5.5 EXAMPLE 4 - REPLACEMENT OF REDUNDANT CONTROL SYSTEMS

PURPOSE AND SUMMARY

The purpose of this example is to illustrate the replacement of analog control systems on redundant safety-related SSCs with digital control systems that contain the same software and CCF is a concern. No HSI modifications are involved.

The Screen conclusion was *adverse* due to the digital-related impacts.

In the Evaluation, a hardware-related CCF conclusion of *unlikely* and a software-related CCF conclusion of *unlikely* were used from the technical support work. The Evaluation concluded that a License Amendment Request for the digital-related impacts was NOT required.

SCREEN

Title:

Replacement of Chiller Analog Control Systems with Digital Control Systems

Proposed Activity Description:

1. The proposed activity will replace the two existing main control room (MCR) Train A and B chillers analog control systems (one per train) with two commercial off-the-shelf digital control systems (one per train).

2. The proposed activity involves the combination of existing electrical and mechanical components (i.e., controllers, bistables, timers, etc.) and functions (i.e., relay logic, equipment protective trips, alarms, etc.) within each division, but the separation and independence of each division is maintained.

[*Author's Note: To illustrate how activities other than those directly related to the harware, software or HSI aspects can accompany a digital modification, all of the activities identified in #3 below are also part of the overall modification. However, these activities are not unique to "digital" since all of these additional activities could have been implemented with a non-digital modification. None of these activities will be addressed in this example, which focuses only on the strictly digital aspects of the modification. In an actual Screen, all of these additional actvities would need to be addressed.*]

3. Several functional performance and sequence of operation changes for the MCR chillers will be made to increase the reliability of the new chillers. These changes include:

(a) The existing system requires manually resetting the controls to energize the high temperature trip relay when electrical power is lost for greater than 60 seconds. With the new system, this manual action is no longer required.

(b) The existing control logic could allow the chiller to start without chilled water flow being present, potentially freezing the chiller, if the chilled water pump shaft was decoupled from its motor. The new control system's start logic will not allow the chiller to start or run when chilled water flow is not present.

(c) The exisiting controller starts the compressor immediately when needed. The new controller will postpone starting the compressor for a 15 second time period while it monitors the power supply to determine that the power supply is stable.

(d) The new control system contains a new feature that will allow the chiller to operate in a limited condition when certain process values enter off-normal conditions.

(e) The new control system contains a new feature that calculates the anticycle time based on how long the chiller was running prior to stopping and how long the chiller has been stopped.

Design Function Identification:

Design Functions for Activity #1:

The UFSAR states that plant locations containing safety-related equipment that need a controlled environment to perform required accident mitigation operations are served by fully redundant environmental control systems.

The UFSAR describes the MCR air conditioning system as consisting of two 100% capacity units, with each unit meeting the single failure criterion, comprised of two 100% capacity package water chillers, two 100% capacity fan-coil type air handling units, and associated pumps, piping, ductwork, and controls.

Design Functions for Activity #2:

The UFSAR states that the MCR air conditioning system is designed "to maintain temperature and humidity conditions throughout the building for the protection, operation, and maintenance and testing of plant controls, and for the safe, uninterrupted occupancy of the main control room (MCR) habitability system (MCRHS) area during an accident and the subsequent recovery period" and the MCR air conditioning system consists of "two 100% capacity units. Each meets the single failure criterion...."

Screen Responses:

1. Does the proposed activity involve a modification, addition to, or removal of a SSC such that the design function of the SSC, as described in the UFSAR, is adversely affected?

YES.

Combination of Components/Functions Assessment

For activity #1, since identical software will be used in each digital control system, there is an ***adverse*** impact on the independence of the chillers described in the UFSAR.

For activity #2, combining components and functions is *not adverse* because the consolidation is implemented only within each independent division; thereby continuing to meet single failure criteria as described in the UFSAR and not creating any new failure mechanisms.

Dependability Assessment

Since the digital control system performs the exact same functions as the analog control system, a direct correlation can be made by comparing the dependability of each control system.

A commercial grade dedication (CGD) of the digital equipment was performed. The CGD demonstrated the digital equipment was equivalent to equipment developed under a 10 CFR 50, Appendix B QA program using a documented life-cycle process.

Based on the qualification activities and critical digital review documented in the CGD report, including software verification and validation, applicable operating history survey, the digital equipment is considered a highly reliable system on a level equal to, or exceeding, the analog equipment.

There is *no adverse* impact on a design function due to a reduction in the reliability of performing a design function.

2. Does the proposed activity involve a change to a procedure that adversely affects how UFSAR described SSC design functions are performed or controlled?

NO.

No portion of the proposed activity involves how individuals interact with the new digital devices or the information presented by the new devices. The same information will be available with the new devices and the information will be used in the same manner. Since no HSI aspects are included in this change, *no adverse* impacts are possible.

EVALUATION

Criterion 2: Does the proposed activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety previously evaluated in the UFSAR?

NO.

Level of Detail

The control systems for the MCR chillers are not explicitly described in the UFSAR, but are part of the chiller system. Therefore, the chiller system will be the appropriate level for which impacts on malfunction likelihood will be addressed.

As described in the UFSAR, two malfunctions of the MCR chillers are described: (1) failing to start, and (2) stops, both of which are caused by mechanical or electrical failures.

The initiators of the existing credible malfunctions identified in the UFSAR for each MCR chiller are:

1. Electrical Failures

2. Mechanical Failures.

Hazard Analysis

The FMEA did not identify any single failure modes of the digital control system that would result in loss of safety function of the associated air-conditioning system.

CCF Considerations - Hardware

The environment in which the digital control system will operate (EMI/RFI susceptibility, seismic, temperature, humidity, and radiological) has been evaluated, further reducing the vulnerability of a CCF due to environmental factors.

A third-party dedicator evaluated the hardware design development process used by the commercial vendor and reviewed the digital control system for potential hazards and failure modes with regard to hardware. The review process, results, and conclusions are contained in the Critical Digital Review (CDR) and FMEA. The evaluation in the CDR also included an operating history review of control system users with similar applications that the users viewed as operationally critical to their plants' performance.

Based on this assessment, it can be concluded that a hardware-related CCF is *unlikely*.

CCF Considerations - Software

A third-party dedicator evaluated the software development process used by the commercial vendor, performed software code reviews, performed verification and validation (V&V) activities to verify all control systems requirements in a similar configuration to the existing plant's installation, and reviewed the digital control system for potential hazards and failure modes with regard to software.

The review process, results, and conclusions are contained in the CDR, Software Requirements Specification (SRS), Software Design Document (SDD), Software Verification and Validation Report (SVVR), Hazards Analysis, and FMEA. The third-party dedicator concluded that the likelihood of software failure is low enough to be considered acceptable. Successful Factory Acceptance Testing operated the chiller package utilizing MCR chiller specific firmware and software which further supports the conclusions reached by the third party dedicator.

100% of the digital control system's software was reviewed and evaluated. In each instance, the code was compliant or the deviation did not warrant a

modification to the code and was not classified as an issue. All identified issues were resolved.

Extensive validation testing, developed from the code review and based upon the documented SRS, was performed by utilizing a test bed with hardware, base software, and specific application configuration settings. The validation testing demonstrated that the digital control system (hardware and software) performed as specified in the SRS under normal and abnormal conditions.

The CCF Susceptibility Analysis determined that most sources of CCF were unlikely, with the exception of a CCF due to a single design defect, for which sufficient preventive measures for the controller operating system could not be fully demonstrated. However, other limiting and mitigative measures are in place to drive the likelihood of CCF from a design defect much lower than those failures already considered in the licensing basis.

Based on this assessment, it is concluded that a software-related CCF is *unlikely*.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Therefore, without a credible new malfunction initiator due to the hardware, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a hardware-related CCF.

The determination that a software-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Without a credible new malfunction initiator due to the software, a malfunction due to a software CCF is not credible. Therefore, there is not more than a minimal increase in the likelihood of a malfunction of an SSC important to safety previously evaluated in the UFSAR due to a software-related CCF.

Criterion 5: Does the proposed activity create a possibility for an accident of a different type than previously evaluated in the UFSAR?

NO.

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Without a credible new accident initiator, a new accident cannot be created due to a

hardware-related CCF. Therefore, since a new accident cannot be created, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a hardware-related CCF.

The determination that a software-related CCF is *unlikely* is equivalent to a licensing condition of an accident initiator that is NOT credible. Furthermore, a MCR chiller is a support system utilized in the mitigation of accidents and is not an initiator of any accident analyzed in the UFSAR and the proposed activity does not create a credible scenario in which the MCR chiller system could become an accident initiator.

Therefore, without a credible scenario in which the new accident initiator would apply, it is not possible to create an accident of a different type than previously evaluated in the USFAR due to a software-related CCF.

Criterion 6: Does the proposed activity create a possibility for a malfunction of an SSC important to safety with a different result than any previously evaluated in the UFSAR?

NO.

Level of Detail

Same level as determined in the response to Criterion #2.

CCF Considerations - Hardware

Based on the assessment outlined in the response to Criterion #2, it was concluded that a hardware-related CCF was *unlikely*.

CCF Considerations - Software

Based on the assessment outlined in the response to Criterion #2, it was concluded that a software-related CCF was *unlikely*.

Result

The UFSAR states that the failure of only one of the redundant chillers is possible and that the standby chiller will start.

Justifications and Conclusions

The determination that a hardware-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a hardware-related CCF is not credible, no results different from those previously evaluated in the UFSAR are possible.

The determination that a software-related CCF is *unlikely* is equivalent to a licensing condition of a CCF malfunction that is NOT credible. Since a malfunction due to a software-related CCF is not credible, no results different from those previously evaluated in the UFSAR are possible.