INL/EXT-18-45683
Revision 0

Light Water Reactor Sustainability Program

Strategy for Implementation of Safety-Related Digital I&C Systems

Ken Thomas
Idaho National Laboratory

Ken Scarola
Nuclear Engineering Automation, LLC

June 2018

U.S. Department of Energy

Office of Nuclear Energy

INL/EXT-18-45683

Strategy for Implementation of Safety-Related Digital I&C Systems

Ken Thomas
Idaho National Laboratory

Ken Scarola
Nuclear Engineering Automation, LLC

June 2018

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Office of Nuclear Engineering
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

ABSTRACT

Digital instrumentation and control (I&C) qualification continues to be a major impediment to addressing the reliability and obsolescence issues of the legacy analog I&C systems of the operating light water reactor (LWR) fleet. In particular, the issue of digital common cause failure (CCF) has been difficult to address and has been the reason some nuclear plant operators have deferred upgrades of these critical plant systems, opting rather to maintain them with costly engineering and maintenance efforts. This has now become far more difficult in the face of declining analog technology suppliers and dwindling availability of spare parts and technical support for critical plant components.

At the same time, the nuclear fleet must now reduce its operating costs to remain competitive in a market of low cost gas generation and heavily-subsidized renewables. Digital technology's inherent capabilities of integration, interconnectivity, and standardization offer the foremost means of implementing performance improvements and cost reductions for this purpose. This has been demonstrated over and over again in other industry sectors, as well as in conventional electric generation facilities. However, these digital technologies present certain I&C qualification barriers that must be addressed to enable full deployment where cost-beneficial.

This report presents an assessment of digital I&C qualification issues and addresses gaps in qualification methods and processes that would potentially benefit from Department of Energy (DOE) sponsored research and development. Two new qualification methods are described that are recommended for further investigation. They are 1) Testability – the exhaustive (100%) testing of certain digital devices accounting for all combinations of inputs and internal states to ensure there are no digital defects, and 2) Elimination of CCF triggers – ensuring that any latent digital defects are not concurrently triggered in multiple digital functions that are assumed to be independent (e.g., redundant safety systems).

In addition, this report presents a strategy for implementation of safety-related digital I&C systems as part of full nuclear plant modernization. This modernization strategy exploits the inherent digital capabilities of integration, interconnectivity and standardization to modernize I&C systems without compromising safety or performance, thereby reducing implementation cost and schedule, and reducing recurring operations and maintenance cost. It similarly addresses other opportunities for operating cost reduction using on-line monitoring and mobile worker/process efficiency technologies. The strategy is based on four interrelated elements that together address the remaining barriers to successful implementation: 1) end-state architecture, 2) cost-benefit analysis, 3) regulatory approach, and 4) implementation plan. The digital qualification methods presented in this report are key facilitators in this full nuclear plant modernization strategy.

CONTENTS

FIGURES

TABLE

ACRONYMS

AIM	Analog input modules
ALWR	Advanced Light-Water Reactor
AOO	anticipated operational occurrences
ATWS	anticipate transient without scram
BTP	Branch Technical Position
CCF	common cause failure
CDF	core damage frequency
CDM	compact digital modernization
CIM	component interface modules
CPLD	complex programmable logic device
CPU	central processing unit
DAS	diverse actuation system
DCS	distributed control systems
DI&C	Digital Instrumentation and Control
DNBR	departure from nuclear boiling ratio
DNP	Delivering the Nuclear Promise
DOE	Department of Energy
DPP	diverse protection processor
EDD	embedded digital devices
EMI	electromagnetic interference
EPRI	Electric Power Research Institute
ESF	engineered safety feature
FMEA	failures modes and effects analysis
FPGA	field programmable gate arrays
FSAR	Final Safety Analysis Report
GDC	General Design Criteria
HSI	human-system interface
I&C	instrumentation and control
I/O	input/output
IAP	Integrated Action Plan
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
ISG	Interim Staff Guidance

IT	information technology
ITS	information technology system
KVM	keyboard, video, mouse
LCO	limiting condition of operation
LDP	large display panel
LERF	large early release frequency
LOOP	loss of offsite power
LWR	light water reactor
LWRS	Light Water Reactor Sustainability
MCR	main control room
MTBF	mean-time-between-failure
NEI	Nuclear Energy Institute
NITSL	Nuclear Information Technology Strategic Leadership
NPP	nuclear power plant
NRC	Nuclear Regulatory Commission
O&M	operating and maintenance
OC	operator consoles
OCF	output compare function
ORNL	Oak Ridge National Laboratory
PA	Postulated Accidents
PCS	Plant Control System
PID	proportional-integral-derivative
PLC	programmable logic controllers
PLD	programmable logic devices
POD	plant overview display
PPP	plant protection processor
PRA	probabilistic risk assessment
R&D	research and development
RFID	radio frequency identification
RG	Regulatory Guide
RPS	reactor protection system
RSR	remote shutdown room
RT	reactor trip
RTB	reactor trip breaker
SBO	station black-out

SDCV	spatially dedicated continuously visible
SDOE	secure development and operational environment
SOE	sequence-of-events
SRM	Staff Requirements Memorandum
SRP	Standard Review Plan
SSPS	Solid State Protection System
TAA	transient and accident analyses
ToR	Topical Report
TS	Technical Specification
TT	turbine trip
UFSAR	Updated Safety Analysis Reports
VDU	video display unit

Strategy for Implementation of Safety-Related Digital I&C Systems

1. INTRODUCTION

Digital instrumentation and control (I&C) qualification continues to be a major impediment to addressing the reliability and obsolescence issues of the legacy analog I&C systems of the operating light water reactor (LWR) fleet. In particular, the issue of digital common cause failure (CCF) has been difficult to address and has been the reason that some nuclear plant operators have deferred upgrades of these critical plant systems, opting rather to maintain them with costly engineering and maintenance efforts. This is getting more and more difficult in the face of declining analog technology suppliers and dwindling supplies of spare parts and support for many critical components.

At the same time, the nuclear fleet must now reduce its operating costs to remain competitive in a market of low cost gas generation and heavily-subsidized renewables. Digital technology's inherent capabilities of integration, interconnectivity, and standardization offer the foremost means of implementing performance improvements and cost reductions for this purpose. This has been demonstrated over and over again in other industry sectors, as well as in conventional electric generation facilities. However, these digital technologies present certain I&C qualification barriers that must be addressed to enable full deployment where cost-beneficial.

For these reasons, the nuclear industry has put considerable focus on addressing the technical and regulatory aspects of digital qualification, especially digital CCF. Likewise, the Nuclear Regulatory Commission is addressing these issues through their Integrated Action Plan (IAP) [1], clarifying and improving regulatory guidance to achieve more predictable and timely outcomes in digital regulatory and licensing processes.

The purpose of this report is to present an assessment of digital I&C qualification issues and address gaps in qualification methods and processes that would potentially benefit from DOE-sponsored research and development. It provides an understanding of the key attributes of digital technologies that enable the desired business improvement, but also introduce new failure modes that must be managed.

In addition, this report presents a strategy for implementation of safety-related digital I&C systems as part of full nuclear plant modernization, addressing three major domains of digital technology deployment: 1) I&C systems, 2) on-line monitoring, and 3) mobile worker/process efficiency. Specific actions are outlined to pursue this strategy as a means for the U.S. nuclear operating fleet to reduce operating costs and improve operating performance, thereby enabling operating lives beyond 60 years.

2. DIGITAL I&C QUALIFICATION

Qualification for digital I&C systems in nuclear power plants involves many technical considerations and evaluations. In fact, qualification is a very broad term as defined by the Institute of Electrical and Electronics Engineers (IEEE) in standard IEEE 100-2000 [2] as follows:

> *The generation and maintenance of evidence to ensure that the equipment will operate on demand to meet the system performance requirements.*

Qualification is often thought to refer just to the ability of systems and components to withstand adverse environmental and operating conditions, as well as the ability to perform specified design functions. However, in the context of this report, qualification for digital I&C systems refers to both technical and regulatory acceptability, in that they are closely intertwined. Moreover, digital I&C systems are subject to conventional qualification requirements as well as unique qualification issues, and these can

be interrelated. This section describes both the conventional and unique qualification issues of digital I&C systems.

The term "digital" as is used in this report refers to all devices that either directly use software for their logic functions or devices whose logic functions are developed using software even though they might be implemented in hardware or firmware. Software devices would include such things as standard computer processors and programmable logic controllers (PLCs). Firmware devices would include such things as Field Programmable Gate Arrays (FPGAs) and Complex Programmable Logic Devices (CPLDs). In both case, the final products are subject to having defects created in the software development process and are therefore of equal concern in digital qualification.

This section overviews the inherent features of digital technology that benefit nuclear plant performance, but also create the potential for new failure modes that can result in adverse safety conditions. This section also describes how those adverse failure modes can be successfully managed, including equipment qualification (or equivalent) to demonstrate that most digital failures can be prevented. For digital failures that cannot be prevented, this section describes plant level mitigation and analysis methods to demonstrate that plant safety is maintained.

2.1 Digital Technology Improves Nuclear Plants

Digital technology offers the inherent capabilities of integration, interconnectivity, and standardization that can significantly reduce nuclear power operations and maintenance (O&M) costs, and improve plant performance and availability, while maintaining or even improving plant safety. Integration refers to the capability to control multiple functions from a single digital controller; thereby reducing the number of controllers with corresponding cost reductions. Interconnectivity refers to the capability for digital data communication between two or more digital controllers; thereby implementing more intelligent automation and/or improved human systems interfaces, and eliminating the initial and recurring costs associated with hardwired connections. Standardization refers to the use of a common digital platform for multiple control functions (i.e., the same controller model number with different applications software); thereby improving engineering and maintenance efficiency.

2.2 Potential for New I&C Failures

However, if not correctly designed, these same inherent capabilities for integration, interconnectivity and standardization can create single sources of failure that can adversely affect multiple control functions; therefore, these are sources of CCF. A CCF is the malfunction of two or more plant components or functions due to a single failure source. That single failure source may be a random failure of a single hardware resource that is shared among multiple control functions, or a defect in a standard design that is shared among multiple control functions.

CCFs have the potential to create unanalyzed malfunctions that may not be bounded by previous plant analyses; thereby, creating unanalyzed plant conditions that may challenge plant safety. Some examples:

1. A single random hardware failure within a controller can result in 1) multiple erroneous control outputs affecting multiple functions integrated within the same controller (i.e., a CCF), and/or 2) erroneous digital data communicated between controllers that can adversely affect control functions in multiple interconnected controllers (i.e., a CCF).
2. A single random hardware failure in a digital data communication interface, can cause a data storm that 1) prevents deterministic data communication between multiple control functions in interconnected controllers (i.e., a CCF), and/or 2) adversely affects the deterministic execution of multiple control functions in one or all interconnected controllers (i.e., a CCF).
3. A hidden digital platform design defect can adversely affect multiple control functions in multiple controllers (i.e., a CCF), even if those controllers have no other shared resources, such as the

controllers in different divisions of a safety system or multiple non-safety controllers that have no interconnections.

In these examples, a control function may be the control of a complex function, such as steam generator feedwater flow control, reactivity control, or reactor coolant temperature control; or more simplistic control of a single plant component (e.g., pump, valve, breaker) in a safety or non-safety system.

Example 3 illustrates the most common industry perception where a CCF is attributed to a design defect in software; this has resulted in the frequently used term "software CCF" (SCCF). But it is important to understand that a design defect can also exist in digital components that have no software, such as FPGAs and CPLDs. While a defect in these devices may originate in the software used to program them, a defect can also originate in the basic design of the programmable hardware itself. Therefore, in this report the term SCCF is not used; instead this report refers to a CCF due to a design defect (i.e., within any digital device).

Examples 1 and 2 describe CCFs that are much less understood in the industry. A single random hardware failure that results in the malfunction of multiple control functions/components is a CCF. Since modern distributed control systems (DCS) exploit the inherent capabilities of digital technology to easily integrate numerous control functions, either directly in the same controller or through the digital communication interface between multiple controllers, this technology introduces sources of CCF that require specific deterministic design attributes to ensure those potential CCFs do not challenge plant safety. These design attributes to prevent a CCF due to shared digital hardware resources tend to be far more complex than preventing a CCF due to shared analog resources, such as a shared power source where redundant power supply auctioneering with voltage regulation on each analog module (to manage an overvoltage failure) is a relatively simple well understood solution.

Individually, these inherent attributes of integration, interconnectivity and standardization pose new potential sources of CCF for digital systems that were inherently prevented in analog technology. Each of these attributes almost always facilitates designs that are far more complex than their analog predecessors. This complexity is compounded when these attributes are used together. Hence, complexity underlies integration, interconnectivity and standardization; making digital systems more susceptible to a design defect.

2.3 New Digital CCFs Can Cause Unanalyzed Plant Events

Plant safety is assured for events that have been considered in the plant's transient and accident analyses (TAA) which is typically Chapter 15 of most Updated Safety Analysis Reports (UFSARs). While the plant may be safe for other events, there is no certainty of safety without additional analysis. Potential CCFs in new digital safety or non-safety systems can create unanalyzed plant conditions because the plant level TAA for currently operating U.S. plants was based on the failures considered applicable to the analog I&C technology when those analyses were performed.

Analog technology had very limited capabilities; there was no integration (i.e., each analog module performed one function) and very little interconnectivity due to the high cost of hardwired connections. While hardwired interconnections could propagate functional failures, they could not propagate failures that could lead to erratic non-deterministic performance. Standardization was also very limited due to the need for specialty analog modules for each different type of function. Therefore, potential CCFs in new digital safety and non-safety systems are typically not encompassed by the deterministic safety analysis of most operating nuclear plants.

This does not mean that these new digital CCFs are not encompassed by CCFs considered in the plant's probabilistic risk assessment (PRA). An examination of the PRA may show that many, possibly all, have been considered. But the purpose of the PRA is to assess core damage frequency (CDF) and large early release frequency (LERF). This is quite different than deterministic analyses whose purpose is

to demonstrate successful mitigation for each postulated anticipated operational occurrence (AOO) and postulated accident (PA) based on specific regulatory acceptance criteria.

In the past, there have been industry efforts to attempt to demonstrate that CCFs that do not result in excessive CDF/LERF based on the PRA and should not require consideration in deterministic accident analyses. This position also identified the adverse potential for new CCFs due to spurious actuation of backup systems, like a diverse actuation system (DAS), which would need to be added to mitigate AOOs/Pas with a concurrent CCF in the primary safety system. These efforts were not successful because 1) PRAs cannot accurately model the CCF likelihood due to a digital design defect (e.g., software error), 2) the consequences of an accident with a concurrent CCF in the primary safety mitigation system are significant, 3) the likelihood for spurious actuation of a backup mitigation system (e.g., DAS) can be reduced to a very low level, and 4) the consequences of spurious actuation of a backup mitigation system (e.g., DAS) are manageable without significant consequences.

The following sections describe the analog technology basis of the CCFs currently considered in the TAA of most plants and the potential new CCFs that can be introduced by digital technology. CCFs in I&C systems that can lead to new unanalyzed plant transients (i.e., initiators) are distinguished from CCFs in systems that are credited in the TAA to mitigate transients and accidents (i.e., mitigators).

For new digital CCFs that cannot be prevented, Section 2.3.3 describes the new plant level analysis needed to demonstrate that plant safety is maintained for these new unanalyzed plant conditions. This section distinguishes the conservatism needed in the analysis methods based on the likelihood of the CCF.

2.3.1 Initiator Failures

The transients analyzed for operating nuclear plants are those that are expected to occur during the life of the plant; these are also referred to as AOOs. Since the TAA for operating nuclear plants were conducted during an era of analog I&C technology, and analog technology inherently requires segmenting control functions into many different controllers, these analyses primarily considered transients that could be initiated by single control function or single component failures, in safety or non-safety systems. There was little or no consideration of the more complex multiple component/function failures (i.e., CCFs) that can occur through the commonly shared resources (i.e., hardware and designs) that are inherent in digital technology, if the systems that employ that technology are not properly designed to prevent those CCFs.

Some examples:

1. A typical overcooling event may consider flow from one main feedwater pump whose analog controller has erroneously demanded full flow. But if two feedwater pumps are controlled by one digital controller, a single random hardware failure within that controller may cause an erroneous demand for full flow from two feedwater pumps (i.e., a CCF); actual sources of this type of failure are discussed later. Therefore, the digital system has the potential to cause a different malfunction at the feedwater control system level. This is a new unanalyzed transient that challenges departure from nuclear boiling ratio (DNBR) margin.
2. A typical power distribution anomaly event may consider a single control rod deviation, or the erroneous withdrawal of one control rod group. But if multiple control rods and multiple groups are controlled by one digital controller, a single random hardware failure within that controller may cause an erroneous motion demand for multiple control groups or multiple asymmetrical control rods (i.e., a CCF); actual sources of this type of failure are discussed later. Therefore, the digital system has the potential to cause a different malfunction at the rod control system level. This is a new unanalyzed transient that challenges local power density fuel design limits.
3. A typical safety system spurious actuation event may consider the erroneous actuation of a single engineered safety feature (ESF) function (e.g., safety injection actuation). But if multiple ESF functions are controlled by one digital controller, a single random hardware failure within that

controller may cause spurious actuation of multiple ESF functions (i.e., a CCF); actual sources of this type of failure are discussed later. Therefore, the digital system has the potential to cause a different malfunction at the ESF actuation system level. This is an unanalyzed transient that challenges several critical safety functions.

These examples illustrate the potential for a digital system to cause a CCF that causes a different malfunction at the system level than previously analyzed for analog technology. Additional analysis is needed to determine the effect of these potential system level malfunctions at the plant level. For example, even though a digital CCF has the potential to cause higher flow than considered in the original overcooling analysis, the margin to the DNBR critical safety function limit may be insignificantly decreased; plant level analysis is discussed later.

2.3.2 Mitigator Failures

The AOOs and PAs in the plant's design basis TAA are analyzed with a concurrent failure in one safety division of the credited mitigation functions; there is typically no consideration of the failure of multiple safety divisions (i.e., a CCF), because compliance to the single failure criterion prohibit shared hardware resources among different safety divisions and safety systems are qualified to ensure they are immune to external hazards (e.g., earthquakes, electromagnetic interference or EMI, high temperature) that have the potential to adversely and concurrently affect both redundancies.

There is also no consideration of a CCF due to a common design defect in the plant's TAA for design basis AOOs or PAs. This design basis was due in part to the inherent simplicity of analog technology. Due to this simplicity, as well as a robust design process, an analog design defect was considered as unlikely as a maintenance error or an environmental hazard that exceeds the equipment qualification envelopes. Hence, failures in mitigating systems due to these potential sources of CCF are also considered unlikely.

Therefore, a CCF of multiple analog safety divisions was considered sufficiently unlikely so as to require no further consideration in the design basis TAA. A CCF of multiple analog safety divisions is considered in the PRA to assess CDF, but it is not considered in design basis plant analyses that demonstrate successful event mitigation.

But the Nuclear Regulatory Commission (NRC) criteria pertinent to anticipate transient without scram (ATWS) and station black-out (SBO) recognize that there are sources of CCF, including a design defect in analog systems that can adversely affect multiple safety divisions. A concurrent CCF is considered for these events, because the events themselves have higher likelihood than other AOOs and PAs. Therefore, the combined likelihood of these events plus a concurrent analog CCF warrants further consideration.

Even with a robust design process, the inherent complexity of digital technology increases the likelihood of a design defect compared to its analog technology predecessor. If a digital system does not contain design attributes that specifically defend against a CCF due to a potential design defect, a CCF due to a digital design defect is more likely than considered for analog technology. Therefore, even though other events have a lower likelihood than ATWS and SBO, the combined likelihood of those other events plus a concurrent digital CCF, together with the adverse consequences of those other events, also warrants further consideration.

Since current analyses of AOOs and PAs, except ATWS and SBO, credit at least one safety division for event mitigation, an accident with a CCF of multiple safety divisions causes a different malfunction at the system level than previously analyzed for analog technology; for these events the plant's capability for successful mitigation is unknown. Therefore, additional analysis is needed to determine the effect of these potential system level malfunctions at the plant level. For example, even though the equipment credited in the TAA for event mitigation is unavailable due to the CCF, other manual or automated equipment may be sufficient to mitigate the event.

The regulatory basis for considering CCF in safety and non-safety initiators and safety mitigators is discussed later. The regulatory basis is consistent with the technical bases described above.

2.3.3 Plant Level Analysis

Single random hardware failures are expected during the life of a nuclear plant. Therefore, to determine the plant level results of these failures, conservative design basis analysis methods are appropriate. Therefore, a digital CCF caused by a shared hardware resource in initiators (safety or non-safety) or mitigators is a design basis event that requires analysis using conservative design basis methods as employed in the plant's safety analyses for all events except ATWS and SBO.

Due to a robust design process controlled by regulatory criteria for safety systems, the likelihood of a CCF due to a design defect in either analog or digital technology is significantly lower than the likelihood of a single random hardware failure. So, an analog or digital CCF that results in ATWS or SBO, or a digital CCF concurrent with any AOO or PA, is considered a beyond design basis event. This low likelihood is also applicable to a digital CCF that results in erroneous outputs from a safety controller and thereby results in a new unanalyzed transient. The low likelihood of these potential CCFs in safety systems permits the use of less conservative methods when analyzing event initiation or mitigation, compared to the more conservative methods employed for design basis events. These less conservative methods are referred to as "best estimate" methods, which are discussed in Section 3.4.1.2.

While a robust design process is regulated for safety systems, it is not regulated for non-safety systems. If a robust design process cannot be demonstrated, a CCF due to a design defect in a non-safety initiator would need to be analyzed as a design basis event. Alternately, if a robust design process can be demonstrated, a new transient would be considered a beyond design basis event; it may be analyzed using best estimate methods, as discussed above for safety systems. A graded approach may be used in assessing the robustness of the design process for non-safety systems, as described in Section 3.2.6.

2.4 CCF Sources and Defenses

CCF is sometimes misunderstood to mean a failure of redundant safety divisions due to a software error. More correctly, CCF refers to the failure of any two or more components, due to a single failure source; this broader definition of CCF is used in this report.

To clearly discuss CCF some basic terms and concepts must be defined. This section describes:

- Shared resources, which are the source of a potential CCF.
- Defensive measures, which are employed within the target I&C system(s) to prevent a CCF from a shared resource, or limit the system level effects of an unprevented CCF.
- Mitigating measures, which are employed external to the target I&C system(s) to cope with a CCF at the plant level.
- Triggers, which are essential to understanding how a design defect can lead to a CCF.

2.4.1 Shared Resource

The potential for a CCF is introduced through shared resources among multiple control functions, safety or non-safety. A shared resource may be a hardware component, such as a digital controller or a digital data communication interface. When that shared hardware component has a random hardware failure, multiple control functions can be adversely affected. A shared resource may also be a design. Even if there are no shared hardware resources, a design defect that affects multiple independent hardware components can adversely affect multiple control functions.

2.4.2 Defensive Measure

Defensive measures are applied to the target digital system, as opposed to mitigating measures which are applied outside the target digital system, as described below. Defensive measures are design and design process attributes that prevent, limit or reduce the likelihood of a CCF. Design attributes are deterministic features of the system. Design process attributes address design defects. There are three types of defensive measures; each is explained in the following sections.

2.4.2.1 Preventive Measure. A preventive measure is a deterministic design attribute that reduces the likelihood of a CCF to a level comparable to other sources of CCF that are not considered in the plant's licensing basis, such as a maintenance error or an environmental hazard that exceeds equipment qualification or testing envelopes. It is important to understand that a preventive measure does not eliminate all possibility of a CCF. When a preventive measure is applied no further consideration of a CCF is needed in deterministic analysis that demonstrate event mitigation. However, a CCF from these highly unlikely sources is still considered in the PRA.

For example, for a power supply that controls multiple functions, a redundant power supply is an example of a preventive measure; it prevents a CCF of multiple functions due to failure of the power supply, which is a shared hardware resource. This does not mean that there is no possibility of both power supplies failing concurrently. But a CCF due to the concurrent failure of both power supplies is considered so unlikely that it requires no further consideration.

2.4.2.2 Limiting Measure. For a CCF that cannot be prevented, a limiting measure is a deterministic design attribute that ensures the potential CCF effects a small number of plant control functions or that the control functions fail in a pre-determined state. Limiting measures are employed to ensure the CCF results in a system level failure that has been previously analyzed, or a failure that is either more easily analyzed at the plant level or results in an acceptable plant level malfunction result. Some examples:

- Controlling only a few plant components from a single digital controller is a limiting measure; it simplifies the analysis needed to determine the system level and plant level effect when those components fail concurrently.
- A limiting measure may ensure the digital feedwater control system always fails in a manner that results in loss of all feedwater rather than an excess feedwater condition. This limiting measure results in a condition that is already analyzed for most plants, rather than a condition that may be unanalyzed. Of course, when a limiting measure like this is applied, other design attributes must ensure there is very low likelihood that the limiting measure will be activated, since the limiting measure itself may be adverse to plant safety.

2.4.2.3 Likelihood Reduction Measure. Since including design attributes to prevent or limit a CCF may not be practical for all applications, a likelihood reduction measure is a design or design process attribute that ensures the potential CCF is significantly less likely than a single random hardware failure. When the system level result of a CCF is different than previously analyzed, a likelihood reduction measure facilitates the use of beyond design basis analysis methods to determine the plant level result. Beyond design basis methods are less conservative than the design basis analysis methods used for most events in the plant's TAA. The regulatory basis for treating some CCFs as beyond design basis events is discussed in Section 3.1.6.

2.4.3 Mitigating Measure

When a CCF is not prevented, the resulting malfunction must be mitigated. Unlike a defensive measure, which is applied internal to the target digital system, a mitigating measure is applied outside the target digital system to ensure the system level or plant level result of a CCF in the target digital system is acceptable. Mitigating measures may be as simple as mechanical or electrical interlocks, or manual or

automated actions from another system. Manual or automated actions initiated from a DAS when there is a CCF in the primary safety system, is an example of a mitigating measure.

2.4.4 Trigger

Although a common design is a shared resource, it should not be assumed that a potential design defect in that shared resource will always result in a CCF. For a design defect to cause any failure, the defect must be triggered. This means that a combination of external input states and internal operating states must be encountered that was overlooked during system testing; if it was not overlooked, the defect would have been triggered, discovered and previously corrected. For a digital system with a robust design process, this combination of overlooked internal and external states would be very rare.

In addition, for that failure to become a CCF, the defect must be triggered in a device that controls multiple functions, or it must be separately and concurrently triggered in multiple different digital devices that share the same design, and hence have the same design defect.

For separate digital devices, concurrent triggers are necessary for a CCF. Despite a common design with a common design defect, concurrent triggers can be prevented through differences in application level configuration and software. NRC has accepted internal diversity as a CCF preventive measure on the basis that diverse designs will not have a common design defect. Application level design differences is an extension of that diversity concept that can prevent concurrent triggers when there are other common design aspects.

But even application level diversity cannot prevent those same trigger conditions from eventually being encountered, even in separate digital devices. Therefore, to prevent a CCF, a triggered defect must be self-announcing. This means that the erroneous operation of the controller must result in a plant disturbance or alarm that is immediately identifiable by plant operators. This self-announcing facilitates identification of the defect, which further facilitates correcting the defect before it is triggered separately in a different controller (i.e., before it becomes a CCF).

Application level differences are common in safety and non-safety initiators, and erroneous control outputs are typically self-announcing because they result in plant transients. Therefore, non-concurrent triggers can often be credited to prevent a CCF of multiple separate control functions (e.g., an overcooling event with a reactivity control event).

But non-concurrent triggers are much more difficult to credit for CCF prevention in safety mitigators, because many safety mitigators operate in a standby mode (e.g., RT and ESF actuation functions). This means that a triggered defect that prevents safety function actuation from a digital device is most likely not self-announcing, because the digital device simply remains in the standby mode (i.e., the trigger and defect remain hidden). Therefore, the same trigger conditions can eventually occur in other digital devices, resulting in a CCF.

In summary, internal diversity eliminates a common design defect; therefore, it prevents a CCF. When there is a common design with an unknown internal defect, application level design differences result in non-concurrent triggers. But to prevent a CCF, a triggered defect must be self-announcing so the defect can be corrected before it is non-concurrently triggered in another device with the same defect. Section 4.1.3 describes digital qualification necessary to credit non-concurrent triggers as a preventive measure for a CCF due to a design defect.

3. REGULATORY BASIS FOR MANAGING COMMON CAUSE FAILURE

Industry reports, such as Electric Power Research Institute (EPRI) 3002005326 “Methods for Assuring Safety and Dependability DI&C Systems” [3], identify potential digital failure sources that can result in a CCF, and defensive measures that can prevent, limit or reduce the likelihood of a CCF. Most of

those defensive measures are rooted in regulatory qualification criteria that have been used to prevent CCF since the earliest days of nuclear power.

The regulatory criteria that establish the basis for digital I&C qualification and analysis to manage CCF is different for safety systems in multiple independent divisions that are credited for accident mitigation, and safety or non-safety systems within the same division that have the potential to initiate transients.

The qualification criteria and their differences are discussed in Sections 3.1 and 3.2. Due to the industry focus on preventing a CCF due to a software design defect, Section 3.3 summarizes the software qualification differences for software.

Similarly, the regulatory criteria that establish the basis for the safety analysis of plant transients and accidents is dependent on the likelihood of the failure source, and whether the failure affects an initiator or a mitigator. These regulatory differences and their basis are described in Section 3.4.

3.1 CCF in Safety Mitigation Systems

While the focus on CCF has increased since the introduction of digital systems, preventing CCF has been the underlying basis of almost all regulatory criteria pertinent to safety systems credited for transient and accident mitigation since the earliest days of commercial nuclear power. This includes prevention of CCF due to environmental hazards, as well as CCF due to certain design errors.

10 CFR 50 Appendix A, General Design Criteria (GDC) 21 [4] requires that protection systems have redundancy to ensure the safety functions credited for accident mitigation and safe shutdown can be performed, even in the presence of a single failure. GDC 21 also requires independence between those redundancies to ensure a failure in one redundancy does not propagate to adversely affect the second redundancy. GDC 22 [4] extends the independence criteria to address other failure sources, including design defects that may adversely affect both redundancies.

Although not stated in this manner, these independence criteria are requirements for CCF prevention. Sources of potential CCFs and defensive measures to prevent CCFs from those sources are addressed in many regulatory criteria that are rooted in the CCF prevention criteria of GDC 21 and GDC 22.

The key sources of CCF and the regulatory criteria that guide prevention of CCF from those sources are described in the sections that follow.

3.1.1 Single Failure

Single failure is defined in the GDC as follows:

> *A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure. Fluid and electric systems are considered to be designed against an assumed single failure if neither (1) a single failure of any active component (assuming passive components function properly) nor (2) a single failure of a passive component (assuming active components function properly), results in a loss of the capability of the system to perform its safety functions.*

In addition, 10 CFR 50.55a (h) [5] requires conformance to IEEE 603-1991 [6], which states the single failure criterion as follows:

> *The safety systems shall perform all safety functions required for a design basis event in the presence of*
>
> *a) Any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures.*

b) All failures caused by the single failure.
c) All failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

The phrase "multiple failures resulting from a single occurrence" from the GDC definition is referred to in this report as a CCF that is within the design basis.

The GDC, including the independence criteria of GDC 21 and 22, preclude shared hardware resources among redundant safety mitigation systems. This provides inherent protection against a CCF of redundant safety mitigation systems due to a single random hardware failure. Single random hardware failures that can lead to a CCF of multiple safety functions within the same safety division are discussed in Section 3.2.1.

3.1.2 Electrical Faults, Fire, Flood

Regulatory Guide (RG) 1.75 "Criteria for Independence of Electrical Safety Systems" [7] endorses IEEE-384 "Standard Criteria for Independence of Class 1E Equipment and Circuits" [8]. These documents establish physical independence and electrical isolation design criteria to ensure an electrical fault cannot propagate between redundant safety divisions, or from non-safety systems to redundant safety divisions. The design criteria for physical independence also ensures that hazards, such as fire and flood, are unlikely to affect multiple safety divisions.

These regulatory criteria target sources of CCF that can be prevented through physical and electrical independence.

3.1.3 Environmental Hazards

The physical independence criteria of RG 1.75 is targeted toward sources of CCF that would affect equipment in relatively close proximity. But redundant equipment that conforms to the physical separation requirements of RG 1.75 can be adversely affected by environmental hazards, because these hazards transcend those physical boundaries. Therefore, there are several regulatory criteria that prevent a CCF of multiple safety divisions due to common environmental hazards.

- RG 1.100 "Seismic Qualification of Electrical and Active Mechanical Equipment and Functional Qualification of Active Mechanical Equipment for Nuclear Power Plants" [9] endorses IEEE-344 "IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations" [10] to establish design and equipment qualification criteria that ensures an earthquake cannot be a source of CCF that could adversely affect multiple safety divisions.
- RG 1.89 "Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants" [11] endorses IEEE-323 "IEEE Standard for Qualifying Class IE Equipment for Nuclear Power Generating Station" [12] to establish design and equipment qualification criteria that ensure an environmental hazard, such as temperature, pressure, humidity or radiation, cannot be a source of CCF that could adversely affect multiple safety divisions.
- RG 1.180 "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems" [13] endorses EPRI TR-102323 "Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants," [14] to establish design and equipment qualification criteria, that ensures EMI cannot be a source of CCF that could adversely affect multiple safety divisions.
- RG 1.204 "Guidelines for Lightning Protection of Nuclear Power Plants" [15] endorses IEEE 665 "Guide for Generating Station Grounding" [16], IEEE-666 "Design Guide for Electrical Power Service Systems for Generating Stations [17], IEEE-1050 "Guide for Instrumentation and Control Equipment Grounding in Generating Stations [18], and IEEE-C62.23 "Application Guide for Surge

Protection of Electric Generating Plants" [19] to establish design and equipment qualification criteria, that ensures lightning cannot be a source of CCF that could adversely affect multiple safety divisions.

3.1.4 Digital Data Communications

Digital Instrumentation and Control (DI&C) – Interim Staff Guidance (ISG) - 04 "Highly-Integrated Control Rooms—Communications Issues" [20] identifies inter-division digital data communications as a source of failure that can adversely affect multiple safety divisions (i.e., a CCF). Digital data communications can propagate erroneous data between redundant safety divisions, and between non-safety and safety divisions. Erratic performance of the digital data communications interface itself can also result in non-deterministic operation of all connected controllers. DI&C-ISG-04 establishes communication independence preventive measures, such as separate function and communication processors, to ensure a digital data communications interface cannot be a source of CCF that could adversely affect multiple safety divisions.

3.1.5 Functional Dependencies

DI&C-ISG-04 also identifies inter-division data as a source of failure that can adversely affect multiple safety divisions. The data itself is distinguished from the communication method, because erroneous data, originating outside the safety division that is used incorrectly by the receiving division, has the potential to adversely affect the safety function of that division, regardless of how that data is communicated between divisions, digital or hardwired. DI&C-ISG-04 establishes functional independence preventive measures, such as priority logic, to ensure data originating from outside the division cannot be a source of CCF that could adversely affect multiple safety divisions.

3.1.6 Design Defects

As discussed above, analog technology was considered relatively simple; therefore, the only regulatory criteria to reduce the potential for a design defect is in the quality assurance criteria of 10CFR50 Appendix B. For example, safety system designs require independent review.

But in addition to the quality assurance requirements of 10CFR50 Appendix B [21], the complexity of digital technology has resulted in numerous regulatory criteria whose goal is to minimize the likelihood of a design defect in digital systems by establishing digital life cycle requirements. These include:

- RG 1.168 "Verification, Validation, Reviews, And Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" [22], which endorses IEEE-1012 "IEEE Standard for Software Verification and Validation" [23].
- RG1.169 "Configuration Management Plans for Digital Computer Software Used In Safety Systems of Nuclear Power Plants" [24], which endorses IEEE-828 "IEEE Standard for Software Configuration Management Plans" [25].
- RG 1.170 "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" [26], which endorses IEEE-829, "IEEE Standard for Software and System Test Documentation" [27].
- RG 1.171 "Software Unit Testing for Digital Computer Software Used In Safety Systems of Nuclear Power Plants" [28], which endorses IEEE-1008, "IEEE Standard for Software Unit Testing" [29].
- RG 1.172 "Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants" [30], which endorses IEEE-830, "IEEE Recommended Practice for Software Requirements Specifications"[31].

It is important to note that NRC considers these design process life cycle requirements to be CCF likelihood reduction measures, not CCF preventive measures. They establish criteria for a robust design process which reduces the likelihood of a design defect to be significantly lower than the likelihood of a

single random hardware failure; thereby facilitating analysis of a CCF due to a design defect as a beyond design basis event, as described in Sections 2.3.3, and in accordance with the Staff Requirements Memorandum (SRM) to SECY 93-087 “Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs” [32] and Branch Technical Position (BTP) 7-19 “Guidance for Evaluation of Diversity and Defense-In-Depth In Digital Computer-Based Instrumentation And Control Systems” [33].

In BTP 7-19, the only preventive measures for a CCF due to a design defect are (1) internal diversity, or (2) simplicity as demonstrated through 100% testing. The requirements for internal diversity and 100% testing are not clear. In addition, there is currently no NRC criteria that addresses preventing a CCF due to a design defect based on application level diversity, which facilitates non-concurrent triggers, as discussed in Section 2.4.4. Therefore, most applicants take internal diversity to mean digital platform diversity.

Additional possible research on digital qualification to address preventive measures for a CCF due to a design defect is discussed in Section 5.

3.1.7 Setpoint Errors

A safety system setpoint error is a type of design defect that equally applies to analog and digital mitigation systems. RG 1.105 “Setpoints for Safety-Related Instrumentation” [34] establishes design process requirements for setpoint determination. These requirements are preventive measures that ensure a CCF due to a setpoint error in multiple safety divisions requires no further consideration.

3.1.8 Security Threats

An unauthorized change to the configuration of a safety system is a type of design defect that can lead to a CCF. RG 1.152 “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants” [35] establishes requirements to ensure a secure development and operational environment (SDOE). When an SDOE is established and maintained, a CCF of multiple safety divisions due to a security threat requires no further consideration.

3.1.9 Hidden Random Hardware Failures

As noted in Section 3.1.1, regulatory requirements for redundancy and independence do not permit shared hardware resources among different safety divisions. Therefore, a random hardware failure only affects a single safety division. However, if that random hardware failure is not detected and repaired, multiple independent random hardware failures can accumulate to result in a failure of multiple independent safety divisions. Multiple random failures are not a common failure source; therefore, they are not a CCF. However, the inability to detect/repair a random hardware is a common failure source, which is a CCF.

This potential CCF is addressed in RG 1.22 “Periodic Testing of Protection System Actuation Functions” [36], and RG 1.118 “Periodic Testing of Electric Power and Protection Systems” [37] which endorses IEEE-338 "Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems” [38]. These criteria ensure that random hardware failures are detectable through periodic surveillance tests. Therefore, these are preventive measures that ensure a CCF due to undetected random hardware failures in multiple safety divisions requires no further consideration.

3.2 CCF In Non-safety and Safety Initiation Systems

As described in Section 2.3.1, safety and non-safety I&C systems that have the potential to directly initiate plant transients (i.e., initiators) have always been designed such that their failure effects are bounded by the transients analyzed in the plant’s TAA. This requirement is addressed in Section 7.7 of the NRC standard review plan (SRP – NUREG-0800) [39].

While the defensive measures identified for safety mitigation systems in Section 3.1 are not intended for safety or non-safety initiators, some have been applied and should continue to be applied using a graded approach to prevent CCFs that could otherwise lead to unanalyzed plant conditions. The graded approach for each CCF source and applicable defensive measures is described in the following sections.

Most of these defensive measures for non-safety and safety initiators are simple extrapolations of the same defensive measures described in Section 3.1 for safety mitigation systems. The NRC considers these defensive measures sufficient to prevent CCF from all potential sources, and licensees view them as practical to implement. However, the defensive measures for a CCF due to a single failure in a shared hardware resource and a defect in a shared design, discussed in Sections 3.2.1 and 3.2.6, respectively, pose challenges to many applications; this is where additional Idaho National Laboratory (INL) research will be focused, as described in Section 5.2.

3.2.1 Single Failure

As described in Section 3.1.1, the regulatory requirements that ensure independence of safety divisions also inherently provide protection to ensure a single hardware failure in one division does not propagate to another division to become a CCF. Since these same criteria do not apply within a safety or non-safety division, the independence within safety and non-safety control functions must be assessed using a graded approach to ensure there is adequate defense against failure propagation to prevent a CCF in multiple non-safety or safety control functions.

The scope of NRC review identified in Section 7.7 of the SRP is “those systems that can, through normal operation, system failure or inadvertent operation, affect the performance of critical safety functions”. As discussed in Section 2.3.1, digital safety and non-safety systems can generate erroneous outputs that adversely affect multiple control functions, causing unanalyzed plant conditions (i.e., malfunctions that lead to transients that are not considered in the plant’s TAA). Although Section 7.7 of the NRC’s SRP identifies this concern and directs NRC staff to consider this potential for unanalyzed plant conditions in their reviews, there is no specific regulatory criteria that directly identifies defensive measures to address this issue.

As such, for analog systems built in the 1970s and early 1980s, NRC conducted highly subjective reviews of safety and non-safety control system designs, looking for shared hardware resources within the same system or division that could lead to malfunctions that had not been considered in the plant’s TAA. These reviews were conducted through audits of paper designs, and also through additional inspections of actual as-built analog systems. It is important to note that these types of subjective inspections were not necessary for different safety divisions, because of the clear regulatory criteria that prohibited shared hardware resources between multiple safety divisions.

When conducting reviews for initiators within the same division, NRC applied a graded approach compared to their review of safety mitigation systems in redundant independent divisions. The failures that are considered for their adverse effect on multiple safety or non-safety control functions in the same division are limited to failures in single active components. This includes active component failures within power supplies, controllers and data communication interfaces.

GDC 25 and 26 [4] distinguish these active component failures as “single malfunctions” versus “single failures” which are discussed in GDC 21 for the protection system and in other GDCs for other safety systems.

Active component failures (i.e., single malfunctions) are considered, because they are expected during the life of the plant. Therefore, the malfunctions resulting from an active component failure, and the plant level effects of those malfunctions are analyzed as design basis events, using conservative methods.

3.2.2 Electrical Faults, Fire, Flood

Regulatory criteria for safety mitigation systems requires electrical isolation and physical independence between redundant safety divisions to prevent a CCF due to electrical faults, fire and flood. But these sources of CCF are considered rare (i.e., significantly less likely than single active component failures), therefore, in general these isolation and independence criteria are not applied to non-safety equipment or to safety equipment within the same division.

The one exception to this is for fire. While fires are rare, they are sufficiently likely to require consideration as beyond design basis events. As a beyond design basis event, best estimate analysis methods may be used to demonstrate the ability to achieve safe shutdown with a fire; consistent with the use of best estimate methods, no other design basis events (e.g., single failure, earthquake), AOOs or PAs are considered concurrently.

In demonstrating the ability to achieve safe shutdown with a fire in the main control room (MCR) or remote shutdown room (RSR), plants credit controlling the plant from the alternate location to achieve safe shutdown. But for the active control location to be effective, erroneous control signals due to short circuits and electrical faults that may originate from the inactive location due to the fire, must be blocked. This ensures they do not propagate to the safety or non-safety control systems, thereby causing potential erroneous control actions in multiple control functions (i.e., a CCF) that could interfere with achieving safe shutdown.

There are no specific regulatory criteria to ensure electrical faults are blocked to accommodate achieving safe shutdown with a concurrent fire. However, the fault isolation guidance in IEEE-384 is commonly employed, even for non-safety systems. Formal equipment qualification is not required for non-safety isolators, but they should be tested/evaluated to comparable criteria to demonstrate adequate isolation performance to prevent a CCF.

Similarly, there is no specific regulatory criteria to ensure erroneous signals that may originate due to fire induced short circuits or hot shorts are blocked. Erroneous signals are typically blocked by relay disconnects or logical blocking in binary and digital systems. These are effective defensive measures to prevent a CCF due to fire induced erroneous signals.

3.2.3 Environmental Hazards

Environmental hazards are equally applicable to safety mitigators, safety initiators and non-safety initiators. They can cause a CCF of multiple control functions that could result in a complex unanalyzed transient.

For safety systems, the equipment qualification criteria described in Section 3.1.3 are sufficient to preclude further consideration of a CCF due to environmental hazards. This is true for both safety system mitigators, as well as initiators.

For non-safety initiators, a graded approach can be applied through testing, to achieve adequate CCF prevention; formal equipment qualification is not needed. Testing conducted by commercial equipment suppliers can be credited, when the testing is documented to encompass the environmental hazards of concern and includes demonstration of successful performance results. This type of testing is common for commercial equipment that is certified to industrial standards such as ISO 9001 [40]. When testing conducted by the equipment supplier is inadequate, it can be supplemented by testing conducted by the end-user.

3.2.4 Digital Data Communications

The preventive measures in DI&C-ISG-04 [20] that ensure inter-division digital data communications cannot cause a CCF of interconnected safety controllers, are also applicable to intra-division safety and non-safety controllers. The guidance for communication processors and function processors with shared

two port memory ensure deterministic performance of the function processor is maintained despite any communication anomalies.

While DI&C-ISG-04 requires electrical isolation for inter-division digital data communication (e.g., fiber optic cables), electrical isolation is not required for most intra-division digital data communication. The one except to this is intra-division digital data communication that could propagate electrical faults that may interfere with achieving safe shutdown due to a fire in the MCR or RSR, as described in Section 3.2.2. For these digital data communication interfaces, electrical isolation (e.g., fiber optic cables) is required to prevent a CCF that could interfere with achieving safe shutdown.

DI&C-ISG-04 [20] establishes communication independence guidance that may be more conservative than necessary for intra-division safety or non-safety systems. Section 5.2.3 describes further INL research into alternate preventive measures for intra-division digital data communication to prevent a CCF due to a digital data communication failure.

3.2.5 Functional Dependencies

The functional independence preventive measures in DI&C-ISG-04 for safety systems ensure that each division can perform its safety mitigation function with no input from other divisions, and it ensures that any erroneous data received from another division (safety or non-safety) cannot adversely affect its own safety function; in these preventive measures ensure the safety division protects itself from erroneous external signals.

Controllers within the same safety or non-safety division, do not require this same level of functional independence. However, control signals that are interfaced between controllers in the same division can be sources of CCF that result in unanalyzed plant transients.

For example, an error in a reactor coolant system average temperature signal (Tave) that is calculated by the turbine bypass regulating valve controller can cause erroneous steam pressure control. If that same erroneous signal is transmitted to the rod control system for reactivity control, a single random hardware failure that results in an erroneous Tave signal can cause a CCF that adversely and concurrently affects both steam pressure control and reactivity control; this concurrent event is likely to be unanalyzed for most plants.

Defensive measures that provide functionally identical but separate calculations in each controller (e.g., separate calculations of Tave), or multiple redundant calculations with separate comparison logic in each controller to identify erroneous signal calculations, can prevent a CCF due to functional dependencies. No further INL research is needed to employ these methods.

3.2.6 Design Defects

Section 3.1.6 identifies the regulatory guides for safety systems that establish criteria for a robust design process which reduces the likelihood of a design defect to be significantly lower than the likelihood of a single random hardware failure; thereby facilitating analysis of a CCF due to a design defect as a beyond design basis event. While Section 3.2.6 specifically addresses mitigation systems, these design defect likelihood reduction measures are equally applicable to safety initiators.

For non-safety initiators, a graded approach can be applied to reach this same conclusion; compliance to the criteria for safety systems is not required. This graded approach must address both the digital platform as well as the application.

A structured life cycle process conducted by commercial equipment suppliers can be credited, when the life cycle process is documented to address the same concerns (e.g., complete requirements, configuration control, and implementation verification) and includes demonstration of high quality design process results. This type of robust life cycle process is common for commercial equipment that is certified to industrial standards such as ISO 9001 [40]. When the design process conducted by the

equipment supplier is inadequate, it can be supplemented by additional quality activities conducted by the end-user.

In crediting this graded approach, a structured life cycle process is also needed at the application level. Different design errors in diverse applications will not cause a CCF of multiple applications; therefore, within the context of CCF this structured life cycle process is not needed to reduce the likelihood of an application design error (although it certainly does that). Instead, a structured life cycle process that includes comprehensive system level testing, where the application and platform are fully integrated, is credited to reduce the likelihood of a common platform level design error that could adversely affect multiple diverse applications.

As discussed in Section 3.1.6, it is important to note that reducing the likelihood of a design defect does not preclude further consideration of a CCF; it only allows that CCF to be analyzed as a beyond design basis event. Simplicity, as discussed on Section 3.1.6, is a CCF preventive measure; but both safety and non-safety control systems are typically quite complex, therefore achieving 100% testing is not practical for more most safety or non-safety initiators. Diversity of digital platforms is also a CCF preventive measure; but diverse digital platforms are much more difficult to interconnect to achieve advanced performance algorithms and integrated human systems interfaces. Diverse digital platforms also preclude the cost savings achieved through plant wide standardization.

Therefore, the only practical preventive measure for safety or non-safety initiators is application level diversity, which facilitates non-concurrent triggers, as discussed in Section 2.4.4. Digital qualification to address application level diversity is discussed in Section 4.1.3 and additional INL research is described in Section 5.2.2.

3.2.7 Setpoint Errors

A potential CCF due to a design defect setpoint error, as described in Section 3.1.7 for mitigation systems, is also applicable to initiating systems.

Section 3.2.5 describes multiple coordinated control functions that employ the same measurement channel(s). But even control functions that employ different measurement channels may be functionally coordinated by their control setpoints. These coordinated control functions are modeled in current transient analysis, based on their analytical setpoints.

AOOs typically consider single control function failures, but not multiple control function failures, that could be the result of errors when calculating measurement channel uncertainties to determine actual installed setpoints in controllers. Multiple setpoint errors could occur due to a common design process error, when determining these uncertainties.

While RG 1.105 “Setpoints for Safety-Related Instrumentation” establishes design process requirements for safety mitigation system setpoints, it can and is often used to establish setpoints for safety and non-safety control systems (i.e., initiators). A graded approach to independent review is commonly applied. These requirements are preventive measures that ensure a CCF due to a setpoint error in multiple safety or non-safety control functions requires no further consideration.

3.2.8 Security Threats

RG 5.71 “Cyber Security Programs for Nuclear Facilities” [41] address “physical protection programs” to defend against cyber security threats. While NRC’s internal policy does not allow cyber threats to be identified as a potential source of CCF, these threats could adversely affect multiple safety divisions and multiple separate non-safety or safety control functions. Despite this NRC policy, compliance to RG 5.71 is a preventive measure that ensures a CCF due to a cyber security threat requires no further consideration for non-safety systems. RG 5.71 provides a graded approach for non-safety systems that is essentially equivalent to RG 1.152 [35].

3.2.9 Hidden Random Hardware Failures

Mitigation systems normally operate in a standby mode; therefore, periodic testing is required to prevent multiple division failures due to the accumulation of independent hidden random failures. Initiating systems do not require periodic testing, because they operate continuously; therefore, failures are self-announcing by the resulting plant transients or plant component performance anomalies. Therefore, the concurrent failure of multiple separate safety or non-safety control functions, due to the accumulation of hidden random hardware failures, requires no further consideration.

It is noted that there are also some non-safety systems that operate in a standby mode. These would include the quick opening portions of the turbine/steam bypass control system (at most plants) and the reactor power cutback system (at several Combustion Engineering plants). While these non-safety systems provide mitigation functions that lessen the severity of some plant transients, those mitigation functions are not credited in the plants TAA. Therefore, periodic testing to prevent a CCF due to hidden random failures is not required; although some plants conduct this periodic testing to improve the availability of these systems.

What is typically more important for these non-safety mitigation systems is to prevent failures that can result in erroneous actuations that are different than the erroneous actuations analyzed in the TAA. For example, the TAA may consider spurious actuation of one turbine bypass valve at full power, not a CCF that results in spurious actuation of multiple turbine bypass valves. All potential failure sources in this section must be examined to prevent these unanalyzed CCF conditions.

3.3 Software Quality

Of all the defensive measures discussed above, software quality is one that tends to be misunderstood, especially in the discussion of its applicability to non-safety systems. The key points of that defensive measure are summarized in this section.

Most digital designs are inherently complex; therefore, it is very difficult to demonstrate that there is no design defect that could lead to a CCF. One commonly applied CCF likelihood reduction measure is a robust digital design process. A robust digital design process reduces the likelihood of a design defect, which inherently reduces the likelihood of a CCF due to a design defect.

The digital design process is highly regulated for safety systems, including requirements for life cycle documentation that includes requirements traceability, independent verification and validation and strict configuration controls. For safety systems, the NRC has accepted that when a robust design process is applied that conforms to regulatory guidance, the likelihood of a safety division failure due to a design defect is significantly lower than the likelihood of a safety division failure due to a single random hardware failure. This establishes the regulatory basis for treating a potential CCF of multiple safety divisions, due to a design defect, as a beyond design basis event. Although there are no regulatory criteria that specifically addresses a CCF of multiple control functions in the same safety division, the same regulatory precedence would apply.

Non-safety systems do not have the same highly regulated design process as for safety systems. However, there is considerable precedence for applying a graded approach to non-safety systems that is based on the regulatory criteria established for safety systems. For example, non-safety systems that can challenge plant safety or availability are commonly tested to EMI criteria that is comparable to the criteria applied to safety systems. Similarly, non-safety systems that can challenge plant safety or availability commonly have software quality assurance and life cycle programs that include verification and validation, although not with the same rigor and personnel independence as for safety systems.

Using this graded precedence, when a robust design process is applied to a non-safety system that conforms to sound commercial practices, the likelihood of a non-safety system failure due to a design defect is significantly lower than the likelihood of a non-safety system failure due to a single random

hardware failure. This establishes the basis for treating a potential CCF from single or multiple non-safety controllers, due to a design defect, as a beyond design basis event.

It is important to understand that the beyond design basis conclusion discussed above applies only to a CCF due to a design defect. If there are other sources of CCF, such as a shared controller, or interconnected controllers, each source of CCF must be addressed separately.

3.4 Plant Level Analysis

The method and acceptance criteria for the plant level analysis of malfunctions depends on the likelihood of the CCF source. The plant conditions for which the CCF is analyzed depend on the type of system affected by the CCF (i.e., an initiator or mitigator). Both of these issues are addressed in the following sections.

These sections use the term “bounded”. The NRC has never defined “bounded”. In the context of this report, a new event is bounded by previously analyzed events, if the margin to the key critical safety function(s) that is challenged by the event, as identified in the TAA, is maintained or insignificantly degraded.

The SRP establishes analysis methods and acceptance criteria for design basis events. BTP 7-19 establishes analysis methods and acceptance criteria for beyond design basis digital CCFs. Descriptions in this section are based on the NRC positions taken for many ALWR reviews, through the design certification process under 10CFR52 [42]. The technical basis of these positions is equally applicable to plants licensed under 10CFR50 [43], and was applied by NRC to the review of the Oconee Reactor Protection System digital upgrade.

Two key points of this precedence are:

1. For a CCF that is from a source that is significantly less likely than a CCF from a random hardware failure, “best estimate” analysis methods may be used.
2. If the CCF affects a mitigator, all AOOs and PAs in the TAA must be reanalyzed concurrent with that mitigator failure. In this regard, a loss of offsite power (LOOP) is one of the AOOs that must be analyzed; but a LOOP does not require consideration concurrent with other AOOs or PAs.

The technical basis for this regulatory precedence is described in the following sections.

3.4.1 Likelihood Effect on Analysis Methods and Acceptance Criteria

CCFs that are within the design basis require more conservative analysis methods and acceptance criteria than CCFs that are beyond design basis. The basis for this is that CCFs that are within the design basis are expected during the life of the plant; CCFs that are outside the design basis are not expected but have potentially adverse consequences that should be managed.

It is important to note that design basis and beyond design basis events are both within the plant’s licensing basis; therefore, they are evaluated using deterministic analysis methods. Events that are outside the plant’s licensing basis, such as a seismic event that exceeds the equipment qualification envelope, are considered only in the PRA to determine the potential CDF and LERF.

It is also important to note that for either design basis or beyond design basis CCFs, manual actions can be credited for mitigation with an evaluation that demonstrates margin between the time available to take the manual action as determined by a thermal hydraulic assessment, and the time required to take the action as determined by a human factors engineering assessment.

3.4.1.1 *Design Basis CCFs.*

If a credible CCF is in the design basis (e.g., a CCF due to a random failure of a shared hardware resource), the following analysis methods and acceptance criteria are applied:

- Design basis methods and acceptance criteria, as currently used in the AOOs and PAs of the Final Safety Analysis Report (FSAR). This is typically a quantitative analysis using computer codes.
- Mitigating systems must be safety related.
- A concurrent failure of one safety division is assumed. Normal automatic control system actions that may lessen the adverse effect of the event cannot be credited. Normal automatic control system actions that worsen the adverse effect of the event are considered concurrent with the AOO or PA.
- The analysis demonstrates that the malfunction does not cause a new type of accident and the plant level result of the malfunction is bounded by AOOs previously analyzed in the plant's TAA. The analysis cannot use PA bounding criteria, because a design basis CCF is an AOO.
- For a new or unbounded AOO, the analysis uses the same AOO acceptance criteria as in the TAA (e.g., primary and secondary pressure boundary limits, minimum DNBR to maintain fuel cladding integrity).
- This new AOO is added to the TAA because it is within the design basis.

3.4.1.2 *Beyond Design Basis CCFs.*

If a credible CCF is beyond design basis (e.g., a CCF due to a design defect, for a system with a robust design process), the following analysis methods and acceptance criteria are applied:

- Design basis or best estimate methods. Best estimate methods employ realistic or nominal initial plant conditions and equipment performance. Best estimate methods allow conclusions based on qualitative expert judgment or quantitative analysis.
- Mitigating systems can be safety or non-safety. Non-safety systems that operate in a standby mode (e.g., DAS) must have augmented quality and periodic testing. Non-safety systems in continuous operation do not require augmented quality because their failure is self-announcing.
- No other assumed equipment failures. Normal automatic control system actions that may lessen the adverse effect of the event can be credited.
- The analysis demonstrates that the malfunction does not cause a new type of accident and the plant level result of the malfunction is bounded by AOOs or PAs previously analyzed in the plant's TAA.
- For a new or unbounded accident, the analysis uses the same AOO or PA acceptance criteria as in the TAA, or the following acceptance criteria:
  - coolable core geometry,
  - containment integrity, and
  - releases do not exceed the 10CFR100 limits
- This new accident is not added to the TAA, because it is beyond design basis.

The thermal hydraulic analyses performed as part of the PRA typically provide useful input to the deterministic analysis of beyond design basis CCFs.

3.4.2 System Effect on Plant Conditions to Be Analyzed

CCFs in systems credited to mitigate plant events are analyzed with different concurrent plant conditions than CCFs in systems that can initiate a plant transient, because a CCF in a mitigating system can remain hidden.

3.4.2.1 Event Initiators. CCFs in systems that initiate plant transients (e.g., malfunctions due to a control system CCF) are analyzed with no other coincident event (e.g., no other AOO or PA) and no other CCF (e.g., no unrelated CCF in a safety system).

The basis is that these CCFs are self-announcing due to the resulting plant transient, alarms or component state changes; therefore, they can be mitigated prior to any other plant event. Put another way, if a control system CCF is self-announcing, then there is no need to consider a control system CCF coincident with each AOO or PA or another CCF, because the CCF would be detected and corrected before an unrelated AOO, PA, or digital CCF would occur.

There is the potential for a CCF in an event initiator that may result in a fail as-is condition with no alarms, which is not immediately self-announcing. For example, this could occur in steam or feedwater bypass valves that are normally not repositioned during stable plant operation. Even though this CCF is not immediately self-announcing, this CCF would be revealed when there is a change in plant power or operating mode. Although this CCF could coexist at the time of an AOO or PA, these systems are not credited for event mitigation and a fail as-is condition would not complicate that mitigation.

3.4.2.2 Event Mitigators. CCFs in systems that are credited for event mitigation (e.g., malfunctions due to a safety system CCF) are analyzed coincident with each AOO and PA. The basis is that these CCFs are not self-announcing; therefore, they can remain hidden and coexist at the time of an unrelated AOO or PA.

However, a beyond design basis CCF is not analyzed coincident with each AOO and PA, and with a concurrent loss of offsite power (LOOP). The basis is that since all current US plants have two independent grid connections, a LOOP is a CCF, and the low likelihood of two unrelated CCFs (i.e., LOOP and digital), including a digital CCF that is beyond design basis (i.e., not expected during the life of the plant), does not require further consideration. However, a LOOP by itself is an AOO, therefore a LOOP alone with concurrent beyond design basis digital CCF is analyzed.

This non-concurrent LOOP analysis position does not apply to a design basis CCF, because a design basis CCF would be expected during the life of the plant.

Similarly, a beyond design basis digital CCF is not analyzed coincident with an SBO, because an SBO is a beyond design basis CCF, and the extremely low likelihood of two unrelated CCFs (i.e., SBO and digital), including both that are beyond design basis (i.e., not expected during the life of the plant), does not require further consideration.

4. CURRENT METHODS FOR ADDRESSING DIGITAL CCF

Most digital CCF sources are well understood and corresponding defensive measures are available from multiple digital equipment suppliers. This section describes digital CCF sources that are not as well understood, and corresponding defensive measures that are not always applied as effectively as they could be.

4.1 Digital CCF Due to a Single Random Hardware Failure

CCFs are most commonly associated with a design defect. But as explained in Section 2.2 and shown through the examples in Section 2.3.1, CCFs can also be caused by a single random hardware failure.

Digital systems are especially susceptible to active component failures (i.e., single malfunctions) that can lead to unanalyzed plant conditions, due to the ease at which different control functions can be integrated within the same controller. This inherent capability makes that controller susceptible to internal single random hardware failures that can adversely affect the multiple functions that it controls (i.e., a CCF). Defensive measures to manage these CCFs are discussed in the following sections.

4.1.1 Segmentation

Segmenting (or distributing) control functions into different controllers can prevent these potential CCFs, and it is certainly the easiest defensive measure to defend with regulators. But segmenting functions to the same extent that they were separated in analog implementations is not cost effective; in addition, when more controllers are employed the mean-time-between-failure (MTBF) for the aggregate of controllers decreases on an exponential scale (e.g., the MTBF of four controllers is one-fourth that of one controller).

Therefore, digital implementations typically segment control functions only to the extent that the effect of a single random hardware failure is limited to fewer components/functions. This does not prevent a CCF, rather it limits the CCF to make it easier to analyze. Where possible, limiting the CCF may result in a plant transient that is bounded by previous transients in the TAA; bounding is discussed in more detail in Section 3.4.

Segmentation is a well understood defensive measure but achieving sufficient segmentation is not always practical. Some examples:

1. In a digital reactor protection system (RPS), one controller will typically provide all ESF functions, because segmenting each function into separate controllers adds cost and unreliability, as discussed above, and it also increases the periodic testing burden. This lack of segmentation makes that single controller susceptible to a random hardware failure that could spuriously actuate all ESF functions. Even if this event can be shown to not threaten plant safety, it poses a substantial economic burden for the plant.
2. A DAS controller that includes several diverse ESF functions poses the same problem. The DAS is intended to mitigate a CCF that results in no actuation of the RPS; but the DAS itself presents new potential CCF sources that can lead to multiple spurious ESF actuations that are also quite onerous.
3. There are numerous control rods in a nuclear reactor (more than 90 in some reactors). Sufficient segmentation to ensure there is only the potential for a single erroneous control rod withdrawal, as analyzed in most TAAs, is not practical.

To address these situations, additional defensive measures discussed below regarding their use and effectiveness.

4.1.2 Output Compare Function – One Controller

The self-diagnostic functions in most digital controllers run in each scan cycle of the controller. Therefore, they are sufficient to detect most hardware failures and shutdown the controller, before erroneous signals can be generated. This does not prevent a CCF, but it limits the CCF to a known controller output state (e.g., fail-off) that can be analyzed with relative ease.

However, due to the large size of controller memory, complete memory self-diagnostics typically requires numerous scan cycles, which can take several minutes to complete. Therefore, there is the potential that a failed memory byte, or a failure that affects multiple memory bytes, could result in a failure of one or more function blocks (e.g., AND gate, LATCH, TIMER, BISTABLE, PID block) that are used by multiple control functions. This could result in spurious actuation or erroneous control commands for multiple functions from the same controller. Analyzing this CCF requires a failures modes and effects analysis (FMEA) that examines the multiple use of every function block; this can be quite onerous and the results are likely to be unacceptable.

Alternately, this CCF can be limited or prevented by employing diverse application logic and then using the receiver of the signals to compare the logic outputs. If the logic outputs differ, the receiver can hold the last good output state. This is referred to as an output compare function (OCF).

OCF can limit or prevent a CCF depending on how the diverse application logic is implemented. It can be implemented in the same controller, using either of the following methods:

1. Different standard function blocks can be employed to implement the same logic functions. For example, for ESF actuation voting, a standard 2oo4 function block can be used for one of the two diverse voting methods, and a combination of standard discrete logic function blocks (e.g., AND/OR gates) can be used to create the second diverse voting method. Similarly, to implement diverse time delays, on-delay timers can be used for one of the two diverse methods and inverted signals with off-delay timers can be used for the second diverse method. This utilization of different standard function blocks ensures that a single failure (e.g., memory byte failure) that causes a standard function block to generate an erroneous output, cannot cause spurious actuation or an erroneous control command in both signal paths of the diverse application logic.
2. Another diversity method is to use two separate sets of logic blocks that are functionally identical, however they reside in different memory areas. Therefore, a single memory block failure will not affect both diverse signal processing paths. This method is not commonly available in most digital controllers.

Either of the two diverse signal processing methods above are intended to compensate for the delay in the digital controllers self-testing to detect a memory error, due to the large size of controller memory. When the outputs of the two diverse signal processing paths do not match, the receiver holds the last matched control signal; thereby, preventing erroneous control actions. When the self-testing eventually detects the memory error, the controller will shut down. This leaves the receiver(s) in its current state (i.e., fail as-is) or a predetermined failure state (e.g., fail-off). Either failure mode limits the CCF to facilitate simpler analysis and/or a more favorable analysis outcome (e.g., a bounded malfunction result).

4.1.3 Output Compare Function – Redundant Controller

An alternative to the diverse signal processing described above, which is intended to prevent a CCF of multiple control functions due to erroneous control actions, is to provide two redundant controllers with the outputs of both sent to each receiver which performs the OCF. When both controllers are operating, both controllers send normal digital data communication to the controllers' output modules and/or to other controllers. The OCF is implemented by each receiver; it compares the outputs from both redundant controllers and only propagates state changes when both controller signals match. If there is a mismatch, the receiver retains the last good matched value. This ensures there are no plant component state changes due to erroneous signals from a single controller.

On the surface, the OCF would appear to limit the CCF to a fail as-is condition, but not prevent a CCF. However, eventually the controller's self-diagnostics will detect the failed memory and force a shutdown of the failed controller. This allows the control function to continue operating, based on the outputs of the one operable controller alone, with no CCF.

Similarly, the OCF appears to degrade control function availability, because the OCF essentially creates a 2-out-of-2 logic function for the redundant controller outputs. However, this availability degradation is avoided by automatic bypass of the OCF. When one controller of a redundant pair shuts down due to a self-detected failure, all digital data communication receivers will recognize the failed controller by a stagnant digital data communication interface. The receivers will then automatically bypass the OCF to receive signals from the one remaining operable controller. Therefore, the OCF prevents erroneous control signals, but allows the control system availability to benefit from the redundant controller configuration.

When operating in a single controller configuration (i.e., after an automatic OCF bypass), an additional failure in the one operating controller could result in erroneous control signals, with no OCF protection. Therefore, the duration of plant operation in this configuration is restricted through administrative controls, such as a plant Technical Specification limiting condition of operation. However,

the completion time for this administrative control is expected to be quite long, due to the high MTBF of modern digital controllers, and the continuous self-diagnostics which will shut down the controller for most failures, before erroneous control signals can be generated.

Due to the OCF that prevents spurious control actions during normal redundant controller operation, and the administrative controls, which restrict operating time in a non-redundant controller configuration, a CCF due to a random hardware failure within the controller requires no further consideration.

However, it is important to note that the OCF cannot preclude multiple spurious actuations from a redundant controller due to a digital design defect, because that defect would exist in both redundant controllers, therefore an OCF mismatch would not occur. Therefore, the transients that can result from multiple erroneous control actions due to a digital design defect in a redundant controller, with a robust design process, are evaluated as a beyond design basis event. A beyond design basis analysis is appropriate because these transients are significantly less likely than transients due to a single random hardware failure.

4.2 Digital CCF Due to a Design Defect

A digital CCF due to a digital design defect is the most difficult to prevent. The following sections discuss preventive measures that are identified in BTP 7-19 [33].

A common interpretation of SECY 93-087 [32] is that due to the potential for a digital design defect, a CCF of multiple safety divisions must be assumed, then analyzed concurrent with each AOO and PA in the TAA to demonstrate adequate mitigation. The analysis methods are described in Sections 3.4.1.2 and 3.4.2.2. Even though "best estimate" methods are permitted, this analysis can be quite burdensome due to the number of events that require reanalysis with a concurrent CCF. History has shown that even with "best estimate" methods, for most plants, a backup DAS is needed to successfully mitigate some events. But BTP 7-19 clarified that no further consideration of a CCF due to a design defect is needed if the protection system has the design attributes of "sufficiently simple" or "sufficient diversity". But "sufficient" is quite subjective; therefore, industry has been unable to find a practical approach to meeting either of these criteria.

But since simplicity and diversity are key attributes of defensive measures accepted by NRC to prevent a CCF due to a design defect, practical methods of meeting each of these CCF preventive measures is discussed in the sections below. Each of these CCF preventive measures is discussed in the sections below.

4.2.1 Diversity

BTP 7-19 states:

> *"If sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action."*

BTP 7-19 gives one example of "sufficient diversity": "An RPS 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." This is more commonly known as digital platform diversity. Digital platform diversity prevents a CCF due to a common design defect in the platform itself.

In addition, platform diversity inherently leads to diverse application development tools, which facilitates preventing a design defect in the application implementation. Of course, actually preventing an application level design defect also requires different implementation teams that are working from diverse functional requirements. Alternately, common functional requirements can be employed with a robust development process that ensures there is no flaw in those functional requirements.

But BTP 7-19 does not require platform diversity. It goes on to say:

"What constitutes "sufficient diversity" should be evaluated on a case-by-case basis, considering diversity attributes and attribute criteria that preclude or limit certain types of CCF. Diversity attributes and associated attribute criteria, and a process for evaluating the application may provide more objective guidance in answering, "What is sufficient diversity?"."

This is the basis of the defensive measure described in Section 2.4.4, which credits application level diversity to prevent concurrent triggers, and thereby, in conjunction with self-announcing and corrective actions, prevents a CCF due to a hidden design defect in the digital platform itself.

Westinghouse credited this basis in their Watts Bar Unit 2 Segmentation Analysis, which is referenced in the NRC's Safety Evaluation Report for this project, NUREG-0847 Supplement 23 [44]:

"The following design and implementation strategies provide reasonable assurance of adequate protection against a common cause failure affecting multiple processor pairs:

• defensive design techniques including multiple processor pairs running asynchronously with different application software…"

A potential research project on this preventive measure is to demonstrate that application level differences even on the same platform are sufficient to prevent concurrent triggers of an unknown digital defect. Such a project is described in Section 5.2

4.2.2 Testability

Section 1.9 of BTP 7-19 defines testability as follows:

Testability – A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case (100% tested).

In practice this would likely be achievable only for digital devices that have very few inputs and very few internal state-based functions. Indeed, this approach has been considered as a means of addressing potential CCF concerns in at least one industry digital modification, but was found to be impractical due to the high number of combinations of inputs and sequences of device states.

Section 3.9 of BTP 7-19 goes on to invoke the guidance of IEEE Std. 7-4.3.2-2003 [45], Clause 5.4.1, Computer system [equipment qualification] testing, as follows:

Computer system [equipment] qualification testing shall be performed with the computer functioning with software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish safety functions, or those portions whose operation or failure could impair safety functions, shall be exercised during testing. This includes, as appropriate, exercising and monitoring the memory, the CPU, inputs and outputs, display functions, diagnostics, associated components, communication paths, and interfaces. Testing shall demonstrate that the performance requirements related to safety functions have been met.

The emphasis here is on ensuring that safety functions are met, recognizing that there are typically other on-board functions that are not necessary to accomplish the safety functions, such as diagnostics and event logging. Therefore, testing must include all portions of the computer system necessary for the safety functions and all other portions of the computer system that could potentially impair the safety functions. BTP 7-19 also extends these requirements to "all components of a safety system relying upon a software development system," thereby invoking the same requirements for firmware digital devices.

There are no established methods at this time for applying testability to eliminate consideration of CCF in digital devices used in the nuclear industry. This has been the subject of several research projects, including model-based testing, and additional potential research is described in Section 5.2.

5. NEW POTENTIAL DIGITAL QUALIFICATION METHODS

Based on the discussion above, two new qualification methods are proposed for further research and development as means of filling gaps in the current options for dealing with digital CCF.

5.1 Elimination of CCF Triggers

As described in Section 4.2.1, BTP 7-19 requires no further consideration of a CCF due to a design defect for digital components that have "sufficient diversity". While this has been historically interpreted to mean different digital platforms, platform diversity is not a BTP 7-19 requirement.

Sufficient diversity, without a diverse digital platform is the basis of Strategy D Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, NUREG/CR-7007, ORNL/TM-2009/302 [46]. This is a strategy to employ a common digital platform, but apply "sufficient diversity" at the application layer to avoid a concurrent trigger for a design defect in the digital platform layer.

Sufficient diversity, without a diverse digital platform is also the basis of NRC's approval of the Watts Bar distributed control system, described in Section 4.2.2. In both of these cases common digital platforms are employed, which may have a hidden design defect, but other diversities are credited to ensure concurrent triggers are avoided that could lead to a CCF.

As discussed in Section 2.4.4, when non-concurrent triggers are coupled with self-announcing that a defect has been triggered in one digital device, a CCF of multiple digital devices can be avoided.

Additional research is proposed that will provide guidance for the following key "sufficient diversity" issues to enable the use of a common digital platform:

1. What application level differences are necessary to constitute "sufficient diversity"? As a minimum, this guidance will consider:
    a. Application program functions and memory load
    b. Input quantity and configuration
    c. Output quantity and configuration
    d. Digital data communication quantity and configuration
    e. Cycle times, task scheduling and central processing unit (CPU) load
    f. Dynamic or different static memory allocation
2. What features are necessary to ensure a triggered defect is self-announcing? As a minimum, this guidance will consider:
    a. Continuous control applications (typical of reactor control systems) vs. standby control applications (typical of safety mitigation systems)
    b. Watchdog timers that detect both underrun and overrun conditions
    c. Exception handlers, such as buffer overflow detection, divide-by-zero, not-a-number

In essence, the recommended future research will build upon the concept of Strategy D discussed in the Oak Ridge National Laboratory (ORNL) Diversity Strategies report.

5.2 Testability

One such method that would be useful in qualifying field components such as sensors and actuators is the concept of testability, these types of components being relatively simple in function compared to large integrated control systems. The issue with these types of field devices is that they are typically used in redundant channels for protection systems. Moreover, the same device, such as a pressure transmitter, can be used in different measurements such as pressure, flow, and level.

If redundant or even different channels use devices of the same manufacturer make and model number, as is typically the case, there would be no diversity in this set of instruments relative to CCF susceptibility and it is conceivable that a digital defect would simultaneously affect all channels and cause the design function to fail, in spite of the redundancy. For highly safety-significant instrumentation, the results of the regulatory-required diversity analysis could be to require an instrument signal diverse from these instruments to cope with a CCF as described in a DOE research report entitled Digital Sensor Technology [47].

However, nuclear plant designers want to minimize the number of devices used in redundant channels in order to achieve similarity of operating characteristics and to minimize engineering and maintenance expenses such as development of additional calculations and procedures, calibration training, and stocking of spare parts and test equipment.

The predecessor analog components were not subject to the diversity requirements as the digital replacements are. For this reason, sensor and actuator device manufacturers typically do not qualify their devices for safety-related usage, due to the digital qualification problem and in particular, CCF.

As stated in Section 4.2.2, this qualification method has never proven to be practical in view of the very large number of combinations of inputs and sequences of device states even for a small digital device. However, many of these combinations are not unique in the sense that they represent the same state space or in that that they represent state space that would not affect the critical design basis functions of the device. On this basis, the state space of interest might possibly be reduced to a manageable dimension through such analysis.

This research would focus on a representative digital device similar in design, function, and complexity to the types of devices that would likely be deployed in nuclear power plants as sensors and actuators. Analysis will first be conducted to determine the feasibility of testing this device in a manner consistent with the NRC definition. Additional analysis will determine an acceptable test method, needed tools (existing or new), and computing resources, all based on engineering and computer science principles. This information will then be used to develop a test specification for I&C device testability that can be used in a future phase of this project to demonstrate digital qualification with respect to common cause failure.

It should be noted that there is no assurance that testability will prove to be a viable qualification method for digital I&C devices. This determination is in fact the first objective of this research project. However, if it proves to be feasible and practical to implement (cost and effort), it would represent a valuable method for qualifying a large population of digital devices for use in safety-related applications for nuclear power plants.

The research should conduct the following activities:

1. Perform an analysis of a representative I&C device a specification for determining the state space that must be analyzed, methods and tools for reducing that state space, methods and resources needed to run the tests, and development of an evidence case to eliminate consideration of CCF.
2. Develop a specification for testability of the representative I&C device that is sufficient to eliminate consideration of CCF.

3. Conduct testing of the representative device in accordance with requirements of the specification.
4. Develop an evidence case to eliminate consideration of a CCF for the representative device.
5. Develop generic guidance for conducting similar testing to qualify such devices such that consideration of CCF is eliminated in accordance with the guidance in BTP 7-19.

6. STRATEGY FOR FULL NUCLEAR PLANT MODERNIZATION

Safety-related digital I&C upgrades are vital for the long-term safe and continued operation of the nation's nuclear power plants. Developing and demonstrating an effective and efficient path forward for licensing and deployment of digital I&C has been elusive thus far. This has resulted in digital I&C upgrade projects at commercial nuclear power plants costing substantially more than expected, taking longer to perform, and has had a chilling effect on modernization and investments of this type in commercial nuclear power plants.

Technical qualification of safety-related I&C system modifications is one aspect of a complex and interrelated set of issues that must be addressed for nuclear utilities to move forward with modernization. Other issues include the defining the end-state digital architecture, developing the business case for implementation, addressing licensing process burden, technical and developing implementation schedules compatible with short refueling outages.

And though this report is largely focused on qualification of safety-related digital I&C, the strategy must be broad enough to address all beneficial digital deployment for nuclear plants. For this reason, it is referred to as a strategy for full nuclear plant modernization. The business case for plant modernization will not stand on safety-related system upgrades alone. There are far more plant I&C systems that are non-safety related and they represent even greater potential cost reductions. Likewise, there are other digital technologies that enable efficient support of the nuclear plants and these must be integrated in a manner that supports needed data sharing. It will take the cost-savings contributions of all of these technologies together to enable the level of work elimination and staffing level reduction to ensure that the nuclear plants are competitive with other forms of electric generation in the coming decades. The strategy must therefore support the coordinated implementation of all of these technologies to result in a technology-based operating model.

Working under the DOE Light Water Reactor Sustainability Program – Plant Modernization Pathway, INL has partnered with the Nuclear Energy Institute (NEI), the Electric Power Research Institute (EPRI) and Exelon Nuclear to define the elements of this strategy. This effort began in July of 2017 with direct discussions between Exelon and the Pathway on potential collaboration for full plant modernization. This was followed by a two-day working meeting held at Exelon Nuclear corporate offices in Warrenville, IL on November 8-9, 2017, with INL, NEI, EPRI, and invited consulting firms participating. One of these firms, Nuclear Automation Engineering, presented a highly-integrated digital I&C architecture referred to as a “compact digital modernization” architecture and it is presented in Section 6.2.1. A direction was set in this meeting to pursue full plant modernization assuming that technical, business case, and regulatory issues can be successfully resolved. It was further decided that, based on the urgency to reduce substantially operating costs, the modernization would be implemented in a single step (future extended outage) in the reasonable near term rather than as an evolutionary implementation over a 10-15 year time frame.

On December 7, 2017, DOE announced an industry funding opportunity DE-FOA-0001817, U.S. Industry Opportunities for Advanced Nuclear Technology Development. One of the industry application pathways was for First of a Kind Nuclear Demonstration Readiness Projects. On this basis, these collaborating organizations decided to submit an application for funding of this modernization strategy, with EPRI as the lead organization for the submittal and INL serving as a sub-recipient. Weekly phone calls to develop the proposal were held from mid-December though January of 2018, with a two-day working meeting held at EPRI in Charlotte, NC, on January 9-10. The results of this planning meeting were that INL and Exelon would have the role of for defining the end-state architecture, NEI would have the role for regulatory strategy, and EPRI would have the role for the business case and the implementation plan.

Exelon would provide support these other main activities as well. The application was submitted to DOE at the end of January.

In April of 2018, it was announced that this plant modernization application was not successful in regard to award of funding. Nevertheless, the industry decided to continue to pursue the full nuclear plant modernization strategy due to the pressing needs to lower operating costs for the nuclear fleet. At the time of this report writing, discussions are underway among these same collaborating organizations to determine a means to pursue a modernization strategy based largely on digital technologies.

Along with these efforts, the Nuclear Regulatory Commission (NRC) has been working for several years working under an Integrated Action Plan (IAP) [1] to modernize the digital I&C regulatory infrastructure as a means of addressing regulatory barriers for digital upgrades. NEI has sponsored a Digital I&C Working Group with industry participation to work with the NRC on finding mutually-agreeable solutions to the perceived barriers for digital I&C implementation, and in particular safety-related I&C systems. This addresses such topics as what digital upgrades the licensees can do under 10 CFR 50.59 in lieu of license amendments, treatment of CCF, streamlining of the digital license amendment process, and ultimately a potential simplification of the entire digital I&C regulatory infrastructure (including digital regulatory guidance).

Based on prospects for success in both the industry collaboration and the NRC efforts, some nuclear utilities are now expressing interest in moving forward with safety-related digital I&C modifications under the assumption that these regulatory barriers can be satisfactorily resolved within a reasonable time frame. The new potential qualification methods recommended Section 5 of this report could perhaps make this even more attractive if they prove to be successful.

The following sections present a strategy for full nuclear plant modernization that is based on the elements that were defined in the recent effort and is now offered as basis for beginning the detailed planning and initiation of activities to pursue full modernization of a first-mover nuclear plant.

6.1 General Approach

Full modernization of the operating nuclear fleet will require a broad coalition of organizations including nuclear operating utilities, the major industry support groups of EPRI, NEI, and the Institute of Nuclear Power Operations (INPO), major technology suppliers, nuclear industry consulting firms including nuclear-experienced architect/engineer firms, DOE national laboratories, and other research organizations including academia.

It is recommended that a formal agreement be put in place that defines roles and responsibilities, as well as needed terms and conditions such as the protection of intellectual property and rights in project results. The agreement might provide for two levels of participation – those directly engaged in research and/or other development activities for products that enable full plant modernization and the first mover nuclear plants, and organizations, including other nuclear operating companies, that desire to participate in advisory roles, providing additional requirements and related technical information to enable the application of the modernization strategy across the entire U.S. operating nuclear fleet. Project funding of all types would also be specified in the agreement, including contributions, cost-sharing, in-kind contributions, and other forms of resource commitments. Funding would be commensurate with the roles and benefits of the participating organizations.

The NRC will of course be in an independent role of licensing and regulatory compliance oversight, where applicable to the modernization activities.

6.1.1 Execution Team

A project management structure and governing controls would be specified in the agreement. A recommended structure for a project execution team would include an Executive Steering Team, a Technical Steering Team, and three parallel Domain Technical Teams to work on three major domains of nuclear plant modernization of:

1. Digital I&C Systems
2. On-line Monitoring
3. Mobile Worker/Process Efficiency Technology

New or existing industry advisory groups may be named to participate at either the Executive Steering Team or Technical Steering Team level as needed to provide independent review of key decisions.

Each of the Domain Technical Teams will develop the four elements of the strategy within their respective domains as follows.

1. End-State Architecture
2. Cost-Benefit Analysis (Business Case)
3. Regulatory Approach
4. Implementation Plan

The Domain Technical Teams will also be responsible for integrating their respective results in each of the four elements into a comprehensive detailed plan for plant modernization, under the direction and oversight of the Technical Steering Team. These teams would also be matrixed to comparable teams within the first-mover utilities to assist them with company level planning for the modernization activities.

6.1.2 End-State Architecture

End-State Architecture is a term used in this report to refer to the arrangement, capabilities, and interconnectivity of digital technologies that are brought together to modernize one of the domains of a nuclear power plant. Even though control, protection, and monitoring requirements vary plant to plant, the architecture of these I&C systems is fairly consistent. Likewise, because nuclear plants have very similar organizations and work functions, it is reasonable that a generalized end-state architecture will have wide applicability throughout the industry. Obviously, these end-state architectures will have to be customized at some level for each site. But the generalized architecture should provide an economy of effort in the industry.

In the I&C systems area, consistent architectures could possibly enable development of standard design change packages, in which the development costs could be spread over a number of benefiting plants. There could be similar economies in the development of 10 CFR 50.59 [48] evaluation packages, procedures, work order models, and training modules. NRC reviews could be more streamlined with submittals based on standard design packages.

The I&C end-state architecture will also address the topic of control room modernization, including the interface of digital I&C systems along with the human factors engineering of improved control room functionality. This is expected to support reductions in operations staffing if fully exploited.

Standardization of the architectures for on-line monitoring and mobile worker/process efficiency technologies will result in savings as well. Suppliers will have fewer customized implementations to address and can possibly reduce prices through higher volume. Depending on the degree of standardization and use of open source applications and standards, many suppliers might be able to offer "plug and play" type applications with very little interface work.

The end-state architectures from each of the domains will be integrated into a comprehensive architecture that can be used for overall planning of the underlying plant and IT communication systems, processor requirements data storage requirements, cyber security requirements, and information display. This information will be the primary input in developing a seamless digital architecture for the plants as described in Section 6.5.

6.1.3 Cost-Benefit Analysis

Several benefit analyses have been undertaken in the LWRS Program for digital technologies, including mobile work packages, outage improvement, and control room modernization. These efforts were conducted to verify that there were substantial benefits in applying these technologies. They were completed using a tool developed in conjunction with ScottMadden Management Consultants, known as the Business Case Methodology for new nuclear plant digital technologies. This tool consists of a complex spreadsheet workbook that has a complete set of plant activities for which savings in eliminated work, savings in making work more efficient, and savings in non-labor expenses can be recorded against these activities in a manner that computes the aggregate savings for a typical nuclear plant.

The BCM leverages the fact that, in spite of what seems to be a wide and disparate array of work activities among a nuclear plant's operational and support organizations, the work activities themselves are largely composed of common tasks. For example, whether work activities are in Operations, Chemistry, Radiation Protection, or even Security, they have in common such tasks as pre-job briefs, use of procedures, correct component identification, emergent conditions requiring work package alteration, etc. It is at this task level that the technologies are applied, and therefore the benefits of the technologies can be realized across as many plant activities as can be identified to employ these tasks. In this manner, a much more comprehensive business case can be derived that greatly increases the benefit/cost ratio. This has the added benefit of driving consistency across the NPP organizations, which is a fundamental principle of successful NPP operational and safety management.

Three business case benefit analyses have been performed on technologies that are relevant to this modernization effort under the DOE Light Water Reactor Sustainability Program. These analyses are directly applicable to the cost-benefit analysis to be conducted under this element of the strategy. They are:

- Pilot Project Technology Business Case: Mobile Work Packages (INL/EXT-15-35327) [49]
- A Business Case for Advanced Outage Management (INL/EXT-16-38265) [50]
- A Business Case for Nuclear Plant Control Room Modernization (INL/EXT-16-39098) [51]

In addition, a more detailed analysis of full I&C and control room modernization was performed under the LWRS Program for the Palo Verde Generating Station in 2017, and a non-proprietary version of this information will be made available for use in the element of the strategy.

Finally, EPRI has conducted cost-benefit analyses of some parts of the plant modernization scope and it is assumed that these will be available to member utilities participating in the nuclear plant modernization efforts of the industry.

The quantification of benefits due to full I&C and control room modernization will need to be determined for the final end-state architecture specification as developed in the first element of this strategy. As mentioned previously, this can largely be an adaptation of the existing benefits analyses described in Section 6.2.1.

Similarly, quantification of benefits will need to be developed for the range of worker and process efficiency technologies, determining the cost reductions due to both eliminating work items and reducing the time and labor requirements for work items that remain. Also, there needs to be consideration of new technologies that displace human efforts such as RFIDs, in-line process instruments, computer vision, etc.

Not as much work has been done on quantifying the benefits of on-line monitoring. It is envisioned that the on-line monitoring function would be implemented as a centralized monitoring center. The scope of the business case will include the financial benefits early detection and avoided impacts of imminent component and structure failures, recovery of plant efficiency losses, and the offset of plant staffing labor costs to perform these functions. All avoided non-labor costs (parts, materials, contracts, replacement power, regulatory impacts, etc.) will be included. In addition, indirect benefits will be collected, such as reduced personnel dose, improved industry performance indicators, avoided regulatory perception issues, etc. The value of these benefits will be developed with station personnel such that they represent realistic and customary assessments of the impacts of these conditions and events had the monitoring center not assisted. The cost savings would be realized in three main ways: 1) early detection of imminent component failures that could evolve to plant transients, nuclear safety challenges, and lost generation, 2) identification of plant efficiency losses (e.g., steam leaks) that might otherwise go undetected, and 3) reduced labor costs for a CMP compared to current labor costs for in-plant monitoring functions.

For each of the three domains of digital technology, the costs to implement the technology must be determined. This includes both the acquisition cost of technology, in-house customization to reflect the standards and business practices of the nuclear operating company, and finally the direct deployment costs. In addition, the ongoing operating costs must be determined.

Based on both the expected costs and expected benefits for each of the digital technology domains, a standard cost-benefit analysis will be conducted using the BCM described in Section 6.2.1. It should be noted that this will produce only a cost-benefit analysis for the full nuclear plant modernization and will not compare the cost of maintaining the status quo (if possible). This comparison is highly company specific and would have to be done on an individual company basis.

6.1.4 Regulatory Approach

Many of the changes being implemented in other aspects of the full plant modernization, including the worker and process efficiency changes, as well as the on-line monitoring implementation, will not need license amendments and will likely screen out of the 10 CFR 50.59 [48] process.

It is expected that the highly-safety significant digital I&C upgrades will require NRC license amendments under 10 CFR 50.90 [52]. As described above, a number of regulatory improvements are being pursued to reduce the burden of the NRC license amendment review.

Care must be taken to evaluate and address all other programmatic aspects of the plant, such as might be described Technical Specifications (would require a license amendment) and the Updated Final Safety Analysis Report (UFSAR) (might require a license amendment), in particular the Appendix B Quality Assurance Program [21]. Some examples of changes that would need review for any possible regulatory impact would include:

- UFSAR Chapter 13 impacts for use of procedures and operations staffing.
- UFSAR Chapter 11 and 12 impacts on radiation protection functions and plant chemistry systems
- Appendix B Quality Assurance Program impacts on use of procedures and records archival.

- Possible interactions from on-line monitoring systems and new sensors with any aspects of the approved I&C design (cyber security, EMI/RFI, electrical separation, etc.)
- Possible interactions of wireless communication systems with the plant I&C systems and the cyber security program.

Each element of the modernization changes will need to be carefully reviewed for regulatory impacts. It is expected that standard industry guidance will be developed to conduct these reviews, perhaps under the direction and efforts of NEI.

6.1.5 Implementation Plan

As stated in Section 6 above, it is the consensus of the collaboration partners that a single step implementation plan for the major I&C systems would be the lowest cost and lowest risk option. This saves the expense of validating each incremental I&C configuration if done piecemeal. It also lowers the number of configurations that operators have to learn and become proficient. However, the acceptability of this depends on plant-specific circumstances on the duration of the outage and the amount of lost revenue.

The implementation of the on-line monitoring and mobile worker/plant efficiency technologies can proceed on a more continuous implementation path, most of which would occur during at-power operations.

A generic timeline will be developed that shows the overall duration of full end-state architecture implementation and the relative implementation time frames of the major components of I&C architecture, on-line monitoring, and worker and process efficiency technologies. This timeline will be challenging and reflect the time frame in which the benefits are needed in order to ensure competitiveness in the electric market for the participating nuclear plants. The timeline will be adjusted by individual nuclear plants to reflect the scheduling realities they have, such as timing of refueling outages and lead times for technology procurement.

6.2 Digital I&C Systems

The following sections describe the development of the four elements of the modernization strategy for digital I&C systems. The scope of this area is safety-related I&C systems (including highly-safety significant systems such as the reactor trip system and engineered safeguards actuation system), non-safety integrated control systems, annunciator and monitoring systems, post-accident monitoring systems, balance-of-plant control and monitoring systems, and control room configuration and human factors.

6.2.1 End-State Architecture

In order to achieve significant NPP O&M cost reductions, in addition to resolving obsolescence and reliability issues for the legacy I&C systems, an advanced digital I&C architecture must be defined. This architecture must be capable of enabling the following types of cost savings:

- Reduced technical specifications and associated surveillance tests
- Reduced maintenance and testing costs through reduced instrument calibrations, use of memory checks in lieu of testing, self-diagnosis, etc.
- Capability to convert a substantial portion of the field logic devices to the control and protection software, thereby allowing these devices and associated cables to be removed or abandoned in place.
- Support control room modernization that leads to reduced operations staffing
- High reliability through fail-over redundancy

- Minimal platforms so that the number and type of maintenance procedures, qualified maintenance tasks, work order models, operations training modules, etc. is minimized.
- Reduced engineering costs by eliminating
- Reduced operational events thereby reducing generation losses, safety challenges, and regulatory impacts.

One end-state architecture meeting the requirements listed above is the Compact Digital Modernization (CDM) concept documented in DOE report INL/LTD-16-39945, *Fully-Integrated Control Room Modernization: A Case Study* [53]. The CDM is a complete plant-wide generic design that encompasses all safety and non-safety I&C systems of a nuclear plant, including human-system interface (HSI), and the interface to plant sensors and controlled plant components (e.g., pumps, valves, electrical breakers). The CDM is characterized by:

- A plant overview display (POD) that is the apex of the information hierarchy in the main control room (MCR). The POD continuously displays the status of all critical power and safety functions, and the plant systems used to control those functions. It also displays all plant alarms including those corresponding to the critical functions and systems.
- Individual video display unit (VDU) -based workstations for each operator; in the CDM these are referred to as operator consoles (OCs). Each OC allows each operator to access all plant information and controls for all plant systems (safety and non-safety), and all plant process computer and information technology system (ITS) applications, through selectable graphic displays.
- A very high level of I&C system integration, while maintaining sufficient segmentation to comply with safety criteria, including CCF that can result from shared hardware resources and common designs.

The highly integrated CDM I&C architecture end-point is shown in Figure 1.

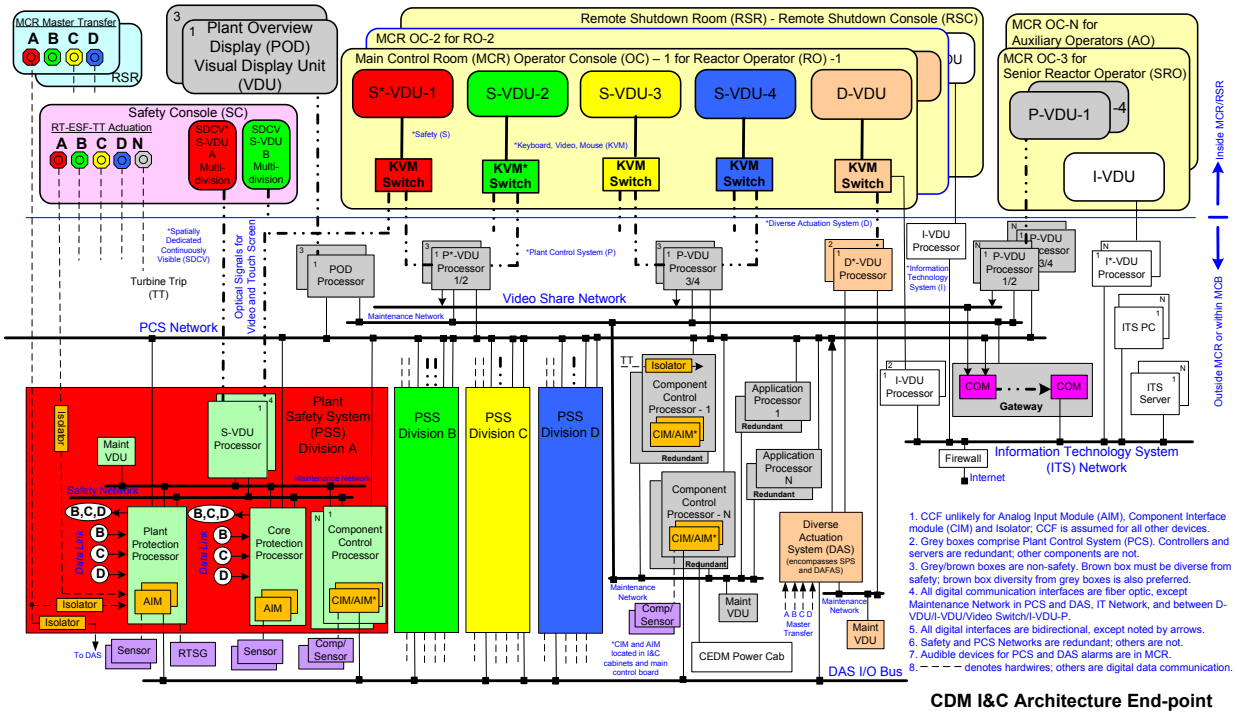

Figure 1. Compact digital modernization I&C architecture.

A more detailed description of the CDM end-state architecture is presented in Appendix A, with explanations of how it addresses the issue of CCF.

The I&C Technical Team will develop a detailed specification for such an architecture. It is recommended that the CDM as used as a starting point, modifying it as needed to satisfy all of the eventual desired features.

The specification would include the following:

- A description and schematic of the architecture, depicting protection, control and monitoring features, as well as HSI arrangements and interfaces to company business networks, plant monitoring systems and centers, mobile worker and process automation, alternate control room and remote shutdown facilities, emergency response facilities.
- A description of the control room and the concept of operations, detailing the staffing requirements and the automated support functions for the operations organization, such as paperless processes.
- A pro forma set of Technical Specifications that reflect the LCO flexibility and reduction in surveillance requirements.
- A description of how the architecture interfaces with the existing plant field logic devices, actuation devices, and associated cabling. Emphasis should be on the amount of field devices that can be eliminated.

The team would work with several qualified reactor vendors and other I&C supplier organizations to develop the desired configuration. These would likely be based on their current product offerings with some proposed modifications to incorporate new features that enable the desired operating performance and cost-reduction. It might be that some vendors would supply only parts of the overall architecture, but these parts would have to be entirely compatible with the overall architecture features.

This specification would also be used as basis in several related activities as described in this report. These include:

- The basis for a cost estimate of the manufacturing and implementation of the end-state I&C architecture.
- The basis for regulatory approval of the end-state I&C architecture, both early approval of new I&C features and later license amendment approvals as the specification was adopted into specific plant designs.
- The basis for implementation planning by decomposing the end-state I&C architecture into a set of sequenced and interrelated design change packages for the various implementation periods.

6.2.2 Cost-Benefit Analysis

The quantification of benefits due to full I&C and control room modernization will need to be determined for the final end-state architecture specification as developed in the first element of this strategy. As mentioned previously, this can be largely derived from the existing benefits analyses described in Section 6.2.1, A Business Case for Nuclear Plant Control Room Modernization (INL/EXT-16-39098) {51]

In addition, a more detailed analysis of full I&C and control room modernization has been performed under the DOE LWRS Program for the Palo Verde Generating Station in 2017, and a non-proprietary version of this information will be made available for use in the developing the cost-benefit analysis.

6.2.3 Regulatory Approach

One of the key tenets of this modernization strategy is to resolve regulatory approval issues before they would be on the critical path of implementation. This could take one or more of several forms of NRC review and approval, including:

- Submitting a topical report (ToR) of the I&C end-state architecture based on the CDM design.
- Work with the NRC to develop a NUREG that addresses the key beneficial features under consideration.
- Submit an industry report (or series of reports) for endorsement by the NRC of the key features of the I&C end-state architecture, perhaps in a Regulatory Guide.
- Work with a first-mover nuclear utility in the early stages of a license amendment to seek early approval of the new I&C features.

The preferred and most effective means of achieving this early review of new I&C features is the use of a topical report inclusive of all beneficial features of the CDM. There are, however, issues to be worked out in how the topical report can be referenced by standard license amendments for the implementing nuclear utilities. Discussions will be held with the NRC, NEI, and industry to determine the best path forward. It is the intent of this strategy to be able to reference some approved document for the new I&C features, and thus limit the regulatory review to how the licensee has implemented those features.

Some parts of the I&C end-state architecture will likely require license amendments under 10 CFR 50.90 to implement, such as digital upgrades of the reactor protection system (reactor trip system and engineered safeguards system). Qualification for digital I&C systems with respect to common cause failure will need to comply with BTP 7-19 of Chapter 7 of the NRC's Standard Review Plan (NUREG-0800).

Many of the I&C architecture components will be able to be implemented under 10 CFR 50.59, especially with the new guidance provided under the NRC's RIS 2002-22 Supplement 1 [54]. This will provide a means of the licensee demonstrating the low likelihood of a CCF and thus be able to proceed with the change under the conditions set forth in this regulation.

6.2.4 Implementation Plan

In 2004 EPRI published a study in TR-1009611 "Full Plant I&C Modernization in 30 Days or Less" [55] which concluded that a one-step plant-wide digital modernization could be implemented in 30 days as a "best case" scenario and 60 days as a "worst case" scenario. This range was highly dependent on the number of people that could install I&C equipment concurrently within the physical constraints of the equipment rooms and the extent of post installation pre-startup testing desired by the plant owner; as stated by EPRI, this testing could actually extend the implementation duration even more. The EPRI study was conducted by a team of highly experienced nuclear professionals from an I&C system supplier, an architecture engineer, and a nuclear utility.

From the EPRI study, it is clear that the most cost-effective modernization effort would be done in a single outage. EPRI concluded that one-step implementation would save approximately 23% over phased implementation. This is due primarily to minimizing the amount of temporary equipment and rework required between phases. In addition, this avoids having to analyze, design, and implement multiple interim configurations, including both the technical and human factors aspects. As also identified by EPRI, the cost benefit analysis for a multi-phased implementation program is negatively impacted by delaying full benefits of modernization for four to five fuel cycles.

Therefore, it is reasonable that if the business case would not work for a single outage, it would also not work for implementing over multiple outages. This however is somewhat contingent on the lost

revenue in an extended single-outage implementation versus no incremental lost revenue if the implementation was limited to the normal critical path duration of refueling outages, in other words, kept off the critical path of the normal refueling outages.

The work for a one-step implementation would be broken down into four categories:

1. Work accomplished during on-line periods prior to the main implementation outage. This includes HSI activities, such as simulator development and operator training.
2. Off-critical path staging work; this is work that would be accomplished in refueling outages prior to the main implementation outage,
3. Work during the main implementation outage, which would be an extended refueling outage. This includes control functions that must remain operable throughout the outage to support other activities that will be going on at the site (e.g., core cooling, spent fuel pool, electrical distribution)
4. Work activities that extend beyond the main implementation outage; this includes commissioning of functions not needed in the startup process, transfer of the temporary control functions used during the outage, and cleanup and removal of old I&C equipment.

The entire implementation would be broken down into a set of design change packages with a set implementation order. These design packages would identify the plant changes as well as the programmatic changes that would be needed to support the implementation. The design change packages would be sequenced over the three implementation periods above.

A very detailed study would be conducted to develop an integrated schedule of the implementation outage, determining the critical path of the implementation and how that affected the critical path of the implementation outage. This would have to be integrated with suitable work windows, defense-in-depth requirements, Technical Specification requirements, system start-up and commissioning testing, and initial operations under the modernized I&C and control room infrastructure. Contingency plans would be required for all appreciable risks.

A comparison of the implementation issues of the CDM to those described in the EPRI report is found in Appendix B.

6.3 On-line Monitoring

The following sections describe the development of the four elements of the modernization strategy for on-line monitoring. The scope of this domain is all plant parameters and instrumentation that can be centrally monitored to reduce labor requirements for the plant operations and maintenance staff, by conversion of the related work activities from time-based inspections and tests, to condition-based monitoring. Over time, the number of work activities that can be converted to monitoring is expected to grow, resulting in more and more savings to the plant. In addition, on-line monitoring is expected to reduce operating costs in the forms of fewer in-service component failures and reduced plant efficiency losses (undetected megawatt losses).

6.3.1 End-State Architecture

As described in the previous section, a sources of plant monitoring data, there are the plant I&C systems that provide the monitoring, control, and protection functions that are necessary for plant operations and nuclear safety. However, there is an emerging counterpart to these I&C systems that addresses plant health monitoring rather than plant operations. This is typically referred to as on-line monitoring and relies on both the same operational plant sensors as well as an augmented set of sensors specific to measuring parameters that indicate the health of structures, systems, and components. The output of these sensors flows to a different set of monitoring and analytical capabilities for detecting and characterizing degradation in time to take actions before incipient failures. These monitoring and

analytical capabilities are, in turn, interfaced to work process, risk management, and mobile work technologies so that appropriate actions can be taken by the plant staff with the greatest efficiency.

On-line Monitoring represents a continuum of activities to acquire knowledge of plant, structure, system, and component level data to determine status and condition for operational, engineering, and long-term planning purposes. On-line monitoring therefore enables nuclear plants to move from time-based periodic maintenance and testing to condition-based monitoring, taking actions only when indicated by data reflecting the actual condition of plant structures, systems, and components. This also reduces maintenance-induced failures and excessive component wear due to testing.

In the broader sense, on-line monitoring consists of overlapping areas of monitoring, from the immediate concern on operations and configuration management through the intermediate and longer-term concerns with plant health, as indicated in Figure 2.

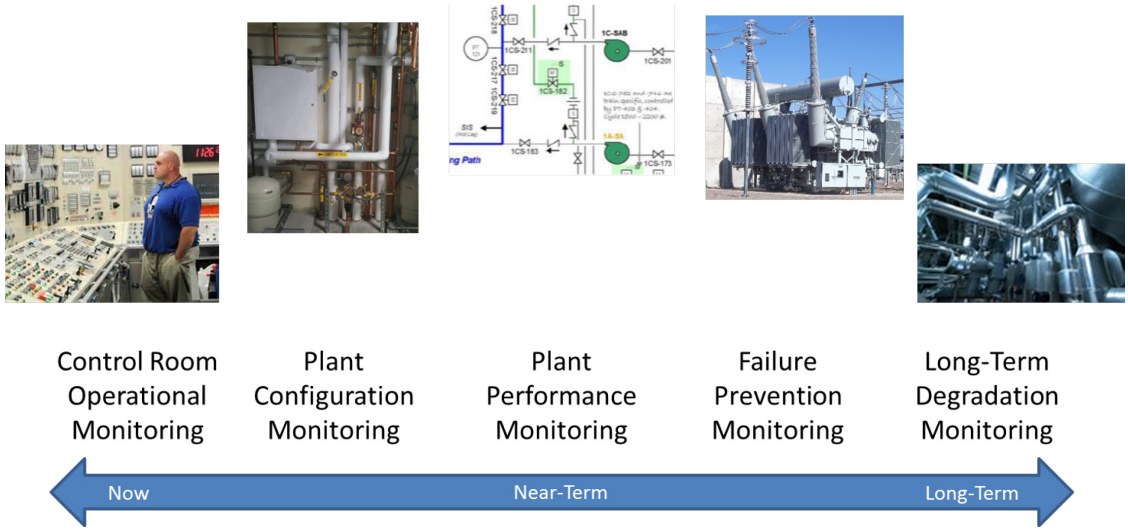

Figure 2. Overlapping domains of on-line plant monitoring.

These on-line monitoring technologies must be configured in a manner to provide an integrated understanding of plant conditions ranging from the immediate to the life of the facility. This requires an on-line monitoring architecture that integrates these considerations into an array of interconnected capabilities integrated into the work processes of all the organizations that have responsibilities for aspects of plant operations and health.

Similar to the end-state I&C architecture, a specification would be developed for the condition-based monitoring architecture and related platform. Initially, it is expected that a centralized on-line monitoring center will conduct the monitoring. In time, some monitoring aspects might consist of automated functions residing in software with capabilities similar to what human experts can do in pattern recognition, cause diagnosis, and prediction of failure times. However, in the nearer term, the monitoring centers would be a blend of human expert and expert systems suited to their respective strengths.

The specification would reflect and build upon the notable industry models and initiatives in this area. One such example is the Luminant Power Optimization Center located in Dallas, Texas, with other examples being the monitoring center initiatives of other utilities including Exelon, Southern Company, and Duke Energy.

The initial focus of on-line monitoring would be technical areas that can be assessed with the existing set of plant sensors used in plant operations. This set of sensors will be augmented in time with more and

more sensors where there is a business case to convert to monitoring. These sensors will not have to comply with the design standards and requirements of the operational sensors in that they will not be credited for these functions. Rather, they can be more economically implemented using wireless communications and powered with batteries or power-harvesting technologies.

A sub-group of the industry end-state implementation group will have the responsibility for defining a specification for on-line monitoring implementation, based on best available technologies. This specification will be revised and enhanced over time as new technologies become available.

In 2017, an industry effort under the direction of the NEI "Delivering the Nuclear Promise (DNP)" published a white paper [56] that stated a range of possible monitoring areas that are thought to be cost-beneficial and are listed in Table 1. There are no doubt many others to be listed, and would likely be identified in a top-down analysis of all plant work activities. New on-line monitoring applications should be evaluated by both research organizations and commercial suppliers for development as enabling sensor and analytical technologies become available.

Table 1. Future on-line monitoring applications.

Future On-Line Monitoring Applications	
Instrument Calibration Monitoring	Equipment Qualification
Gas Voiding	Cycles
Radiation Monitoring	Thermal Fatigue
Current	Chemistry
Generator Condition	Condenser/Heat Exchanger Performance
Transformer	Plant Configuration
Thermography	Section XI
Radwaste	Flow-Assisted Corrosion
Fire Protection	Security

6.3.2 Cost-Benefit Analysis

The On-Line Monitoring team will perform a cost-benefit analysis for the proposed scope of the on-line monitoring function. In general, this business case will quantify expected savings in converting from time-based testing and maintenance to condition-based monitoring. There are at least three types of savings:

- Those derived from avoided maintenance costs and production losses by early detection of component degradation.
- Those derived from identification and correction of plant efficiency losses.
- Those derived from reduced labor and materials cost for condition-based monitoring and by deferring unneeded time-based maintenance and testing.

The cost-benefit analysis would benefit from input provided by the nuclear utilities that are operating on-line monitoring centers presently, assuming they will provide data and experience for this purpose. This should provide a baseline cost-benefit analysis that is grounded in actual operating experience. From there, the analysis can be extrapolated to consider additional forms of monitoring enabled by new monitoring technologies, and the cost offsets can be estimated for them. This process will continue over time as the scope of on-line monitoring is expanded (see Table 1) to encompass more of the traditional maintenance and testing costs until it is optimized on a cost basis.

Finally, it is important for the participating utilities to collect and analyze cost savings on a consistent basis so that the results can be combined to measure the total cost-savings potential of all the monitoring technologies that are employed in the operating fleet.

6.3.3 Regulatory Approach

Regulatory approval for use of monitoring technologies is not required in general. However, there might be aspects of the deployment of these technologies that need to be considered from a regulatory compliance or licensing perspective. For instance, the implementation of new sensors will need to be evaluated from the standpoint of design changes, even if not relied upon for any operational or safety functions. The licensee must ensure that the installation of monitoring devices does not impact other functions described in the licensing basis through 10 CFR 50.59 screening or evaluation.

There might be some improvements that licensees will want to pursue that require licensing amendments, such as reduction or alterations in Technical Specifications based on monitoring capabilities. These changes might benefit from coordinated industry efforts in generic licensing packages. One such potential change would be for on-line calibration monitoring. This would need to be recognized under NRC-endorsed industry guidance such as NEI 04-10, which addresses licensee control of Technical Specification surveillance frequencies. Today this is based on an engineering program to evaluate as-found calibration values and would need to allow credit for real-time monitoring of calibration drift.

Another example would be possible crediting of on-line monitoring functions in lieu of ASME code testing and inspection requirements. These might involve development and approval of new code cases. Utilities typically commit to ASME code compliance in their licensing basis for such things as in-service testing and in-service inspection programs and that means new methods of compliance must be approved.

One other aspect of regulatory compliance for monitoring is the potential deployment of new low-cost sensors whose purpose is strictly for system, structure, and component health monitoring. It is important that operators not rely on these sensor outputs for any functions for which the instruments are not qualified. A means of differentiating these purposes must be maintained and observed in all operator protocols.

The On-Line Monitoring team will need to examine all of the potentially beneficial monitoring technologies and determine what regulatory evaluations and licensing actions might be needed to deploy these in a regulatory-compliant manner.

6.3.4 Implementation Plan

While implementation of on-line monitoring technology can be successfully done in many different sequences and time frames, for the purpose of this strategy, implementation planning should be coordinated with the development and planning for the I&C end-state architecture. This is to ensure maximum integration of sensors, communications, and data access consistent with design and licensing basis requirements.

The implementation plan should address all aspects of the shift from time-based periodic maintenance and testing to that of condition-based monitoring. This includes the stand-up of centralized on-line monitoring centers and related IT capabilities, staffing, acquisition of data, implementation of analytical software, protocols for communications with the monitored plants on discovered conditions, and archival/ record keeping for all monitoring activities.

The implementation plan should also take into consideration industry guidance on sensor recommendations to detect the various forms of degradation and failure of nuclear plant components and structures. Thus, the implementation plan should identify suitable opportunities to install these sensors when the least impact on plant operations and component availability.

Finally, a long-range implementation forecast should be developed to project when emerging monitoring technologies are expected to be available for production use. This will allow the industry to collectively focus on support for these developments, generate guidance for installation and usage, forecast of future O&M cost savings, and develop plans for the organizational and work process changes enabled by their usage.

6.4 Mobile Worker/Process Efficiency Technology

The following sections describe the development of the four elements of the modernization strategy for mobile worker/process efficiency technology. Recognizing that most office functions are automated through customized IT applications, the scope of this area focuses on mobile workers that today are mostly using paper-based processes with considerable inefficiencies in all the process requirements, human-error prevention requirements, and work approval/release requirements needed to conduct field work. There are large variety of work activities for support of a nuclear plant to be considered. However, they have a great deal in common in how they are conducted at a task level in terms of worker qualifications, work packages, pre-job briefs, use of procedures, work sign-on, use of MTE, post-job processing, etc. There is great economy of scale in implementing mobile worker technologies in a nuclear plant.

The process efficiency technologies refer to emerging capabilities (such as bar codes, RFID, computer vision, wireless instruments, etc.) to accomplish what field workers typically perform today. These have the potential to eliminate human efforts altogether, or reduce the number of workers that must be assigned to a single job. An example is the use of bar codes or RFID tags to correctly identify components in lieu of assigning a second worker to a job whose only function is to serve as a verifier.

6.4.1 End-State Architecture

The nuclear power industry has been engaged in deploying new digital technologies for plant worker for several years now, focusing on capabilities to improve the efficiency of work and reduce human error. These technologies include computer-based procedures and work packages, which provide an array of features that reduce time to complete field work, reduce the number of plant workers per task, improve work coordination, and prevent errors that would otherwise result in costly corrective actions. In addition to these, there are new standalone technologies that can offset human worker requirements of today, such as use of in-line chemistry instruments, RFID technologies, use of computer vision, etc. These technologies can transform how current labor-intensive work activities are accomplished and reduce operating costs accordingly.

A specification will be developed as to the most effective means of mapping these technologies onto the typical nuclear plant operating model and related organization structure, resulting in the broadest possible application of these technologies. The specification will be developed in a top-down manner to identify both technology coverage and technology gaps with respect to automating plant work activities and processes. The specification will identify technology sources and best practices for implementation. It will address the technology gaps as research priorities for DOE, EPRI, other research organizations, and commercial product developers for future operating cost reductions.

The end-state architecture will also enable new virtual-based business models in which remote third parties can provide real-time services just as effectively as if they were on site. This is expected to have significant cost savings potential compared to maintaining on site competency and continuous availability for so many technical services. New service models for these technical areas are expected to emerge as the nuclear plants make provisions for them in their business models and digital architectures.

6.4.2 Cost-Benefit Analysis

Several benefit analyses have been undertaken in the LWRS Program for digital technologies, including mobile work packages, outage improvement, and control room modernization. These studies

were conducted to estimate and confirm that there are substantial benefits in deploying these technologies. They were conducted using a tool developed in conjunction with ScottMadden Management Consultants, known as the Business Case Methodology (BCM), to assess the impact of new nuclear plant digital technologies. This tool consists of a complex spreadsheet workbook that has a complete set of plant activities for which savings in eliminated work, savings in making work more efficient, and savings in non-labor expenses can be recorded against these activities in a manner that computes the aggregate savings for a typical nuclear plant.

The BCM calculates and totals the cost improvements at the task level for all of the plant activities that can benefit from particular technologies. In this manner, a much more comprehensive business case can be derived that greatly increases the benefit/cost ratio. This has the added benefit of driving consistency across the NPP organizations which further reduces many forms of support and administrative costs.

Two business case benefit analyses have been performed on technologies that are relevant to this modernization effort under the DOE Light Water Reactor Sustainability Program. These analyses are directly applicable to the cost-benefit analysis to be conducted under this element of the strategy. They are:

- Pilot Project Technology Business Case: Mobile Work Packages (INL/EXT-15-35327) [49]
- A Business Case for Advanced Outage Management (INL/EXT-16-38265) [50]

Finally, EPRI has conducted a number of cost-benefit analyses, as well as workforce staffing studies, for portions of the plant modernization scope and it is assumed that these will be available to member utilities participating in the nuclear plant modernization efforts of the industry.

6.4.3 Regulatory Approach

There would typically be little regulatory concern or impact with worker and process efficiency technologies, as long as they met requirements set forth in the licensing basis. These requirements are typically general enough that conversion to digital technology capabilities would not impact them. These requirements are found in such documents as Technical Specifications – Administrative Controls section, UFSAR Chapter 13 Conduct of Operations, Quality Assurance Program and associated implementing directives and procedures, committed regulatory guides such as RG-1.33 Quality Assurance Program Requirements [57] referencing ANSI/ANS 3.2 Managerial, Administrative, and Quality Assurance Controls for Operational Phase of Nuclear Power Plants [58], and individual plant regulatory commitments.

Because many nuclear plant directives and procedures are credited for implementing the requirements of the Quality Assurance Program, they would need to be updated to the extent that use of the digital-based worker and process efficiency technologies is authorized and has an adequate level of management and administrative controls. These directives and procedures are typically designated as nuclear-safety related.

The Mobile Worker/ Process Efficiency Technology team will develop generic guidance for utilities to follow in regard to addressing in issues in their respective licensing bases. It is recognized that many nuclear utilities have already implemented various forms of digital technologies for mobile workers and process improvements. An early such example were hand-held devices used for operator rounds. More recently, many utilities have begun to implement computer-based procedures. The team will draw on this experience to ensure that the range of potential regulatory concerns have been identified and considered.

6.4.4 Implementation Plan

Similar to implementation planning for on-line monitoring, implementation for worker and process efficiency technologies can proceed in varied order as nuclear utilities address certain aspects of their operations. However, for the purpose of this strategy, the key consideration is coordination of the implementation of these technologies with those in the other two major domains to produce the earliest and

greatest cost savings and performance improvement. For example, mobile work processes such as computer-based procedures for auxiliary operators can enable control room efficiencies in directing critical field operational activities, contributing to the justification to operate with reduced control room staffing. Similarly, use of worker and process efficiency technologies can reduce costs for plant health monitoring when it is not yet possible to fully-automate the acquisition of monitoring data.

The Mobile Worker/ Process Efficiency Technology team will develop an implementation plan based on the readiness of digital technologies, reflecting a preferred sequence of implementation to gain the maximum savings in the shortest time frame. It will work with the team addressing the seamless digital environment (Section 6.5) to implement the needed IT infrastructure to integrate these technologies into the process applications the plants use to conduct and manage work processes.

6.5 Seamless Digital Environment

The following sections describe the development of two required elements in the modernization strategy for the development of a seamless digital environment. The scope of this effort is all the underlying digital architecture that is not part of the digital I&C systems end-state architecture. However, the interface to this the I&C architecture is part of the scope for the purpose of getting real-time plant data into the on-line monitoring and the mobile worker/process efficiency technology end-state architectures. The intent of this seamless digital environment is that all plant workers have virtually effortless access to the data they need to do their jobs, allowing them to focus completely on value-added tasks rather than spending time obtaining information and reformatting it for their usage. This also eliminates the opportunity to introduce new errors into the data streams.

6.5.1 Digital Architecture

A major premise of the nuclear plant modernization strategy is that significant business improvement can be achieved through the integration of plant systems, plant processes, and plant workers through the application of digital technology. For example, data from digital I&C systems can be provided directly to work process applications and then, in turn, to plant workers carrying out their work using mobile technologies. This saves time, creates significant work efficiencies, and reduces errors. So, this seamless digital environment can be thought of as integrating information from plant systems with plant processes for plant workers through an array of interconnected technologies as follows:

- **Plant systems**. Beyond centralized monitoring and awareness of plant conditions, deliver plant information to digitally based systems that support plant work and directly to workers performing these work activities.
- **Plant processes**. Integrate plant information into digital field work devices, automate many manually performed surveillance tasks, and manage risk through real-time centralized oversight and awareness of field work.
- **Plant workers**. Provide plant workers with immediate, accurate plant information that allows them to conduct work at plant locations using assistive devices that minimize radiation exposure, enhance procedural compliance and accurate work execution, and enable collaborative oversight and support even in remote locations.

Figure 3 illustrates the interconnections of these areas:

Figure 3. Seamless information architecture.

An end-state architecture for a seamless digital environment will serve as the underlying structure for the three domains of I&C systems, on-line monitoring, and worker and process efficiency. A specification will be developed for a seamless digital architecture of plant information supporting the information requirements of the domains of plant I&C systems, plant monitoring, and plant worker and process efficiencies. The specification will address generic means of connecting data to systems and work activities, addressing such issues as

- Data quality
- Data latency
- Bandwidth
- Cyber Security
- Application interface

The Nuclear Information Technology Strategic Leadership (NITSL) has addressed similar needs in their work and could possibly play a coordinating as well as a developing role for this requirement. It is recognized that the actual implementation is dependent on utility standards and practices, as well as selected commercial IT products, and will have to be adapted to these in actual implementation.

Working with NITSL and utility partners, the DOE LWRS Program has completed two reports on digital architecture that are relevant to defining the seamless digital architecture. They are:

- Digital Architecture Requirements (INL/EXT-15-34696) [59]
- Digital Architecture: Results From a Gap Analysis (INL/EXT-15-36662) [60]

6.5.2 Implementation Plan

An implementation plan for developing and installing the underlying plant networks, processors, and other information technology components will be developed in conjunction with the developments of the end-state architectures of the I&C systems, on-line monitoring, and worker/process efficiency technologies, drawing on the related work on digital architecture described above. It is recognized that

nuclear plants typically have many of these components in place, but they might not be configured to connect all of the information assets and processing of a modernized nuclear plant, nor attain the maximum efficiency in the exchange of information among all of the plant work functions. In other cases, new information technology components will need to be installed, such as comprehensive wireless access for mobile workers and new sensors. Finally, appropriate means of interfacing to existing plant instrumentation and control systems must be implemented where needed for support functions, consistent with all design and licensing criteria such as independence, separation, and cyber security.

The product of this activity will be a phased integrated implementation plan that will support the technologies of each of the end-state architectures as they are implemented. It will necessarily be generic to some degree in that the infrastructure additions will vary from plant to plant. Yet it will serve as a template for detailed planning and scheduling for individual plants as they customize it for their specific requirements.

7. Summary

For the U.S LWR operating, addressing digital I&C qualification is key to resolving the reliability and obsolescence issues of the legacy analog I&C systems, as well as enabling the business performance improvement and cost reductions of modern digital technologies. This report addresses the unique aspects of digital I&C technology that both enables these improvements, and yet introduces new types of failure modes that must be addressed to ensure nuclear safety and operational reliability.

A key purpose of this report is to present an assessment of digital I&C qualification issues and address gaps in qualification methods and processes that would potentially benefit from DOE-sponsored research and development. In particular is the concern of CCF. Two new qualification methods are described that are recommended for further Department of Energy-sponsored research and development. They are 1) Testability – the exhaustive (100%) testing of certain digital devices addressing all combinations of inputs and internal states, and 2) Elimination of CCF triggers – ensuring that any latent digital defects are not concurrently triggered in redundant and back-up safety systems.

In addition, this report presents a strategy for implementation of safety-related digital I&C systems as part of full nuclear plant modernization. This modernization strategy exploits the inherent digital capabilities of integration, interconnectivity and standardization to modernize I&C systems without compromising safety or performance, thereby reducing implementation cost and schedule, and reducing recurring operations and maintenance cost. It similarly addresses other opportunities for operating cost reduction using on-line monitoring and mobile worker/process efficiency technologies. The strategy is based on four interrelated elements that together address the remaining barriers to successful implementation: 1) end-state architecture, 2) cost-benefit analysis, 3) regulatory approach, and 4) implementation plan. The digital qualification methods presented in this report are key facilitators in this full nuclear plant modernization strategy.

8. NEXT STEPS

The next step in this project is pursue industry consensus and adoption of the full nuclear plant modernization strategy, both with the existing collaboration partners as well as other nuclear operating utilities, nuclear industry suppliers, and the NRC. It is likely that useful suggestions and alternations of this strategy will be identified in this process and a revision to this report will be considered. Otherwise, the strategy for full nuclear plant modernization found in Section 6 of this report is offered for industry use.

The plant modernization collaboration effort described in this report will be supported through the work and results of this research project, as well as other projects under the DOE Light Water Reactor Sustainability Program. The scope of full nuclear plant modernization will draw on virtually every

research project and technology development in the history of the Program. Guidance on the use of the information in this report, as well as all related research results and products, will be offered to the proposed industry modernization effort.

Finally, the two new potential qualification methods for safety-related I&C systems in defense against CCF will be pursued consistent with LWRS Program priorities and funding. The next steps in the development of a Testability method (see Section 5.2) are the subject of a new research project which will be conducted over the next six months. The development of a method for Elimination of CCF Concurrent Triggers (see Section 5.1) needs some further definition in order to be submitted as a recommended research project. This will be pursued for review and approval in the coming months.

9. REFERENCES

1. Nuclear Regulatory Commission, *Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure, Revision 1*, ML17102B307, March, 2017
2. Institute of Electrical and Electronics Engineers, The Authoritative Dictionary of Standard IEEE Terms, Seventh Edition, IEEE Std. 100-2000, Piscataway, NJ, 2000
3. Torok, R., "Methods for Assuring Safety and Dependability DI&C Systems," Electric Power Research Institute (EPRI) Report 3002005326, June, 2016
4. U.S. Code of Federal Regulations, 10 CFR 50 Appendix A, General Design Criteria for Nuclear Power Plants, Washington, DC
5. U.S. Code of Federal Regulations, 10 CFR 50.55 a(h), Codes and Standards (Protection Systems), Washington, DC
6. Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," IEEE Std. 603-1991, Piscataway, NJ, June, 1991
7. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.75 Revision 3, Criteria for Independence of Electrical Safety Systems, Washington, DC, February, 2005
8. Institute of Electrical and Electronics Engineers, Standard Criteria for Independence of Class 1E Equipment and Circuits, IEEE Std. 384-1992, Piscataway, NJ, June, 1992
9. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.100 Revision 3, Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants, Washington, DC, September, 2009
10. Institute of Electrical and Electronics Engineers, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std. 344-2004, Piscataway, NJ, June, 2005
11. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.89 Revision 1, Environmental Qualification of Certain Electric Equipment Important to Safety for Nuclear Power Plants, Washington, DC, June, 1984
12. Institute of Electrical and Electronics Engineers, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations, IEEE Std. 323-1974, Piscataway, NJ, February, 1974
13. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.180 Revision 1, Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems, Washington, DC, October, 2003
14. Shank, J., Meininger, R., and Shankar, R., Guidelines for Electromagnetic Interference Testing in Nuclear Power Plants Electric Power Research Institute (EPRI) TR-102323, September, 1994

15. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.204, Guidelines for Lightning Protection of Nuclear Power Plants, Washington, DC, November, 2005

16. Institute of Electrical and Electronics Engineers, IEEE Guide for Generating Station Grounding, IEEE Std. 665-1995, Piscataway, NJ, 1995

17. Institute of Electrical and Electronics Engineers, IEEE Design Guide for Electrical Power Service Systems for Generating Stations, IEEE Std. 666-1991, Piscataway, NJ, 1991

18. Institute of Electrical and Electronics Engineers, Guide for Instrumentation and Control Equipment Grounding in Generating Stations, IEEE Std. 1050-1996, Piscataway, NJ, February, 1996

19. Institute of Electrical and Electronics Engineers, Application Guide for Surge Protection of Electric Generating Plants, IEEE Std. C62.23-1995, Piscataway, NJ, February, 1995

20. U. S. Nuclear Regulatory Commission, Digital Instrumentation and Control (DI&C) – Interim Staff Guidance (ISG) - 04, Highly-Integrated Control Rooms—Communications Issues, Washington, DC, September, 2007

21. U.S. Code of Federal Regulations, 10 CFR 50 Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants, Washington, DC

22. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.168, Revision 2, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Washington, DC, July, 2013

23. Institute of Electrical and Electronics Engineers, IEEE Standard for Software Verification and Validation, IEEE Std. 1012-2004, Piscataway, NJ, February, 2004

24. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.169, Revision 1, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Washington, DC, July, 2013

25. Institute of Electrical and Electronics Engineers, IEEE Standard for Software Verification and Validation, IEEE Std. 828-2005, Piscataway, NJ, 2005

26. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.170, Revision 1, Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Washington, DC, 2013

27. Institute of Electrical and Electronics Engineers, IEEE Standard for Software and System Test Documentation, IEEE Std. 829-2008, Piscataway, NJ, 2008

28. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.171, Revision 1, Software Unit Testing for Digital Computer Software Used In Safety Systems of Nuclear Power Plants, Washington, DC, 2013

29. Institute of Electrical and Electronics Engineers, IEEE Standard for Software Unit Testing, IEEE Std. 1008-1987, Piscataway, NJ, 1987

30. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.172, Revision 1, Software Requirement Specifications for Digital Computer Software and Complex Electronics Used in Safety Systems of Nuclear Power Plants, Washington, DC, 2013

31. Institute of Electrical and Electronics Engineers, IEEE Recommended Practice for Software Requirements Specifications, IEEE Std. 830-1998, Piscataway, NJ, 1998

32. U. S. Nuclear Regulatory Commission, Staff Requirements Memorandum (SRM) to SECY 93-087 "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs, Washington, DC, 1993
33. U.S. Nuclear Regulatory Commission, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Branch Technical Position 7-19, Washington, D.C., 2007
34. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.105, Revision 3, Setpoints for Safety-Related Instrumentation, Washington, DC, 1999
35. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.152, Revision 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, Washington, DC, 2011
36. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions, Washington, DC, 1972
37. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.118, Revision 3, Periodic Testing of Electric Power and Protection Systems, Washington, DC, 1995
38. Institute of Electrical and Electronics Engineers, Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, IEEE Std. 338-1987, Piscataway, NJ, 1987
39. U. S. Nuclear Regulatory Commission, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition — Instrumentation and Controls (NUREG-0800, Chapter 7), Washington, DC, 2016
40. International Organization for Standardization (ISO), Quality Management Systems, ISO 9001, 2015
41. U. S. Nuclear Regulatory Commission, Regulatory Guide 5.71, Cyber Security Programs for Nuclear Facilities, Washington, DC, January 2010
42. U.S. Code of Federal Regulations, 10 CFR Part 52, Licenses, Certifications, and Approvals for Nuclear Power Plants, U.S. Nuclear Regulatory Commission, Washington DC
43. U.S. Code of Federal Regulations, 10 CFR Part 50, Domestic Licensing of Production and Utilization Facilities, U.S. Nuclear Regulatory Commission, Washington DC
44. U. S. Nuclear Regulatory Commission, NUREG 0847, Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Units 1 and 2, Washington, DC, 2011
45. Institute of Electrical and Electronics Engineers, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," IEEE Std. 7-4.3.2, 2003, Piscataway, New Jersey, 2003
46. U. S. Nuclear Regulatory Commission, NUREG/CR 7007, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, Washington, DC, 2010
47. Quinn, E., Mauck, J., Bockhorst, R., and Thomas, K., Digital Sensor Technology, INL/EXT-13-29750, Idaho National Laboratory, 2013
48. U.S. Code of Federal Regulations, 10 CFR 50.59, Changes, Tests and Experiments, U.S. Nuclear Regulatory Commission, Washington DC
49. Thomas, K., Lawrie, S., Vlahapolis, C., and Niedermuller, J., 2015, Pilot Project Technology Business Case: Mobile Work Packages, INL/EXT-15-35327, Idaho National Laboratory, 2015
50. Thomas, K., Lawrie S., and Niedermuller, J., 2016, A Business Case for Advanced Outage Management, INL/EXT-16-38265, Idaho National Laboratory, 2016

51. Thomas, K., S. Lawrie., and J. Niedermuller, 2016, A Business Case for Nuclear Plant Control Room Modernization, INL/EXT 16 39098, Idaho National Laboratory, 2016

52. U.S. Code of Federal Regulations, 10 CFR 50.90, Application for Amendment of License, Construction Permit, or Early Site Permit, Washington DC

53. Thomas, K., and K. Scarola, 2016, Fully Integrated Control Room Modernization: A Case Study, INL/LTD 16 39945, Idaho National Laboratory, 2016

54. U. S. Nuclear Regulatory Commission, Regulatory Issue Summary 2002-22 Supplement 1, Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems, Washington, DC, 2018

55. Hasenkopf, J., Kawanago, S., Kurth, W., and Nasar, J., "Full Plant I&C Modernization in 30 Days or Less -- A Feasibility Study," Electric Power Research Institute (EPRI) TR-1009611, 2004

56. Nuclear Energy Institute, Delivering the Nuclear Promise White Paper, Use of Advanced Remote Monitoring Technology to Reduce US Nuclear Station O&M Costs, June, 2017

57. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.33, Revision 3, Quality Assurance Program Requirements (Operation), Washington, DC, 2013

58. American National Standards Institute (ANSI)/ American Nuclear Society (ANS) 3.2-2012, Managerial, Administrative, and Quality Assurance Controls for Operational Phase of Nuclear Power Plants, 2012

59. Thomas, K. and J. Oxstrand, Digital Architecture Requirements, INL/EXT-15-34696, Idaho National Laboratory, 2015

60. Oxstrand, J., Thomas, K., Fitzgerald, K., Digital Architecture – Results From a Gap Analysis, INL/EXT-15-36662, Idaho National Laboratory, 2015

61. U. S. Nuclear Regulatory Commission, Digital Instrumentation and Control (DI&C) – Interim Staff Guidance (ISG) - 02, Diversity and Defense-in-Depth Issues, Washington, DC, 2007

62. U.S Nuclear Regulatory Commission, Regulatory Guide 1.97, Revision 4, Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants, Washington, DC, 2006

Appendix A
Compact Digital Modernization End-State Architecture

This appendix describes the Compact Digital Modernization (CDM) End-State Architecture features that exploit the integration, interconnectivity and standardization capabilities of modern digital technology to achieve cost effective digital modernization. It also explains how these capabilities of modern digital technology introduce new potential sources of CCF, the CCF defensive measures employed in the CDM to manage that potential, and their basis for licensing approval.

A simplified diagram of the CDM I&C architecture is shown the Figure 1 in Section 6.2.1 of this report.

PLANT SAFETY SYSTEM

The CDM Plant Safety System (PSS) significantly reduces the number of digital controllers and I/O modules compared to prior digital implementations, through a combination of features as described below. Some of these features have been previously employed; others have not.

1. Reactor trip (RT) and engineered safeguard features (ESF) functions reside in the same plant protection processor (PPP). There is licensing precedence for this on several previous plants, because for the accidents where ESF functions are credited, they are not a separate echelon of defense from RT (i.e., both safety functions are needed). Combining RT and ESF functions is in accordance with ISG-02 [61] and BTP 7-19 [33].
2. There is no hardware redundancy within a safety division because the safety divisions are already redundant to each other, and redundancy reduces mean-time-before-failure (MTBF), which increases O&M costs. Instead, high availability of each division is achieved through modern digital technology with very high MTBF. A significant contributor to high availability is also continuous self-testing, which results in very short mean-time-to-repair (MTTR). Continuous self-testing also eliminates all manual periodic surveillance tests that would otherwise require controllers to be taken out of service with the plant on-line. There is licensing precedence for crediting self-testing to eliminate on-line periodic surveillance tests.
3. There is no hardware duplication within a safety division to prevent spurious actuation (e.g., 2oo2 logic), because hardware duplication reduces MTBF and availability, which increase O&M costs. CCF due to a random hardware failure that leads to spurious RT/ESF actuation is prevented as follows:
    a. The output compare function (OCF) within each non-redundant PPP is employed for RT and ESF actuation, as explained in Section 4.1.2. Crediting the OCF within single controllers to prevent CCF due to spurious actuation will be introduced for licensing approval in the proposed CDM ToR.
    b. An energize-to-actuate configuration for ESF. This is commonly employed in most operating plants.
    c. An energize-to-actuate configuration for RT, at the division level. Compliance to the fail-safe requirement of GDC 23 is achieved at the system level if both divisions fail. This will be introduced for licensing approval in the proposed CDM ToR.
4. Each PSS Component Control Processor (CCP) controls approximately 50 plant components. This is achieved using modern digital controllers with large memory capacity and gigahertz performance. Non-redundant controllers with segmentation are employed to ensure a CCF due to a random hardware failure that leads to spurious actuation or erroneous control is tolerable. Where it is not, redundant controllers are employed with an OCF as described in Section 4.1.3. This OCF method is

employed only where necessary to prevent CCF, because it reduces MTBF and only provides a small improvement to availability. Crediting the OCF with redundant controllers to prevent CCF due to spurious actuation will be introduced for licensing approval in the proposed CDM ToR.

5. There is single point I/O for all data acquisition and control (e.g., no conventional hardwired analog signal distribution to multiple input modules). Analog input modules (AIM) and component interface modules (CIM) include simple hardware sections (i.e., 100% testable) that are shared by PSS and diverse actuation system (DAS). These modules include diverse digital data communication for PSS and DAS interfaces (i.e., internal diversity) to ensure a digital design defect does not exist that could affect the digital data communication to both PSS and DAS. The AIM and CIM designs will be introduced for licensing approval in the proposed CDM ToR.
6. Interfaces from CIMs to plant components are optimized to minimize the hardwired connections. This facilitates a compact CIM whose location is flexible (e.g., within existing control boards, motor control centers, auxiliary cabinets) to ensure that no new cables are required. Flexible CIM locations will be introduced for licensing approval in the proposed CDM ToR.
7. Digital communication is employed for all PSS interfaces within the CDM architecture. Class 1E data links and networks with software qualified to IEEE 1012 [23] software integrity level 4 (SIL-4) have been previously approved by NRC. PSS processors comply with ISG-04 [20] to protect themselves from erroneous control commands from outside their division. Inter-division digital data communication, with compliance to ISG-04 to prevent CCF for both unidirectional and bidirectional data, has been previously approved by NRC.
8. Visual display units (VDU) are employed for all PSS human systems interfaces (HSI), with the exception of conventional switches for RT and ESF manual initiation and main control room (MCR) to remote shutdown room (RSR) transfer. Safety VDUs with software qualified to SIL-4 have been previously approved by NRC. VDUs with compliance to ISG-04 to prevent CCF due to erroneous control commands, have been previously approved by NRC.
9. Dedicated safety VDUs are limited to spatially dedicated continuously visible (SDCV) displays for Regulatory Guide 1.97 [62] Type A and B variables. Other safety VDUs have selectable displays and serve two purposes:

    a. They are normally connected to the Plant Control System (PCS) using keyboard, video, mouse (KVM) switches. This allows those safety VDUs to normally display complex plant control system (PCS) graphics and provide control of all non-safety and safety plant components/functions.

    b. In the event of PCS failure, the safety VDUs can be KVM switched to the PSS. This allows all safety components/functions to be controlled from safety VDUs.

    Controlling safety plant components from the non-safety PCS has been previously approved by NRC. KVM switching for PSS safety VDUs will be introduced for licensing approval in the proposed CDM ToR.

    Multi-purpose safety VDUs not only reduce digital equipment, but they also facilitate compact operator consoles that can be installed in existing control rooms during the initial step of a multi-phase CDM implementation program.

10. There are no sequence-of-events (SOE) I/O modules and no hardwired SOE connections. All PSS digital controllers include internal time stamping relative to a periodic reference pulse from the SOE application server. The SOE application server assembles plant-wide SOE reports based on these relative time stamps and the deterministic response time of the digital data communication architecture. PSS internal SOE time stamping will be introduced for licensing approval in the proposed CDM ToR.

11. Application level diversity among different PSS controllers, with self-announcing, is credited to prevent concurrent triggering of a design defect in multiple CCPs that leads to spurious actuation or erroneous control actions. Therefore, a triggered design defect may result in erroneous control action from only one CCP or spurious actuation from one PPP. This "sufficient diversity" preventive measure will be introduced for licensing approval in the proposed CDM ToR. Non-concurrent triggering of a design defect is not credited to prevent a CCF that leads to failure-to-actuate, because this failure is not self-announcing; for this CCF the DAS is credited for mitigation.

DIVERSE ACTUATION SYSTEM

A key component of the CDM cost reduction is the non-safety DAS which requires no measurement channels, actuators, I/O modules or hardwired connections; the DAS is limited to only diverse digital processing for actuation and HSI. This is achieved as follows:

1. Backup RT and ESF functions reside in the same diverse protection processor (DPP). This is common for DAS implementations at most plants.
2. There is no redundancy within the DAS, because the DAS provides backup RT and ESF functions for a CCF in the PSS, and redundancy reduces MTBF which increases O&M costs. High availability is achieved through digital components with long MTBF and continuous self-testing to achieve short MTTR, as described for the PSS. Many DAS implementations have no redundancy.
3. There is no hardware duplication within the DAS to prevent spurious actuation (e.g., 2oo2 logic), because hardware duplication reduces MTBF and availability, which increase O&M costs. CCF due to a random hardware failure that leads to spurious actuation is prevented as follows:
    a. Parallel processing within the single non-redundant diverse protection processor (DPP) is employed for RT and ESF actuation, as explained for the OCF in Section 4.1.2 and explained above for the PPP. However, instead of an OCF, the parallel DAS signals are combined in the CIM using conventional 2oo2 logic. This design facilitates testing the conventional hardware-based CIM priority logic without unnecessary component repositioning. There is prior licensing precedence for this configuration.
    b. An energize-to-actuate configuration for backup RT and ESF functions. This is commonly employed for most plants with a DAS or ATWS mitigation system.
4. One DAS controller actuates all plant components required for accident mitigation with a concurrent CCF in the PSS. There is no component control logic in the DAS, because CIMs employ state-based priority logic and optimized essential component protection interlocks reside in external conventional circuits.
5. The DAS has no I/O modules. It receives its measurement channel inputs from the PSS AIMs and it interfaces its outputs to plant components via the PSS and PCS CIMs. There is licensing precedence for this signal sharing with the PSS. The AIM and CIM digital data communication interfaces to the DAS are implemented using digital data communication technology (i.e., the DAS I/O Bus) that is diverse from all digital data communications in the PSS; this includes diverse data communication processors in each AIM and CIM. The diverse digital communication interface designs will be introduced for licensing approval in the proposed CDM ToR.
6. The DAS has no interfaces to plant components. All interfaces are via the CIMs of the PSS and PCS.
7. Digital communication is employed for all DAS interfaces within the CDM architecture. This includes internal signals interfaced to the DAS audible alarm device in the MCR, which prompts

operators to recognize a PSS CCF. The DAS method of detecting a CCF in the PSS has been previously approved by NRC.

8. Visual display units (VDU) are employed for all DAS HSI, with the exception of MCR-RSR transfer signals which are hardwired from the PSS master transfer switches using conventional isolators. Hardwiring the signals directly to the DAS, with no PSS digital processing, ensures there is no digital design defect in the PSS that can erroneously transfer both the PSS/PCS HSI and the DAS HSI. There is no DAS HSI in the RSR because a PSS CCF does not require consideration concurrent with a MCR evacuation. Although there is no DAS HSI in the RSR, blocking erroneous DAS commands when there is a fire in the MCR prevents CCFs that could adversely affect achieving safe shutdown from the RSR. The DAS master transfer design will be introduced for licensing approval in the proposed CDM ToR.
9. There are no dedicated DAS VDUs. There are two DAS VDUs in the MCR with selectable displays. These DAS VDUs serve two purposes:

    a. They are normally connected to the Information Technology System (ITS) using keyboard, video, mouse (KVM) switches. This allows those DAS VDUs to normally display normal plant support functions, such as work management applications.

    b. In the event of a PSS CCF, the DAS VDUs can be KVM switched to the DAS processor. This allows all DAS functions credited for accident mitigation and safe shutdown to be controlled from the DAS VDUs.

    Controlling safety plant components from the DAS has been previously approved by NRC. KVM switching for DAS VDUs will be introduced for licensing approval in the proposed CDM ToR.

    Multi-purpose DAS VDUs not only reduce digital equipment, but they also facilitate compact operator consoles that can be installed in existing control rooms during the initial step of a multi-phase CDM implementation program.
10. There are no SOE I/O modules and no hardwired SOE connections. The DPP includes internal time stamping; this is the same functionality as described above for the PSS. DAS internal SOE time stamping will be introduced for licensing approval in the proposed CDM ToR.
11. Application level diversity among different DAS controllers cannot be credited, because there is only one DPP. Therefore, a triggered design defect may result in spurious actuation of multiple safety divisions from the DAS. A design defect in the DAS is significantly less likely than a single random hardware failure due to the DAS augmented quality program. As described in Section 2.3.3, this facilitates a beyond design basis analysis for this event, which employs “best estimate” methods. This analysis credits that, regardless of any erroneous commands from the DAS, the state-based priority in the CIMs ensures the PSS can always put plant components in their safe state position; therefore, this is not an onerous analysis. A triggered defect that results in DAS failure-to-actuate is benign because the DAS is a backup to the PSS, and triggering of two separate design defects (i.e., one in PSS and one in DAS) does not require consideration.

Plant Control System

The CDM PCS significantly reduces the number digital controllers and I/O modules compared to prior digital implementations through a combination of features as described below. Some of these features have been previously employed, others have not.

1. Continuous control functions and discrete state component control functions reside in the same controller for the same plant system. These functions are separated with analog implementations due to the distinct electronic components required. There is no need to separate these functions in digital controllers that have a broad library of continuous control and discrete control function blocks.

2. High availability of each control function is achieved through modern digital technology with long MTBF and continuous self-testing to achieve short MTTR; both contribute to low O&M costs. Redundancy is provided for some controllers, to implement the OCF function described in Item 4 below; but this is a small contributor to high availability.
3. Hardware duplication is provided to accommodate multiple VDUs in the MCR and RSR. This inherently results in high availability of HSI functions.
4. Each PCS CCP controls approximately 25-50 plant components. This is achieved using modern digital controllers with large memory capacity and gigahertz performance. Non-redundant controllers with segmentation are employed to ensure a CCF due to a random hardware failure that results in erroneous control is tolerable. Where it is not, redundant controllers are employed with the OCF, as described in Section 4.1.3. This OCF method is employed only where necessary, because it reduces MTBF and for controllers with long MTBF and short MTTR, controller redundancy only provides a small improvement in availability.
5. There is single point I/O (e.g., no analog signal distribution to multiple input modules) for all data acquisition and control. Where the PCS requires the same process measurements as the PSS, the PCS receives redundant measurement channel signals from the PSS via the PCS network (i.e., digital data communication). The PCS employs signal validation processing to ensure a failure in a shared measurement channel does not cause a plant transient while the PSS is also degraded by that same measurement channel failure.
6. The PCS employs the same optimized interface to plant components as the PSS to achieve a compact CIM design. Therefore, PCS CIMs have the same location flexibility as the PSS CIMs to eliminate the need for new plant cables. The PCS CIMs also employ a separate digital data communication interface to the DAS I/O Bus to accommodate non-safety components actuated by the DAS, such as diverse power interruption for control rod power supplies.
7. Digital communication is employed for all PCS interfaces within the CDM architecture. This includes bidirectional data communication with all PSS controllers to receive process measurement channels and to send non-safety control commands from PCS HSI and control processors to safety plant components/functions. PCS processors comply with ISG-04 to minimize the potential for erroneous control commands. This includes generating two distinct control messages (e.g., as for the OCF) and testing to demonstrate that environmental hazards do no cause spurious commands.
8. Visual display units (VDU) are employed for all PCS human systems interfaces (HSI), with the exception of conventional switches for turbine trip (TT) manual initiation; the PCS receives MCR-RSR transfer signals from the PSS via the PCS Network.
9. The PCS large display panel (LDP) provides the following SDCV information:
    a. Key parameters, digital values and trends, for critical safety functions and critical power production functions.
    b. Key parameters and component status for the preferred normal and emergency success paths for each critical safety function and critical power production function.
    c. Corresponding alarms for the functions in (a) and (b) above. Grouped alarm icons are provided for all other plant alarms, with drill down via selectable PCS HSI.

    In the event of an LDP failure, the LDP graphic, including dynamic trends and alarms, can be displayed on other selectable PCS HSI.
10. There are no SOE I/O modules and no hardwired SOE connections. All PCS digital controllers include internal time stamping; this is the same functionality as described above for the PSS and DAS.

11. Application level diversity among different PCS controllers, with self-announcing, is credited to prevent concurrent triggering of a design defect in multiple PCS CCPs that leads to erroneous control actions. Therefore, a triggered design defect may result in erroneous control action from only one PCS CCP. This “sufficient diversity” preventive measure has been credited in prior licensing actions, as described in Section 4.2.2; it will also be submitted for licensing approval in the proposed CDM ToR.

Appendix B
CDM End-State I&C Architecture Implementation

This appendix validates the EPRI 30-Day Implementation Outage report [55] conclusion regarding the feasibility of a short implementation outage for the CDM by comparing the it to the plant-wide I&C design in the EPRI study to identify any impact to the assumptions and methods that led to the EPRI conclusions, and any resolution to the barriers previously identified. This section also examines the methods considered by EPRI in attempting to minimize the modernization schedule, to identify any significant risks or potential for improvements that are facilitated by the CDM.

As can be seen from the information in the sections below, the CDM offers a substantial reduction in the amount of digital equipment needed and the number of hardwired interface connections needed over the I&C/HSI design used in the EPRI study; these improvements have come about through digital technology advances and innovations over the past 15 years. These improvements reinforce with much higher confidence the EPRI conclusion of achieving a 30-day one-step modernization. With these advanced CDM features it is reasonable to expect that EPRI's "worst case" scenario of 60 days can be reduced to 44 days; therefore, a 60-day one-step modernization is achievable with very high confidence.

The EPRI report is quite detailed regarding what must be done to achieve one-step modernization. The sections below examine those aspects of the EPRI modernization program that would be impacted by the advanced features of the CDM. While this substantially increases confidence that a one-step modernization is achievable in a maximum of 60 days, for any specific plant a detailed modernization plan would be needed.

OPERATOR TRAINING

The EPRI report identifies the need for two simulators – one for the current plant and one for the modernized plant. This is a significant implementation cost adder. The CDM does not need two simulators, because CDM operator consoles (OC) can be installed in the areas occupied by current plant computer consoles. This CDM installation is facilitated by more compact OCs for both reactor operators and the control room supervisor (i.e., the senior reactor operator) and a more compact safety console (SC) than assumed by EPRI, and the elimination of the DAS panel. All of these CDM features are facilitated by visual display units (VDU) with KVM switching that provide operator selectable connections to multiple I&C systems.

When operators are training for the existing plant, the CDM OCs can duplicate only the monitoring functions of the current plant computer workstations; operators will use the conventional HSI on the bench boards for all control actions. When operators are training for the modernized plant, the CDM OCs will function with multi-division soft controls; plant overview displays will be mounted temporarily in front of the existing bench boards.

The simulator computer models all analog control functions for the existing plant and will emulate all digital controllers for the modernized plant. This facilitates an easy software configuration swap between either plant configuration.

CABLE PULLING AND ROUTING

To achieve a 30-day modernization, EPRI defined a goal of no cable pulling into the main control room (MCR). However, they state that some new cables will be required and plan to accommodate this with a new raised floor in the MCR. Achieving the goal of no new cable pulling (and no new raised floor in the MCR) is very likely to be achieved with the CDM for several reasons:

1. The CDM employs single point data acquisition. This means that for every field input there is only a single input module to interface the signal to the digital system (i.e., there is no analog distribution of

field inputs to different input modules for different controllers or systems). Similarly, for every interface from the digital system to plant components there is only one output module. Therefore, if two digital systems control the same plant component, such as for the PSS and DAS, the digital outputs are combined into a single output module.

2. Analog input modules (AIM) and component interface modules (CIM) are compact and environmentally hardened. They can be located within existing cabinets, within the main control boards or within motor control centers and switchgear cubicles. This eliminates the need to run new cables to the AIMs and CIMs.
3. All interfaces between digital controllers within the CDM digital architecture employ digital data communications. Hardwired connections are not needed to ensure response time performance or independence.

CONTROLLING ESSENTIAL SYSTEMS

A few systems, such as residual heat removal, cooling water and HVAC are needed during the main outage. The compact OCs of the CDM facilitate this quite well because they can be installed in the existing MCR without disturbing the current bench board analog HSI for these systems. Then these systems can be transferred to the new digital controls and HSI one division at a time, ensuring that at least one division remains operable at all times in either its analog or digital configuration.

EPRI suggests various solutions to ensure temporary I&C and HSI remain available for these systems, including the division-by-division approach described above for the CDM. However, EPRI cautions that the space in the existing control room as well as current dedicated consoles (consoles welded to floor) may not be amenable to this solution. The compact HSI and minimum I&C equipment of the CDM overcomes this caution.

EQUIPMENT MINIMIZATION

The EPRI report emphasizes the importance of minimizing the I&C and HSI equipment that must be installed to achieve the lowest modernization cost and the shortest installation schedule. While EPRI presents an efficient I&C/HSI design (vintage 2003), the following features of the CDM (vintage 2018) reduce I&C and HSI equipment even further:

1. The CDM employs KVM switching which reduces the number of VDUs in the MCR and remote shutdown room (RSR), and eliminates the conventional DAS control panel in the MCR.
2. The CDM has no gateways to facilitate inter-division digital data communication. All controllers have built-in communication modules that comply with the inter-division communication guidance in ISG-04.
3. The EPRI MCR HSI design include two selectable large screen displays to facilitate operating crew interaction. The CDM facilitates crew interaction by allowing operators to share any VDU display, including corresponding pointer movements, with any other operators or with personnel outside the MCR (e.g., at the technical support center or emergency offsite facility). Therefore, there is no need for large screen selectable displays.
4. EPRI describes two methods of controlling safety components from non-safety VDUs – one employs additional confirm switches, the other employs additional qualified flat panel displays (FPD). In the CDM, safety components are controlled directly from non-safety VDUs with no additional hardware. Instead software-based priority logic within the safety controllers is credited to ensure functional independence; this CDM method has been previously licensed for the US-APWR.

5. The CDM employs single point data acquisition, as describe in Section 7.2. This reduces the number of I/O modules needed for the digital modernization. This is especially important for PCS and DAS functions that share the same measurement channels with the PSS (i.e., only the PSS has analog input modules for these measurement channels).

6. EPRI describes a distributed control system (DCS) with redundant safety and non-safety controllers within each safety and non-safety division to enhance system availability and facilitate on-line testing. The CDM employs redundancy between divisions, not within a division. This results in a ~50% reduction in the number of digital controllers.

   The CDM achieves high availability using non-redundant digital controllers with very long MTBF and very short MTTR. Very long MTBF is achieved using modern controllers with large scale integration and low heat producing electronics. Very short MTTR is achieved through a combination of documented ~100% self-diagnostic coverage and a high degree of plant-wide standardization that facilitates failed module replacements by plant operators. Redundant controllers are employed in the CDM only where necessary to prevent unbounded CCFs.

   The CDM requires no on-line testing. Most manual periodic surveillance tests are replaced with automated self-tests. The few manual tests that remain can be conducted during refueling outages.

7. EPRI describes NSSS and BOP control system controllers that are separate from component logic system controllers. This reflects the historical separation of continuous control and discrete state control in the existing analog I&C architecture. For the CDM continuous and discrete control for the same plant system are combined in one controller, thereby reducing the number of controllers required.

8. EPRI describes a DAS with two controllers whose outputs are wired in a 2oo2 configuration to prevent spurious actuation. The CDM employs only one DAS controller. Spurious actuation is prevented.

9. In the EPRI design, the existing SOE recorders and cable interfaces to I&C safety and non-safety systems are retained. Even though existing cables can be reused, this requires additional digital outputs from the new digital systems that must be installed and connected, and these outputs and the SOE inputs must be maintained for the life of the plant. The CDM does not require these cables or output modules, because events are time stamped within each PSS, DAS and PCS controller.

10. To prevent spurious RT, the EPRI configuration reconfigures the existing reactor trip breakers (RTBs) with new cable interfaces to achieve a selective 2oo4 configuration. The CDM prevents spurious actuation, without changing the existing 1oo2 two division RTB configuration. Instead the CDM employs a unique energize-to-actuate interface from each division, with fail-safe actuation at the system level from both divisions.

11. For each of the four safety divisions, EPRI describes Process Protection Controllers that are separate from Process Logic Controllers. This reflects the historical separation of process protection system cabinet from the solid-state protection system cabinet. For the CDM, both functions are combined in one controller, thereby reducing the number of controllers required.

12. EPRI describes a CIM with built-in controls and indicators to facilitate post installation testing of field interface connections. The CDM CIMs have no built-in HSI, facilitating a more compact CIM that provides more flexibility for distributed mounting. Post installation testing is facilitated by temporarily connecting the CIM to a portable tablet computer.

13. EPRI describes the environmental limitations of their CIM, which precludes its location in uncontrolled environments, such as within motor control centers. The CDM CIM is hardened for this type of uncontrolled environment.
14. EPRI describes a maintenance, test and gateway interface controller within each safety channel and within each safety train (i.e., six total). In the CDM these functions are built-in to the PSS PPPs and CCPs; therefore these additional separate controllers are not required.

KEY ASSUMPTIONS

EPRI defines several key assumptions to achieve a one-step modernization in 30 days. The following assumptions are favorably affected by the CDM.

1. *All necessary new cables have been pulled prior to the outage.* As described in Section 7.2 above, the CDM minimizes the need for new cables, making this assumption readily achievable.
2. *The raised flooring in the MCR can be installed prior to the outage.* By minimizing the need for new cables, the CDM eliminates the need for a raised floor in the MCR.
3. *The modernized systems (controllers, I/O modules, circuits, software logic, interfaces between new systems, etc.) are all fully tested in the factory. The systems include self-diagnostics features to detect failures of the controllers, the communication networks, the multiplexed I/O busses, etc. Therefore installation tests will only confirm (via appropriate overlap testing) that the proper connections are made to existing circuits and that the new equipment is able to interface to the circuits*. The CDM self-testing is documented through a failure modes and effects analysis (FMEA) to achieve ~100% coverage. In addition, the CDM has no hardwired connections internal to the I&C/HSI architecture; all interfaces are continuously self-tested digital communication interfaces. Therefore, the post installation tests are limited primarily to the interface of plant instruments (e.g., transmitters, RTDs) and plant components (e.g., solenoid valves, motor control centers).

KEY CONCERNS

A key concern identified by EPRI is the number of people that must work concurrently within the confined space of the electrical equipment rooms. EPRI cautioned that this has the potential to add 10 more days to the "best-case" 30-day modernization schedule. The CDM is expected to eliminate the need for this 10 day contingency due to the following attributes:

1. Due to the elimination of controller redundancy within the same division, the CDM requires installation of many fewer controllers in each equipment room, as discussed above.
2. Due to the use of digital data communications for all inter-controller interfaces, the CDM requires fewer I/O connections, as discussed above.

Fewer controllers and connections to install requires fewer people to install them.

Another key concern identified by EPRI is the need for additional post installation testing. The CDM self-testing minimizes the need for these tests. In addition, it is important to note that the simulator employs emulations of the actual CDM I&C/HSI system software. Since the simulator does not recode that software, the simulator accurately reflects the expected performance of the CDM I&C/HSI system in conjunction with the dynamic fidelity of the simulator's plant models.

While having no post installation testing is unrealistic, EPRI's 14-day post installation test period is certainly considered "worst case" with very high confidence.