EPRI 3002005326

Worked Example 4: Chiller Controls

Note: Tables A-33 and A-34, which are heavily referenced in this example, are attached at the end of the write-up, along with their introductory material. The hyperlinks in this excerpt are not active.

H.1 Scope

This example describes an analog-to-digital upgrade of redundant commercial grade chiller controls used in a safety-related main control room (MCR) HVAC system.

H.2 Failures and Conditions Considered in Existing Analyses

The safety analysis considers a single random hardware failure within either MCR HVAC train concurrent with a Postulated Accident, and credits the redundant HVAC train for providing HVAC functions necessary to achieve and maintain safe shutdown of the unit. HVAC functions assumed or credited in the safety analysis include:

- Heating or cooling necessary for maintaining operability of safe shutdown equipment in the MCR envelope (i.e., keep the temperature within specified limits)
- Ventilation to maintain MCR habitability, including isolation, recirculation and filtering of radioactive materials

The PRA considers the need for control room HVAC, but does not explicitly model it. Loss of control room HVAC would be readily noticeable by the operators. If attempts to restore HVAC were unsuccessful, then prestaged portable ventilation would be aligned to establish alternate ventilation. Radiological conditions outside the control room would not be expected to exist and even if they did the operators would don face masks for protection as opposed to abandoning the control room.

H.3 Concept

Figure H-1 illustrates the proposed conceptual design. The upgraded chillers in each division are identical, and each is supplied with a digital controller that provides:

- Control of a variable speed drive on a centrifugal compressor
- Control of chiller auxiliaries (e.g., oil pump, water pumps, etc.)
- Monitoring and local display of controller inputs and outputs
- Menu display for changing chiller operating modes
- Menu display for changing chiller parameter values
- Dry contact output for a chiller trouble alarm

- Data communications (Ethernet and Serial) for remote indication and control

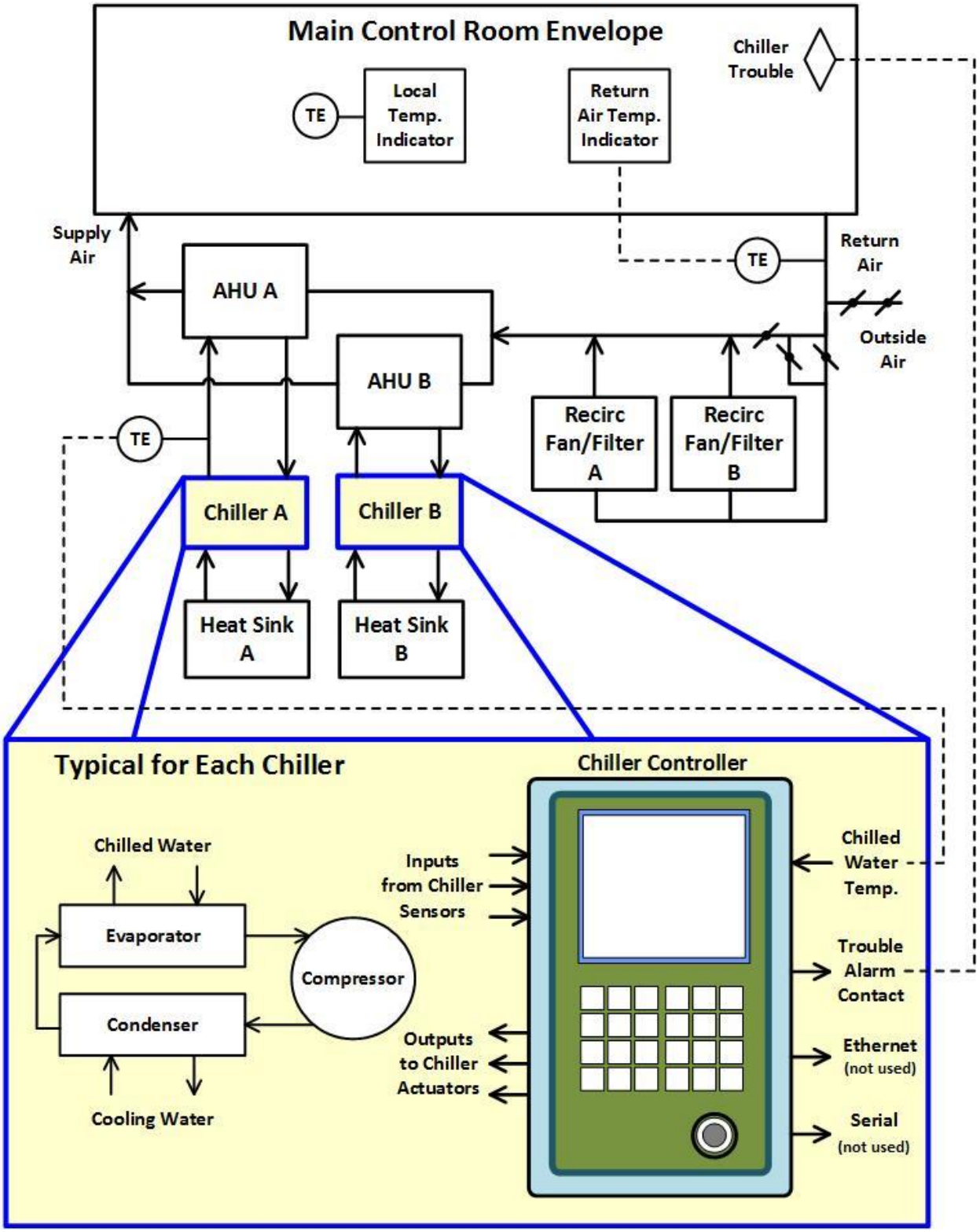

Figure H-1
Chiller Conceptual Design

Each digital controller utilizes a real-time operating system that supports multi-tasking and interrupts. Each controller is provided with a watchdog timer that will shut it down in the event of a scan overrun. The controllers in each chiller each division are configured identically, and they are qualified and commercial grade dedicated (CGD) by a third party. In addition, the operating history shows an accumulated total of over 5000 unit-years spread over 10 years, using the same hardware and OS versions in continuous operation, with no software errors.

Each chiller supplies chilled water at a controlled setpoint of 45°F to an associated air handling unit (AHU) that provides conditioned supply air to the MCR. MCR air is returned to each AHU, where heat is removed by a heat exchanger that is cooled by the chilled water, which is then returned to the chiller evaporator in a closed loop. The chiller uses a closed refrigerant loop to transfer heat to a cooling water system via a condenser, and each cooling water system has its own, dedicated heat sink.

The main control room envelope can be supplied with a combination of outside air and return air, and the indications and controls for the air handling units (AHU), recirculation fans & filters, and dampers are independent from the chiller controls. In addition, independent indications of MCR room temperature and return air temperature are provided in the MCR.

H.4 CCF Susceptibility Analysis

A CCF susceptibility analysis performed for the conceptual design is provided in this section.

H.4.1 CCF Susceptibility Caused by a Random Hardware Failure in a Shared Resource

Each chiller is independent of the other, and there are no shared I&C, electrical or mechanical resources between divisions in the conceptual design.

Therefore, the likelihood of a CCF of the setpoint adjusters caused by a failure in a shared resource is considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis).

H.4.2 CCF Susceptibility Caused by an Environmental Disturbance

High Temperature or Humidity

The chillers are located in separate areas of the plant, and each area is supplied with its own independent HVAC. In the event of a single HVAC failure, one chiller may be affected, but the other chiller will remain unaffected, thus meeting A23-P2.

Therefore, the likelihood of a CCF of the chiller controls caused by high temperature or humidity is considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis).

Electro-Magnetic Interference (EMI)

The conceptual design does not describe any measures related to EMI. However, the design specification for the project will require the equipment to be qualified to the design basis EMI conditions without failure, thus meeting preventive measure A25-P1.

Therefore, the likelihood of a CCF of the chiller controls caused by EMI is considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis).

Seismic Event

The conceptual design does not describe any measures related to seismic events. However, the design specification for the project will require the equipment to be qualified to design basis earthquake conditions without failure, thus meeting A27-P1.

Therefore, the likelihood of a CCF of the chiller controls caused by a seismic event is considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis).

Radiation

The chillers are located in separate areas of the auxiliary building, which may experience some radiation dose before and during a Postulated Accident (PA). Therefore, the design specification will require qualification without failure up to an including the design basis accumulated radiation dose, thus meeting A29-P2.

Therefore, the likelihood of a CCF of the chiller controls caused by radiation is considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis).

Fire or Smoke

The chillers are located in separate fire zones. The design meets A31-P2 such that a fire within one zone will not affect more than one chiller.

Therefore, the likelihood of a CCF of the chiller controls caused by fire or smoke is considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis).

H.4.3 CCF Susceptibility Caused by a Design Defect

Operating System Design Defect

The conceptual design describes the use of a real-time, multitasking operating system that is used within each digital controller to acquire input signals, calculate responses (via application files), and provide output signals to chiller actuators (e.g., the variable speed drive on the compressor). As such, they do not completely meet any of the preventive measures (A33-P1, P2, P3 or P4) listed in Table A-33:

- Although some of the provisions of A33-P1 are met by the proposed operating system, A33-P1 also includes provisions for different quantities and configurations of I/O, different cycle times, and different CPU loads between controllers, and since the chiller controllers are configured identically, A33-P1 is not fully met. Therefore, the provisions of A33-P1 intended for reducing the likelihood of a CCF caused by a design defect to Level 2 are not met.
- A33-P2 refers in part to A33-P1, and since A33-P1 is not fully met, neither is A33-P2. Therefore, the provisions of A33-P2 intended for reducing the likelihood of a CCF caused by a design defect to Level 2 are not met.

- A33-P3 includes a provision for "…no external inputs or data communications that are active at the time the SSC must be in its required position…" to provide assurance that there are no potential defect triggers that could erroneous position the SSC away from its required position. The proposed design does not indicate if data communications will be used or not, but it does show that external inputs from chiller sensors and the return air temperature sensor are active, as would be expected for close-loop continuous control. Therefore, the provisions of A33-P3 intended for reducing the likelihood of a CCF caused by a design defect to Level 2 are not met.
- A33-P4 provides a different operating system for each controller so that a design defect in one controller effects only one SSC. In this case, the chiller controllers are identical. Therefore, the provisions of A33-P4 intended for reducing the likelihood of a CCF caused by a design defect to Level 2 are not met.

In addition, none of the limiting measures for an operating system defect listed in (A34-L1, L2, L3, L4 and L5) are fully met either:

- A34-L1 has provisions for ensuring low likelihood of a defect through documented software quality and a simple operating system (e.g., single tasking), and ensuring an activated defect forces the affected controller(s) to a predictable shutdown state. The commercial grade dedication for the digital controllers provides evidence that the OS is equivalent in quality to one that is developed under a nuclear QA program, but it is not a single tasking OS, and the only measure described in the conceptual design for forcing a controlled shutdown is a watchdog timer (in the event of a scan overrun). A34-L1 also includes provisions for buffer overflow and exception handling protection which are not indicated in the conceptual design.
- A34-L2 refers to A34-L1, but allows for the use of operating history in lieu of documented software quality to demonstrate low likelihood of an OS defect. But A34-L1 is not fully met, so neither is A34-L2.
- A34-L3 and A34-L4 refer to operating system preventive measures A33-P1 and A33-P2 respectively, while allowing for a limited number of SSCs that share a controller. It is true that a limited number of active components are connected to each chiller controller within each division, but the proposed design does not meet A33-P1 or A33-P2, as described above, so A34-L3 and A34-L4 are not met.
- A34-L5 provides the same measures as A33-P4, except that each controller controls multiple SSCs. In this case, A33-P4 is not met, so neither is A34-L5.

The likelihood of a CCF of both chillers caused by a design defect in the chiller controls is not considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis). However, the commercial grade dedication of the chiller controls indicate the operating system quality is equivalent to that produced by a nuclear quality program, and a failure of a chiller controller in one division does not influence the chiller in the other division because they are physically and electrically independent. In addition, the proposed design makes no use of data communications while the chillers are in service.

Therefore, the likelihood of a CCF of both chillers caused by a design defect in the chiller controls is considered to be Level 1 (less likely than CCFs considered in the traditional conservative safety analysis, but still possible).

H.4.4 CCF Susceptibility Caused by a Human Error

Human Error

The proposed design does not describe any measures related to preventing a CCF caused by a human error. However, the design specification will require the HSI to be developed, verified and validated in accordance with the plant HFE program that meets NUREG 0700 and NUREG-0711. In addition, the plant already has in place the administrative controls for meeting A45-P1.

Therefore, the likelihood of a CCF of the chiller controls caused by a human error is considered to be Level 2 (as unlikely as CCFs not considered in the traditional conservative safety analysis).

H.4.5 CCF Susceptibility Caused by Other Sources

An evaluation of the proposed design shows that no other sources of CCF are identified. However, the design specification will require disclosure of any other potential CCF sources that may be identified by the equipment vendor.

H.5 CCF Coping Analysis

The CCF coping analysis evaluates each CCF, by source and likelihood, as identified in the CCF susceptibility analysis above and illustrated below in Figure H-2:

SSC connected to each controller in the Type 2 design.

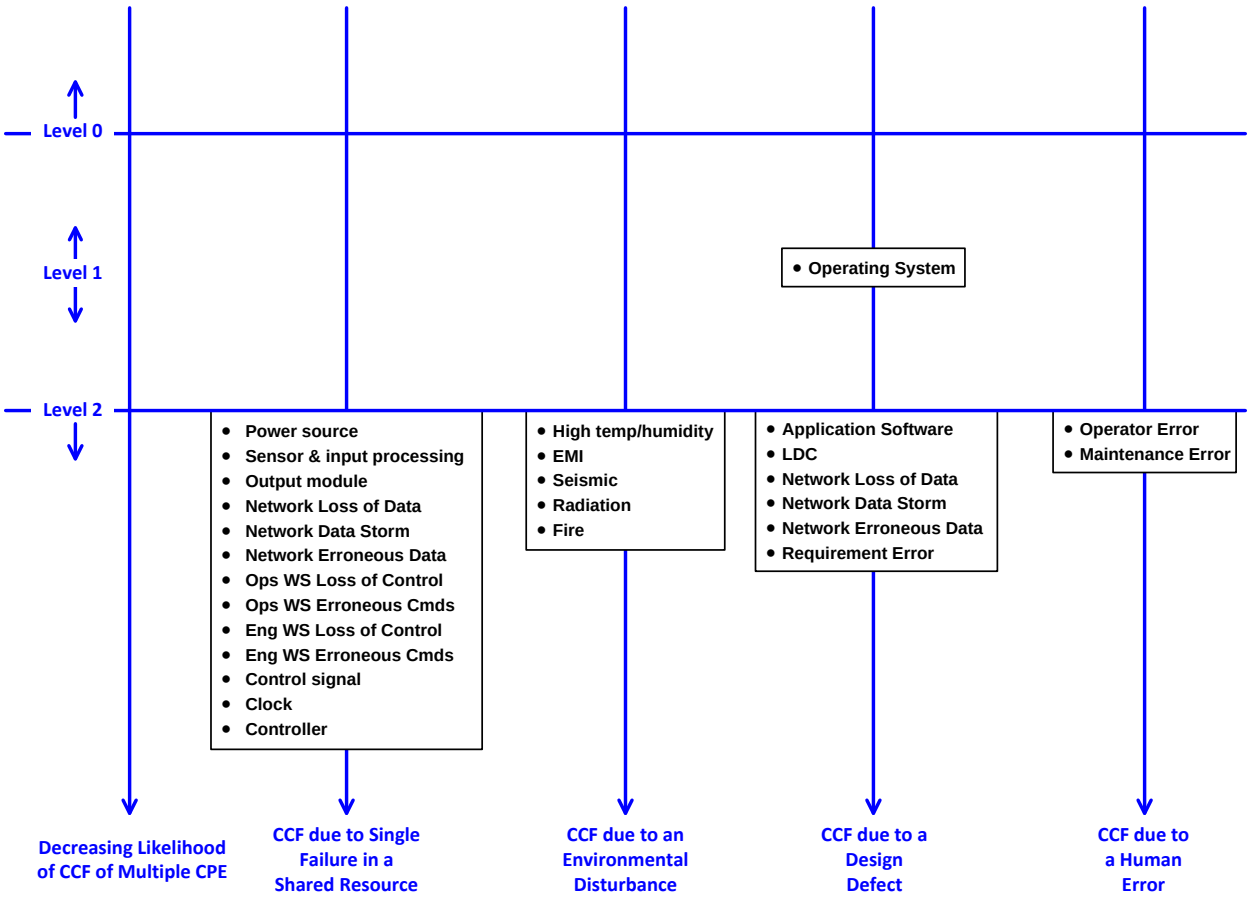

Figure H-2
CCF Susceptibility Analysis Results

H.5.1 Level 0 Coping Analysis

The Level 0 coping analysis considers CCFs of multiple controlled SSCs that are as likely as those traditionally considered in the conservative safety analysis. Therefore, a CCF at Level 0 is analyzed using conservative methods and acceptance criteria. In this case, there are no CCFs that are considered to have a Level 0 likelihood.

H.5.2 Level 1 Coping Analysis

A Level 1 coping analysis is performed for CCFs caused by a design defect where the likelihood of the CCF is considered to be at Level 1 (i.e., less likely than CCFs traditionally considered in the conservative safety analyses, but still possible), using best estimate methods and acceptance criteria.

As described in Section H.4.3, the likelihood of a CCF of both chiller caused by a design defect in the chiller controls is considered to be Level 1, and the postulated CCF can be analyzed using best estimate methods, assumptions and acceptance criteria, for example:

- Nominal conditions at the beginning of the transient or accident (e.g., no conservatisms with respect to initial power levels, primary coolant conditions, decay heat levels, etc.)

- Credit for non-safety related mitigating systems and operator actions
- Criteria similar to those accepted for PRA applications, including maintaining a coolable core geometry, and maintenance of containment integrity (e.g., containment isolated with environmental conditions less than its ultimate capacity)

In this case, the chiller states that would result from a CCF of both chiller controllers may be unknown, because the proposed design does not fully meet any of the limiting measures for an operating system defect, which would limit the effects of the activated defect to a predictable state. However, the upper and lower limits of chiller operation is determined by its mechanical, electrical and physical characteristics, which can be considered as maximum heat removal, in BTU/hr. at the upper limit of chilled water flow rate, or minimum heat removal, which would be zero (i.e., a dead chiller). All other chiller states are considered to be within the range of chiller capabilities.

The maximum heat removal case has no adverse impact on MCR equipment and personnel beyond creating uncomfortably cool conditions. Heaters are provided in the MCR HVAC system for controlling humidity within limits, and the heater controls are independent of the chiller controls.

However, the minimum heat removal case should consider eventual overheating of equipment located in the MCR envelope, including equipment required for achieving and maintaining safe shutdown. In the event that a total loss of heat removal by the chillers occurs, the control room operators will detect an increase in temperature by feel or by surveillance of MCR room temperature or MCR return air temperature indications, which are independent from the chiller controls.

Furthermore, calculations show that 2 hours (as indicated in the facility Technical Specifications) is enough time to begin safe shutdown from 100% power under normal conditions in the event of a total loss of MCR HVAC, before any adverse impacts on safe shutdown equipment occur caused by overheating. Whether the plant is at power or the I&C failure is assumed to occur during a transient or accident, only the chillers are affected by the CCF that would be caused by controller failure. Air handling units and dampers remain unaffected, and are available for supplying outdoor air so that the MCR temperature is kept near the seasonal outdoor air temperature, and one or more MCR doors can be opened to exhaust hot air. Furthermore, the operators can open safe shutdown equipment cabinet doors to reduce the local temperature rise caused by self-heating. Under these conditions, the equipment required for safe shutdown is not expected to reach their specified temperature limits.

With the ability of the operators to provide alternate cooling to the control room to limit ambient temperatures, no mitigating systems are expected to be affected by the loss of control room HVAC. With adequate core cooling available, little or no fuel damage is expected, reactor vessel integrity is likely to be maintained and containment systems remain operable. Even if loss of HVAC were to occur during accident conditions, multiple additional failures would need to occur in addition to the HVAC controllers to result in adverse consequences on-site or to the public.

H.5.3 Expanded Simplified Coping Analysis

With the ability of the operators to provide alternate cooling to the control room to limit ambient temperatures, no mitigating systems are expected to be affected by the loss of control room HVAC. With adequate core cooling available, little or no fuel damage is expected, reactor vessel integrity is likely to be maintained and containment systems remain operable. Even if loss of HVAC were to occur during accident conditions, multiple additional failures would need to occur in addition to the HVAC controllers to result in adverse consequences on-site or to the public.

H.5.4 EDG Chiller Controls Safety Significance Evaluation

The following presents a flow chart and brief description to show how the safety significance based graded approach of Section 4 might apply to this example. Note that from the safety significance perspective, the need for robust preventive design measures in the new chiller I&C might be relatively modest compared to those considered in the susceptibility analysis in Section H.4.

The Figure 4-1 flow chart could be used to guide iterative application of the various activities described in Section 3, making changes as needed until a clear *little or no safety significance* conclusion has been achieved. Figure H-3 shows the paths through the flow chart for a potential CCF of the main control room (MCR) chiller controllers in this example.

The MCR chiller controller modification is a replacement of existing analog chiller controllers with digital controllers. The MCR HVAC is relied upon in the safety analysis for two purposes: to maintain control room environmental conditions and to preclude exposure of control room personnel to external radionuclides. The controlled SSCs are identical before and after the modification. Therefore, the resulting (blue) path through the flow chart for the safety analysis indicates that the modification does not increase the number of controlled SSCs (compressors and auxiliaries). Selected attributes of the new system are credited to conclude that the reliability of the new system is at least as good as that of the replaced system (Section 3.5), and so the CCF is deemed to have *little or no safety significance*. Note that if the modification had increased the number of controlled SSCs or affected multiple plant systems, it might have been possible to reach a *little or no safety significance* conclusion through other paths.

The path through the flow chart differs for the PRA (orange), however, as the PRA typically does not model the main control room HVAC system. Rather, it is assumed that the loss of control room HVAC will be obvious to the operators and as the room heats up, doors will be opened and natural or portable circulation of outside air will maintain an acceptable control room environment. Under realistic assumptions, radionuclide concentrations in the environment outside containment would be minimal, as many more failures beyond the control room HVAC would have had to occur in order for there to be significant fuel damage. For these reasons, the main control room chiller modification is considered to have *little or no safety significance* for the PRA as well.

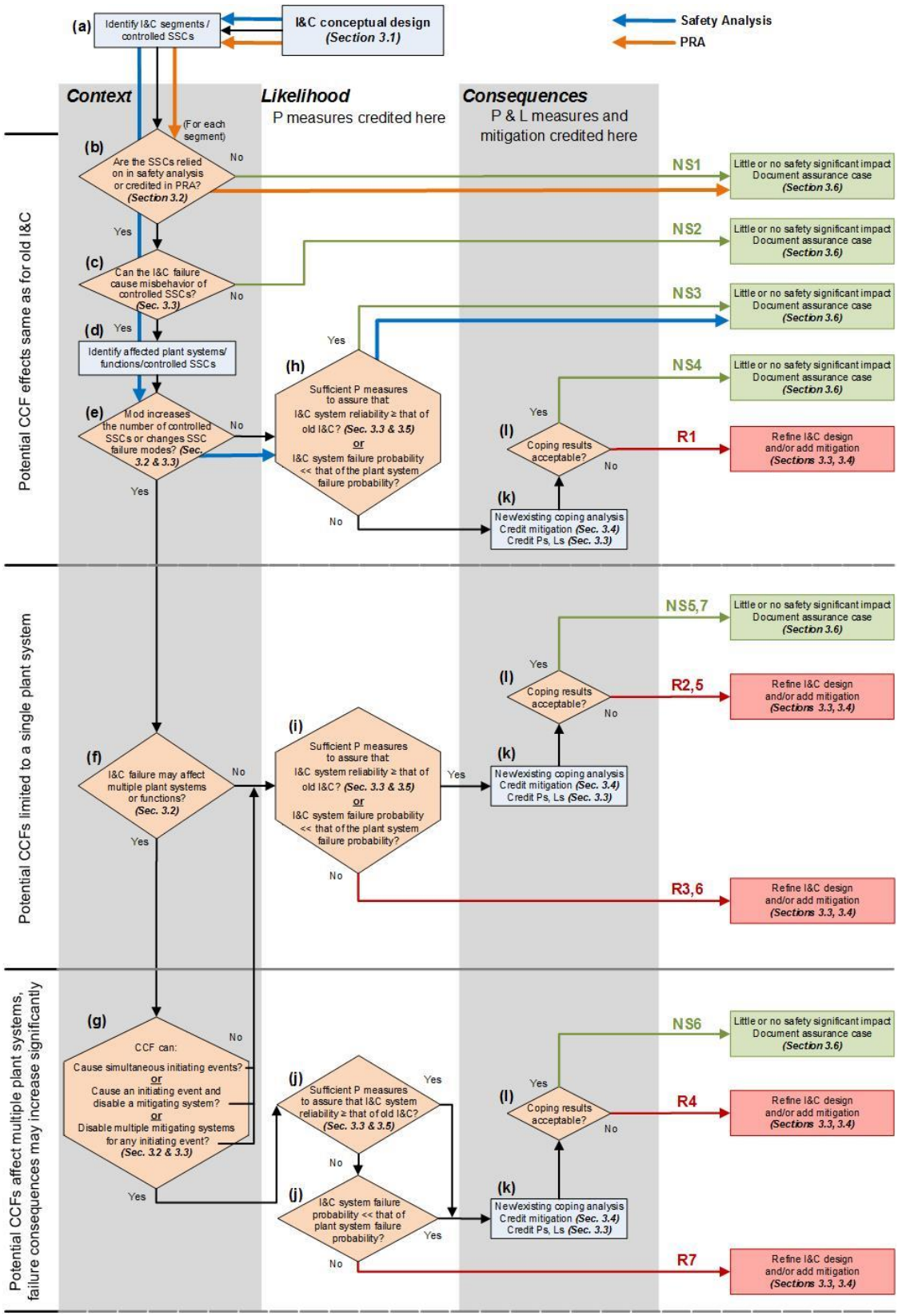

Figure H-3. Application of safety significance flow chart to control room chiller example

Excerpts from Appendix A: Defensive Measures

A.3 CCF Caused by a Design Defect

This section applies to any *design defect* in one or more controllers, either in a Type 1 Design shown in Figure A-1 (multiple SSCs on one controller) or in a Type 2 design shown in Figure A-1 (one SSC on each controller) as noted for each defensive measure. The following types of *design defect*s are addressed in this section:

- Operating system defect
- Application logic defect
- Embedded digital device defect
- Requirements error or omission
- Data communication defect

The measures listed in this section are a more detailed set of measures that are derived from industry experience and prior EPRI research [20].

A *design defect* cannot cause a CCF until it is activated. For a CCF to occur in a Type 1 design, the defect needs to be activated within a single controller. For a CCF to occur in a Type 2 design, the defect must be common among multiple controllers, and the defect must be activated concurrently in multiple controllers. For a Type 2 design, if the likelihood of concurrent triggers can be significantly reduced and an activated defect can be made self-announcing, thereby allowing the defect to be corrected in all controllers, then the likelihood of CCF is considered to be Level 2. Figure A-18 illustrates these principles (note that the middle figure shows separate but concurrent *activating condition*s):

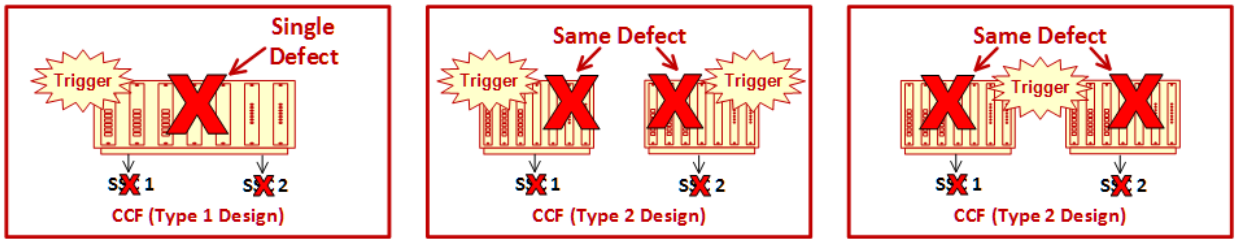

Figure A-18
CCF Caused by an Activated Design Defect

It is noted that duplex and triplex configurations provide no preventive or limiting measure for a *design defect* if the same defect resides in each controller.

Compared to the other I&C failure sources addressed in Sections A.1 (random hardware failure within the I&C), A.2 (environmental disturbance), and A.4 (operations and maintenance error), many of the preventive and limiting measures for SSC malfunctions caused by I&C design defects tend to be more qualitative and subjective, and depend more on specific attributes of the I&C system and the application. For example, what is judged to constitute adequate documentation of software quality may depend on the complexity of the I&C platform and the functional complexity of the application, as well as the safety or operational significance of the potential failure, all of which introduce subjective considerations. Consideration of operating

history will involve some judgment regarding the relevance of the operating history to the nuclear plant application, as well as how much successful operating history is enough to be meaningful. Overall assessment of protection against failures caused by design defects will effectively be a subjective, graded approach, with the preventive and/or limiting measures applied accordingly, possibly including consideration of multiple preventive measures to support an overall assurance argument. Additional discussion of causes of CCFs involving design defects and preventive measures that can reduce their likelihood can be found in [20].

In this guide, the likelihood of a CCF caused by a design defect is considered to be at Level 2 if the potential defect and/or its triggering conditions have been adequately managed using preventive measures, for example if the target system has been subjected to robust requirements engineering methods (See also Section 5.2), and then developed and implemented under structured development and quality assurance processes that are joined with defensive design features. These criteria may be applied to safety or non-safety systems and are the underlying basis for some of the preventive and limiting measures described in this section.

A.3.1 Operating System Design Defect

A *design defect* in the operating system can cause one or more controllers to generate erroneous outputs or the outputs to freeze in their current state.

For the purpose of this guideline, an operating system (OS) is the portion of the software that "comes with the box" in the sense that it is generally not configurable by end users, and the OS alone does not perform any application-specific logic that would be designed for influencing or controlled any CPE (which is the subject of Section A.3.2). An OS can be a commercially available, multi-tasking, real-time package available from a third party, or it can be a single task, once-through firmware program designed by the equipment vendor and embedded in their digital product. The only software distinction made in this guideline is that between an OS and application, which often have different characteristics under the control of different entities.

A.3.1.1 Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in the Operating System to Level 2

To reduce the likelihood of a CCF caused by a *design defect* in the operating system, applying one of the measures from Table A-33 (or comparable measures) is recommended.

Table A-33
Measures Intended to Reduce the Likelihood of a CCF caused by a Defect in the Operating System to Level 2

Preventive Measures	
P1	**Minimize potential for concurrent activating conditions, demonstrate an activated defect is self-announcing, and reduce defect potential through documented software quality**. This measure is only applicable to a Type 2 design because it takes advantage of the requirement for concurrent activating conditions among separate controllers or control segments before a CCF can occur. Projects that are composed of different application logic among control segments are more likely to meet this preventive measure. Note that the specific measures a) through j) provide one or more of the following defenses against CCF: • help reduce the likelihood of a defect • provide assurance that that a defect is not activated concurrently among multiple controllers • provide assurance that that an operating system defect that is activated in one controller or control segment is detected and corrected before it is activated in additional controllers a) The failure or spurious actuation of any SSC is immediately detectable through means that are independent of the affected controller. An activated defect that affects components that are in continuous modulation or frequently repositioned becomes self-announcing. An HFE evaluation demonstrates that a control room HSI allows operators to quickly detect the adverse control condition. Administrative controls (e.g., plant procedures) provide prompt failure investigation and correction, with the intent to correct the defect in all controllers before it is likely to be activated in additional controllers. Periodic testing is not sufficient for triggering a defect or detecting an activated defect, because the testing may not stimulate or reveal the defective part of the design (i.e., periodic testing would need to be equivalent to 100% testing to stimulate or reveal defects). b) For a multi-tasking operating system, employ different tasks with different task scheduling in different controllers. Also employ a cycle time that is within the manufacturers specifications for reliable multi-tasking. Otherwise, employ a single task operating system such that the OS steps are invariant during plant operation (“blind” to plant transients), so plant transients cannot trigger design defects in the OS. c) For controllers with dynamic memory allocation, provide an analysis to demonstrate different allocations among different controllers. Otherwise employ static memory allocation. d) Provide different quantities and configurations of I/O for different controllers. Otherwise employ function processing that is completely independent and asynchronous from I/O processing. e) Provide different configurations of data communication interfaces for different controllers. Otherwise employ function processing and I/O processing that is completely independent and asynchronous from communication processing. f) Provide different cycle times for different controllers. g) Provide different CPU loads for different controllers. h) Provide watchdog timers, independent from the functions processors, to detect scan overrun and underrun conditions. Watchdog timeout results in a forced shutdown condition. Watchdog timers have no reliance on the function processor that is executing the software for which they are detecting scan overrun and underrun conditions.

<table>
<tr><td colspan="3">Preventive Measures</td></tr>
<tr><td></td><td colspan="2">i) Provide buffer overflow detection with error recovery and reporting, or forced shutdown in the event of successive overflows. Provide exception handlers for situations such as out of range inputs, calculated results (e.g., divide by zero), or not-a-number (NaN). Exception handlers will a) provide predefined data defaults to reduce the likelihood of controller shutdown (with alarm), or b) result in controller shutdown.
j) Provide a high quality software development process in accordance with the table below.</td></tr>
<tr><td colspan="3">Preventive Measures</td></tr>
<tr><td></td><td>Safety Divisions
k) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.).
l) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.).
m) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.</td><td>Non-safety Division
n) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design.
o) Confirm good practice security methods during software development.
p) Provide defensive measures for preventing unintended operating system changes when the system is installed.</td></tr>
<tr><td>P2</td><td colspan="2">Same measures as A33-P1, except the low likelihood of a defect is demonstrated through the operating history of the OS in lieu of documented software quality by meeting the following conditions:
a) Substantial and successful operation in multiple different bounding applications of continuous operation without manual or automatic controller reset, or a controller error, including a crash or freeze.
b) The experience base bounds the target application as follows:
1) The software and hardware versions are the same as the target versions. This applies to all operating system software including software for all interfaces and HSIs. Hardware and software problems are reported and promptly and appropriately dispositioned. Hardware and software changes are controlled.
2) The quantity of application program memory is equal to or exceeds the target.
3) The library function blocks encompass all function blocks used in the target.
4) The quantity of modules for each type of I/O is equal to or exceeds the target.
5) The types of data communication interfaces, including interfaces for HSI, encompass the target, and the quantity of each interface type is equivalent to or exceeds the target.
6) The controller’s function processing, I/O processing and communication processing cycle times are equal to or are faster than the target application.</td></tr>
</table>

Table A-33 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by a Defect in the Operating System to Level 2

Preventive Measures	
P3	**Demonstrate that a defect will not be activated when the SSC is needed to perform its required function. .** Applicable only where the controlled SSC is normally in the state needed to perform its required function. Include all of the following defensive measures: a) Administrative controls are in place to provide assurance that the time the controlled SSC is not in the state needed to perform its required function is minimal. Therefore, manipulations are of a short duration and the SSC is returned to its required position after any manipulation. b) Administrative controls to provide assurance that any manipulations that put the controlled SSC in an alternate state (i.e., not the required state) occur for only one SSC at a time. This provides assurance that a defect activated by the manipulation will negatively affect only one SSC. c) Alarms or frequent administrative monitoring controls are in place to immediately identify an SSC that is not in its required state. If the SSC is not being intentionally manipulated this would self-announce an activated defect. d) Provide plant procedures that direct failure investigation and correction, with the intention of correcting the defect in all controllers before the defect is likely to be triggered in multiple controllers. e) The positioning features and alarm/monitoring features (defined above) do not rely on any common design features that could result in erroneous SSC positioning and failure to detect that erroneous positioning. f) The digital device has no external inputs or data communication that will change states when the SSC must be in its required position. This provides assurance that there are no potential defect triggers that could erroneously position the SSC away from its required position.
P4	**Employ a different operating system for each controller so that a failure caused by a design defect in one controller is less likely to affect multiple SSCs.** Applicable only where there are separate controllers controlling individual SSCs. If this preventive measure is applied to controllers in different divisions of a safety system for the same safety function, the impact on Technical Specification Completion Times (CT) and Bypass Times (BT) is assessed, because the safety function relies on internal diversity within the safety system to reduce the likelihood of a CCF, and that diversity is adversely affected when a division is taken out of service. On the other hand, if a diverse backup system is employed to cope with a safety system CCF, then the diversity is not adversely affected when a division of the safety system is taken out of service.

A.3.1.2 Limiting a CCF Caused by a Design Defect in the Operating System

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures in Table A-34 may be helpful.

Table A-34
Measures for Limiting a CCF Caused by a Design Defect in the Operating System

<table>
<tr><th colspan="3">Limiting Measures</th></tr>
<tr><td>L1</td><td colspan="2">Reduce the likelihood of defects through documented software quality and a simple OS, and provide assurance that an activated defect forces the affected controller(s) to a predictable shutdown state. This measure is applicable to a Type 1 Design or a Type 2 Design with a) insufficient controller differences or b) an activated defect is not detectable (in either case, triggering of a defect in multiple controllers cannot be prevented.) See Section A.3.6 for guidance on coping with a CCF caused by an operating system defect.
a) Single task operating system (OS steps are invariant during plant operation (“blind” to plant transients), so plant transients cannot trigger design defects in the OS).
b) Static memory allocation.
c) Execution of all function blocks applicable to the application in a cyclical non-varying manner, regardless of the input states to each function block (i.e., no branching that would skip a function block).
d) Function processing that is completely independent and asynchronous of I/O processing and digital data communication processing (i.e., separate processors for function, communication and I/O with shared memory for data exchange).
e) Watchdog timers to detect scan overrun and underrun conditions, with forced shutdown condition on a watchdog timeout. Watchdog timers have no reliance on the function processor that is executing the software for which they are detecting scan overrun and underrun conditions.
f) Buffer overflow detection with forced shutdown.
g) Exception handlers for situations such as out of range inputs, calculated results (e.g., divide by zero), or not-a-number (NaN). Exception handlers provide predefined data defaults to reduce the likelihood of controller shutdown.
h) Provide a high quality software development process in accordance with the table below.</td></tr>
<tr><td></td><td>Safety Divisions
i) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.).
j) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.).
k) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.</td><td>Non-safety Division
l) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design.
m) Confirm good practice security methods during software development.
n) Provide defensive measures for preventing unintended operating system changes when the system is installed.</td></tr>
</table>

Table A-34 (continued)
Measures for Limiting a CCF Caused by a Design Defect in the Operating System

Limiting Measures	
L2	**Same as A34-L1, except low likelihood of a defect is demonstrated through operating history of the OS in lieu of documented software quality by also demonstrating that the operating history of the OS meets the same conditions listed under A33-P2**.
L3	**Provide all of the same measures as A33-P1, but limit the number of SSCs that share a controller**. When a common operating system is applied to all controllers, but each controller controls multiple SSCs, the defensive measures in P1 limit the CCF to the SSCs controlled by a single controller. This is different than the generic limiting measure (limit the number of SSCs that share a CCF source), because the application of the operating system with the *design defect* is not limited.
L4	**Provide all of the same measures as A33-P2, but limit the number of SSCs that share a controller**. When a common operating system is applied to all controllers, but each controller controls multiple SSCs, the defensive measures in P2 limit the CCF to the SSCs controlled by a single controller. This is different than the generic limiting measure (limit the number of SSCs that share a CCF source) because the application of the operating system with the *design defect* is not limited.
L5	**Provide all of the same measures as A33-P4, except that each controller controls multiple SSCs.** Therefore, a design defect in one controller can result in spurious actuation of multiple SSCs in that controller.