internal or external input, it can impact control and monitoring functions, potentially without the operator being aware of the problem.
- Digital inputs or the process responses can be changed from remote locations, potentially with out the operator being aware of the change. It is also possible these changes can impact the system immediately causing a plant transient that can challenge safety systems.
- Introduces new failure mechanisms, potentially resulting in unanticipated transients or complicating the operator response to transients.

### 4.7.2 Operating Experience

Several US plants using ultrasonic flow measurement instruments have experienced actual or potential reactor overpower events. Errors in core power calculations based on data provided by the ultrasonic flow instruments resulted in extended operation above licensed power limits at both Byron Station and River Bend Station. Plant personnel, at both sites, were unfamiliar with some of the technical aspects of the new technology. This made subsequent identification and diagnoses of system problems more difficult. For one corporate-driven modification that affected several plants, training for engineering and maintenance staff was not implemented until after the modifications were installed and problems developed.

In April of 2000, at the Monticello Plant, with the reactor at 100 percent power, a technician calibrating the feedwater flow transmitters noted a small mismatch between transmitter calibration values and the corresponding values generated by the plant

process computer. The investigation determined that the span of the feedwater transmitters was changed in October of 1998, following a 6 percent power uprate. However, the process computer calibration constants for feedwater flow were not changed. These computer points are used in the reactor thermal power calorimetric calculations. The error resulted in calculated reactor power being approximately 3.7 MWt, or 0.2 percent below actual power. The net effect of this error was that actual reactor power exceeded the maximum licensed power by 0.2 percent for 316 days. The design review did not capture the change in the transmitter spans impact on the calorimetric.

In March of 2003, at the Browns Ferry Nuclear Plant, a first-of-a-kind control system was installed on Unit 2. This changed the control of the reactor recirculation flow system from a hydraulic-mechanical system to a digital control system. During post modification testing, several false ground faults occurred on the new system that tripped the reactor recirculation pumps, thereby requiring operators to scram the reactor. The Browns Ferry digital drive control system was designed without alarms and indications for all critical parameters that trip the drive system. In addition, plant personnel lacked sufficient information and understanding about the system's control functions. As this was the first modification the vendor had provided to a nuclear power plant, they did not understand the need for higher standards of system and component reliability because they had not been identified by plant engineers initiating and tracking the design change.

In June 2003, at the Shearon Harris Nuclear Power Plant, during a turbine load reduction an unexpected transient occurred due to the positioning of the main turbine governor valves. The governor valves overshot their intended position for the expected reduction in turbine load and began to reposition in the open direction. A design change was made to the digital electro -hydraulic control system without a complete failure modes and effects analysis. The vendor change did not test actual plant response or ensure the design inputs and testing methods were validated. Plant personnel did not verify the design change or its impact on plant operation. The cause was plant personnel directly involved in the review, installation, oversight and approval of the modification did not have the necessary knowledge and skills to implement it. Personnel did not understand how the new or modified equipment worked and their effect on plant operations. A secondary cause was the failure to identify potential failure modes associated with modifications, including component and system interactions. This should have been done for all potential operational modes and plant configurations. This could have helped prevent problems with the modification by identifying plant risk and better defining the scope of post-modification testing.

In June of 2005, at the Columbia Generating Station, the reactor tripped from 100% power. The trip was caused by an RPS actuation when the four turbine control valves simultaneously stroked from full open to fully closed. Nineteen minutes later, all four of the turbine control valves reopened with no operator action. During the time from the reactor trip to the turbine control valves reopening, the main turbine failed to trip as

designed. Thirty minutes following the reactor trip, plant operators manually tripped the main turbine from the front standard resulting in the re-closure of the turbine control valves. Following the event, plant personnel troubleshooting activities could not identify the cause. The three circuit cards providing the control signals to all four turbine throttle valves were replaced as they were identified as the most likely source of the system failure. The cause of this event was that the digital EHC system design had single point vulnerabilities. A significant contributing cause was the design of the system did not evaluate the impact of Balance of Plant system failures.

In November of 2007, at the Perry Nuclear Plant, the reactor automatically scrammed because of a main turbine trip initiated by an invalid high reactor water level trip signal. This invalid trip signal originated from a loss of power in the Digital Feedwater Control (DFWC) system. The loss of power occurred when the backup DFWC system power supply experienced a complete and sudden failure and the primary power supply was unable to assume system load. If the output voltages between the primary and secondary power supplies are close, they share the system load. If the output voltage values are not closely matched, the power supply with the highest voltage carries the system load. At some point, prior to the transient, the primary power supply degraded to a condition in which the voltage was within acceptable limits, but unable to carry a load greater than about 1 amp. The DFWC system did not detect the problem with the primary power supply as system alarms and power supplies did not indicate the presence of a fault. When the secondary power supply failed the primary power supply was unable to carry system load. Immediately following the failure, both reactor feedwater pumps tripped and the motor-driven did not start due to the false high level signal. The cause of the event was determined to be that plant and supplemental personnel involved in designing, reviewing, implementing, and approving the plant modifications did not fully understand how the changes affected the plant under all operating conditions. The lack of knowledge or skills on new technology adversely affected subsequent plant operation and maintenance activities.

### 4.7.3 Industry Studies and Initiatives

#### 4.7.3.1 EPRI report on Operating Experience Insights on Common-Cause Failures (CCF's) in Digital Instrumentation and Control (DI&C) Systems.

The EPRI project team reviewed over 300 OE reports of plant events involving digital I&C systems spanning a twenty year period. There were spikes in the number of events when first of a kind modifications were done such as the transfer to digital feedwater and electro-hydraulic control systems. As the number of events went down in the following years, it is apparent that one time fixes are solving these problems. The operating experience reviews examined and characterized events in terms of their causes, effects, and associated corrective actions categories.

Software did not stand out as a dominant contributor to potential and actual CCFs. More prevalent were utility process errors, such as execution of a maintenance procedure or

in calculation of setpoint values. There were also a number of events due to not validating the software under all operating conditions. Both safety and non-safety systems showed similar ratios in terms of software to non-software events.

The EPRI study recommended that the industry continue to focus on prevention of hardware failures, which are the triggering condition for an event. At the same time, industry should continue applying lessons learned from the OE to improve software and human performance.

An international study was done by the industry in 2005 that provided three key recommendations for utilities:

1. Validate performance claims of designs made by both plant and supplemental organizations through testing or demonstration. Review the performance assumptions, calculations, extrapolations, and models. Observe critical pre-installation testing.
2. Perform software validation and verification testing with oversight by plant personnel. Develop tests that verify and validate the monitoring, control, and alarm functions of software in all plant conditions. Ensure unused software functions are isolated and will not adversely interact with the operable software functions.
3. Expand the scope of testing to detect modification installation errors and unintended failure modes and effects during anticipated operational modes and plant configurations. Verify margins to trip setpoints and key system control functions during this testing.

#### 4.7.3.2 NEI 08-09

Plants are required by 10 CFR 73.54 to protect digital computers, communication, and networks of the following functions from cyber attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data and/or software.

- Safety related or important to safety functions
- Security functions
- Emergency preparedness functions, including offsite communications
- Support systems and equipment which would adversely impact the safety, security, or emergency preparedness functions.

This NEI document assists plants in the development and implementation of their cyber security plans. It includes a cyber security template, technical security controls, and management/ operational controls.

### 4.7.3.3 NRC Actions and Regulations

Table 1 includes a listing of NRC documents by title associated with Digital Control systems.

### 4.7.3.4 Evaluation of Digital Control Issues

The NRC performed a staff evaluation for a scram at the Columbia Generating Station. (LER 2009-004). Two digital instrument and control (DI&C) systems failed to perform their functions in response to a plant transient caused by a main turbine trip with a concurrent reactor scram. The trip and scram were caused by an electrical bus failure creating Generator Load Reject.

1. During the Generator Load Rejection transient, the Digital Electro-Hydraulic Control (EHC) system incorrectly determined a high reactor pressure spike was an invalid signal. The invalid signal caused the software to place the Bypass valve control into the manual operating mode, locking the Bypass valves 100% open. The operators did not recognize the system failure and this led to the reactor cooling down of 106°F in about 6 ½ minutes.

2. Following the scram, the Digital Feedwater Controls (FWC) attempted to rapidly ramp up feedwater pump turbine speed, however, the demand signal caused feedpump suction pressure to drop below its low suction pressure trip limit. This resulted in low suction pressure trips for the feedwater pumps requiring the use of safety-related systems for level control.

Both the EHC and FWC systems were modified using the 10 CFR 50.59 process. Based upon the review of this event, software design errors were introduced during these modifications. These latent software errors became self-revealing during the load reject transient. The EHC software design error contributed to an excessive cooldown rate, challenging structural components subject to embrittlement from radiation. The FWC software design error caused a complete loss of feedwater flow to the reactor vessel, which challenged safety system response to control reactor level.

The lessons learned from the event described above include;

- The modifications were fast tracked, not allowing sufficient time to perform comprehensive design reviews or testing to ensure that equipment functioned properly for all plant conditions (including transients).

- The changes used the plant simulator to test and identify design problems with the proposed modifications. The plant simulator had not been updated to allow exercising all of the features associated with modified DI&C systems behavior.

The staff study notes that the use of the simulator to support verification and validation of digital systems is a questionable practice. This operating experience provides two potential generic areas to inspect for DI&C upgrades:

- Is the plant adequately implementing the regulatory guidance for the verification and validation of systems important to safety pursuant to 10 CFR 50.59?

- Is the plant adequately maintaining the simulator in accordance with the regulatory guidance when considering its actual use in system verification and validation, or operator training?

Susquehanna Steam Electric Station had 2 separate events associated with the implementation of upgrades to a digital feedwater level control system.

- In the first scram, while placing the second reactor feedpump is service, the DFW system unexpectedly increased reactor level by 12 inches. An operator took manual control of one of the reactor feedpumps to lower level, this combined with the DFW system lowering level resulted in a low reactor water level scram.

- The second scram was caused by testing at approximately 65% power. The test tripped one of four condensate pumps. The condensate pump trip, resulted in a recirculation pump runback, as expected. This created a larger than expected steam/feed flow mismatch. The DFW control system gain settings caused level to increase approximately 30 inches per minute, resulting in a level 8 trip of reactor feed pumps and the main turbine.

The following factors created the conditions for these two scrams.

- The initial gain settings in the DFW system did not account for the system performance characteristics at low power conditions. At low power more steam is needed to change feed pump speed, therefore the FDW circuit gains must be higher.

- DFW gains were not set to handle a los of a condensate pump. When recirculation flow decreased from the runback, the reactor feedpump speed did not decrease fast enough to prevent a level 8 trip.

Three issues were documented as root causes for the scrams associated with the DFW upgrade.

1. As with the Columbia event discussed previously, the simulator was used to validate the gain settings used in the DFW system. In both of these cases, the simulator did not accurately reflect plant response to the actual conditions of the tests being performed.

2. No alternate methods were used to validate the changes against actual plant performance. Given that in both of the Susquehanna scrams, the plant did not respond as expected, based upon simulator data, alternate methods such as vendor modeling could have been used to verify gain settings.

3. The process used to do the set up of the DFW system did not adequately assess the risk associated with the various potential DFW initiated transients. This in turn led to a lack of independent oversight, the application of additional analytical techniques and personnel to verify the test program.

As a final issue, Susquehanna identified a missed opportunity to prevent the second scram, by using a causal analysis to look for other potential errors in the DFW testing process.

#### 4.7.3.5 NRC Position on Digital System Modifications

As a result of the reviews of ALWR design certification applications for designs that use digital protection systems, the NRC has established the following four-point position on D3 for ALWRs and for **digital system modifications to operating plants:**

> **Point 1-** The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate they have addressed vulnerabilities to common-cause failures.
>
> **Point 2-** In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR).
>
> **Point 3-** If a postulated common-cause failure could disable a safety function, a diverse means that is unlikely to be subject to the same common-cause failure, should be required to perform the same function. The diverse function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
>
> **Point 4-** Displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems identified in Points 1 and 3.

The above position is based on the NRC's concern that software design errors are a credible source of common-cause failures. As software cannot typically be proven to be error-free, it is therefore considered to be a source of potential common-cause failures. If identical copies of the software are present in redundant channels of safety-related systems, the potential exists for common cause failures to be present in the system.

When digital system modifications are made to operating plants, retention of existing displays and controls in the main control room may satisfy Point 4. To defend against potential common-cause failures, it necessary to have high quality system designs, including the use of defensive design measures to avoid or tolerate faults and cope with unanticipated conditions. High-quality software and hardware reduce failure probability however, despite this and the use of defensive design measures, software errors may still defeat safety functions in redundant, safety-related channels.

NRC Branch Technical Position 7-19 provides guidance for evaluating a plant's assessment and design for manual controls and displays to ensure their conformance with the NRC position on I&C systems incorporating digital computer-based reactor trip systems (RTS) or engineered safety features actuation systems (ESFAS). The objective is to confirm that vulnerabilities to common-cause failures have been addressed in accordance with the guidance of the staff requirements memorandum (SRM) on SECY-93-087, specifically to:

- Verify that adequate diversity has been provided in a design to meet the criteria established by the NRC's requirements.
- Verify that adequate defense-in-depth has been provided in a design to meet the criteria established by the NRC's requirements.
- Verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the protection systems.

NUREG/CR-6303 documents the defense in depth and diversity (D3) analysis methods used in advanced light water reactor (ALWR) design certification **and for operating plant retrofits.** This document describes an acceptable method for performing assessments. **When the reactor trip system (RTS) or anticipated transient without scram (ATWS) mitigation system in an operating plant is modified, the requirements of the ATWS rule, 10 CFR 50.62, must be met.** 10 CFR 50.62 requires that the ATWS mitigation system be composed of equipment that is diverse from the RTS. If the difference in the manufacturer cannot be demonstrated, a case-by-case assessment of the mitigation system designs should be conducted. This analysis should include differences such as manufacturing division (within a corporate entity), software (including implementation language), equipment (including central processing unit architecture), function, people (design and verification/validation team), and initiating events.

The Staff has identified four echelons of defense against common-cause failures:

1. Control System - The control system echelon consists of non-safety equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is used in the normal operation of the reactor.
2. Reactor Trip System - The RTS echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

3. Engineered Safety Features Actuation System - The ESFAS echelon consists of safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).
4. Monitoring and Indicators - The monitoring and indicators echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

### 4.7.4 Summary

Distributed systems will continue to be integrated into current plants and are the cornerstone of the ALWR designs. Digital systems provide a different set of challenges for the regulator in ensuring that they are properly designed and tested so they do not add common cause failures or be subjected to cyber security threats. Use of plant specific simulators as a test platform is only as effective as the ability of the simulator to exactly mimic the plants physical characteristics.

**Table 1 NRC References**

| | |
|---|---|
| NRC Branch Technical Position 7-19 | Verifies diversity, defense in depth, and manual controls for critical operator actions |
| 10 CFR 73.54 | Each licensee will submit a cyber security plan for Commission review and approval. |
| NUREG/CR-6303 | Defense in depth and diversity in ALWR designs, including the ATWS rule requirements in 10CFR 50.62 |
| NUREG 0493 | Defense in depth and diversity in integrated Protection systems |
| 10 CFR 50.55a(h), | "Protection and Safety Systems," |
| 10 CFR 50.62, | "Requirements for Reduction of Risk from Anticipated Transients without Scram |
| 10 CFR Part 50, | Appendix A, General Design Criterion (GDC) 21, "Protection Systems Reliability and Testability," |
| GDC 22, | "Protection System Independence," |
| GDC 24, | "Separation of Protection and Control Systems," |
| GDC 29, | "Protection Against Anticipated Operational Occurrences," |
| Regulatory Guide 1.53, | "Application of the Single-Failure Criterion to Safety Systems," clarifies the application of the single-failure criterion (GDC 21) |
| NUREG/CR-6303, | "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," |
| DI&C-ISG-02 interim staff guidance | This guidance says that there is no distinction in the reactor protection systems D3 criteria between the existing and new plants. |
| DI&C-ISG-05 interim staff guidance | Provides clarification on crediting manual operator actions on diversity and defense in depth (D3) issues. |
| NRC IN 96-56, | "Problems Associated with Testing, Tuning, or Resetting of Digital Control Systems While at Power". |
| IN 2010-10, | "Implementation of a Digital Control System under 10 CFR 50.59". |
| Regulatory Guide 5.71. | "Cyber Security Programs For Nuclear facilities". |