ELECTRIC POWER
RESEARCH INSTITUTE

2013 TECHNICAL UPDATE

# Emergency Diesel Generator Digital Control System Upgrade Requirements

# Emergency Diesel Generator Digital Control System Upgrade Requirements

All or a portion of the requirements of the EPRI Nuclear Quality Assurance Program apply to this product.

YES [✓ NO]

EPRI Project Manager
R. Rusaw

ELECTRIC POWER RESEARCH INSTITUTE

3420 Hillview Avenue
Palo Alto, CA 94304-1338
USA

PO Box 10412
Palo Alto, CA 94303-0813
USA

800.313.3774
650.855.2121

askepri@epri.com

www.epri.com

**3002002098**

Technical Update, December 2013

## DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

**EXCEL Services Corporation**

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS **NOT** SUBJECT TO THE REQUIREMENTS OF  10 CFR PART 21.

**This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.**

**NOTE**

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or
e-mail askepri@epri.com.

Electric Power Research Institute, EPRI, and TOGETHER…SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

Copyright © 2013 Electric Power Research Institute, Inc. All rights reserved.

# Acknowledgments

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

EXCEL Services Corporation
11921 Rockville Pike, Suite 100
Rockville, MD 20852

Principal Investigators
P. Golub
G. Lang

This report describes research sponsored by EPRI.

EPRI extends a special thanks to Steve Greul of Fairbanks Morse Engine for his contributions to this report.

This publication is a corporate document that should be cited in the literature in the following manner:

*Emergency Diesel Generator Digital Control System Upgrade Requirements.*
EPRI, Palo Alto, CA: 2013.
3002002098.

# Abstract

This interim report documents the development of system requirements for a digital control system upgrade to the station emergency diesel generators (EDGs). Operators of nuclear power plants (NPPs) must be able to replace and upgrade equipment in a cost-effective manner while continuing to meet safety and reliability requirements and controlling modification costs. Upgrades to plant equipment—especially instrumentation and control (I&C) systems—typically involve replacement of analog devices with more modern digital technology. However, the use of digital technology has identified new design and licensing issues.

This report will help NPP operators design, license, and implement digital upgrades to the station EDGs. It focuses on the qualification methodology to meet the regulatory requirements of defense-in-depth and common cause failures of digital control systems. The report addresses all relevant system requirements and serves as supporting documentation for future license amendment requests by member utilities interested in installing digital control systems to address reliability and obsolescence issues.

**Keywords**
Digital systems
Digital systems licensing
Emergency diesel generator control systems
Instrumentation and control (I&C) systems
Licensing
Nuclear power plants (NPPs)

# Table of Contents

# List of Figures

# List of Tables

# Section 1: Introduction

This report provides a generic design and licensing basis for the replacement of an analog emergency diesel generator (EDG) start-stop instrumentation and control (I&C) system with a digital control system at nuclear power plants (NPPs). The purpose of the control system I&C replacement is to address analog system reliability and obsolescence issues. This report can be used in conjunction with a design modification and licensing action, such as a license amendment request (LAR). This report, combined with plant-specific logic and design information, is intended to provide sufficient input for generation of functional and systems requirements specifications.

This report is vendor-neutral, although it considers field-programmable gate arrays (FPGAs) as the replacement technology for the existing relay-based EDG start-stop logic. FPGAs were selected as the replacement technology due to the difficulty and expense associated with gaining regulatory approval for the alternative—microprocessor-based systems. FPGAs offer greater simplicity of design and potentially easier regulatory approval.

The simplicity referred to here comes from the absence of hardware and software components that are not directly involved in performing the primary I&C functions but are not independent, therefore possibly interfering with the I&C functions. Examples are operating systems, peripheral hardware and software and associated drivers, and ancillary functions that may be desired (for example, self-testing and diagnostics) but are implemented in such a way that they could impact the I&C functions. These additional, potentially interdependent hardware and software components complicate the design, assessment of reliability, and safety justification [1].

The safety-related portion of the EDG start-stop control logic is relatively simple and currently implemented at operating plants using relay logic. This report proposes to replicate that relay logic on an FPGA without changing the logic or adding functionality. The combination of simplicity and limited scope is intended to ease the burden of demonstrating adequate reliability and safety for an FPGA-based solution.

The guidance in this report builds on the information about FPGA applications in NPPs documented in the EPRI report *Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems* [1]. Appendix B provides an overview of the FPGA technology and its advantages.

## 1.1 Acronyms and Abbreviations

The following list defines acronyms and abbreviations as they are used in this report:

| | |
|---|---|
| ac | alternating current |
| ANSI | American National Standards Institute |
| AOO | anticipated operational occurrence |
| BISI | bypassed and inoperable status indication |
| BTP | Branch Technical Position (NRC) |
| CCF | common-cause failure |
| CFR | Code of Federal Regulations |
| D3 | diversity and defense-in-depth |
| EDG | emergency diesel generator |
| EPRI | Electric Power Research Institute |
| ESF | engineered safeguard feature |
| ESFAS | emergency safeguard feature actuation system |
| FMEA | failure modes and effects analysis |
| FPGA | field-programmable gate array |
| GDC | General Design Criteria |
| HMI | human-machine interface |
| I&C | instrumentation and control |
| IEEE | Institute of Electrical and Electronics Engineers |

| | |
|---|---|
| ISG | Interim Staff Guidance (NRC) |
| kVac | kilovolt(s) alternating current |
| LAR | license amendment request |
| LOOP | loss of off-site power |
| MCR | main control room |
| NPP | nuclear power plant |
| NRC | U.S. Nuclear Regulatory Commission |
| RG | Regulatory Guide (NRC) |
| SAR | Safety Analysis Report (NRC) |
| SBO | station blackout |
| SE | Safety Evaluation (NRC) |
| Std. | standard |
| TS | Technical Specification |

# Section 2: Scope

The scope of this report covers the replacement of the safety-related portions of the EDG start and stop logic. It does not include replacement of the voltage regulator, synchronization system, or load sequencing logic, nor does it include the loss of off-site power (LOOP) undervoltage relay voting logic. No other portions of the EDG's mechanical components, auxiliary systems, or electrical components are affected. The existing EDG control logic relays would be replaced by FPGAs. The scope assumes reuse of existing control cabinet terminal blocks and wiring to/from existing terminal blocks to plant equipment. Existing main control room (MCR) indications and controls are maintained and connected to the new FPGAs, and existing connections to the plant's computer or other data collection systems are maintained and established with the new FPGAs. In order to minimize cost and limit the project's risk, existing plant licensing bases are maintained as much as possible.

The scope is intentionally minimal, including only select safety-related logic functions. Although there are many new features that a simple digital system can offer (for example, additional diagnostic capability, historian functions, and network communications), the proposed upgrade scope only replaces existing functions and does not add new ones. The reason for the limited scope is to minimize the cost, construction impact, and licensing design bases changes and to increase regulatory certainty associated with any approvals for licensing actions.

# Section 3: Background

NPPs' EDGs are large diesel engines coupled to electric generators that provide power to plant safety and control systems when required. Emergency diesel generators are critical safety components of Generation II NPPs because they provide the electrical power necessary to activate and control reactor cooling and safety systems following a LOOP event and prevent a station blackout (SBO). Generally, a reactor unit is equipped with two to four Class 1E (that is, one per train or one per division), physically separated EDGs whose control systems are isolated and do not rely on common interconnection. In some installations, multi-unit plants implement the capability to cross-connect EDGs between reactor units.

Each EDG includes both safety-related and nonsafety-related components. The safety-related components include the diesel engine, generator, automated control system (including the automatic voltage regulator), and a subset of sensors. The nonsafety-related components are subsystems that are not directly related to the safety-related function of the EDG, such as ventilation and the fuel supply system.

## 3.1 Description of the EDG Startup-Shutdown System

See Figures 3-1 and 3-2 for generic start and stop logic diagrams. Note that these are representative logic diagrams based on various operating NPPs' EDGs. Individual utilities are required to develop their plant-specific EDG logic for implementation of the FPGAs.

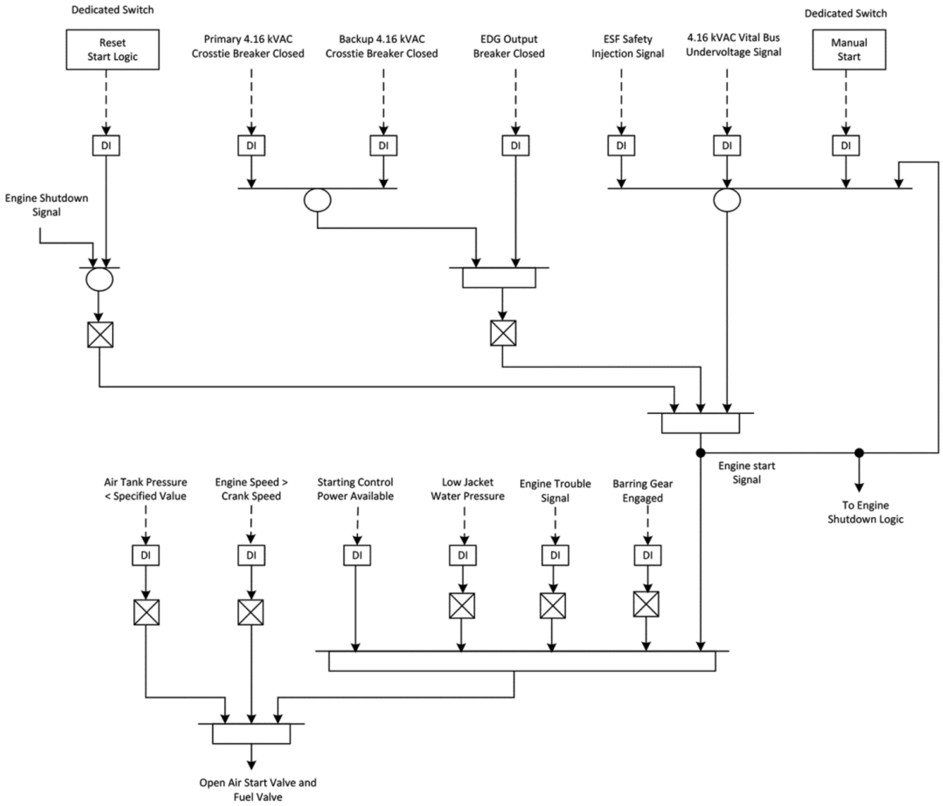
Dedicated Switch
Reset Start Logic
Primary 4.16 kVAC Crosstie Breaker Closed
Backup 4.16 kVAC Crosstie Breaker Closed
EDG Output Breaker Closed
ESF Safety Injection Signal
4.16 kVAC Vital Bus Undervoltage Signal
Dedicated Switch
Manual Start
DI
Engine Shutdown Signal
Engine start Signal
To Engine Shutdown Logic
Air Tank Pressure < Specified Value
Engine Speed > Crank Speed
Starting Control Power Available
Low Jacket Water Pressure
Engine Trouble Signal
Barring Gear Engaged
Open Air Start Valve and Fuel Valve

*Figure 3-1*
*Engine startup functional logic*

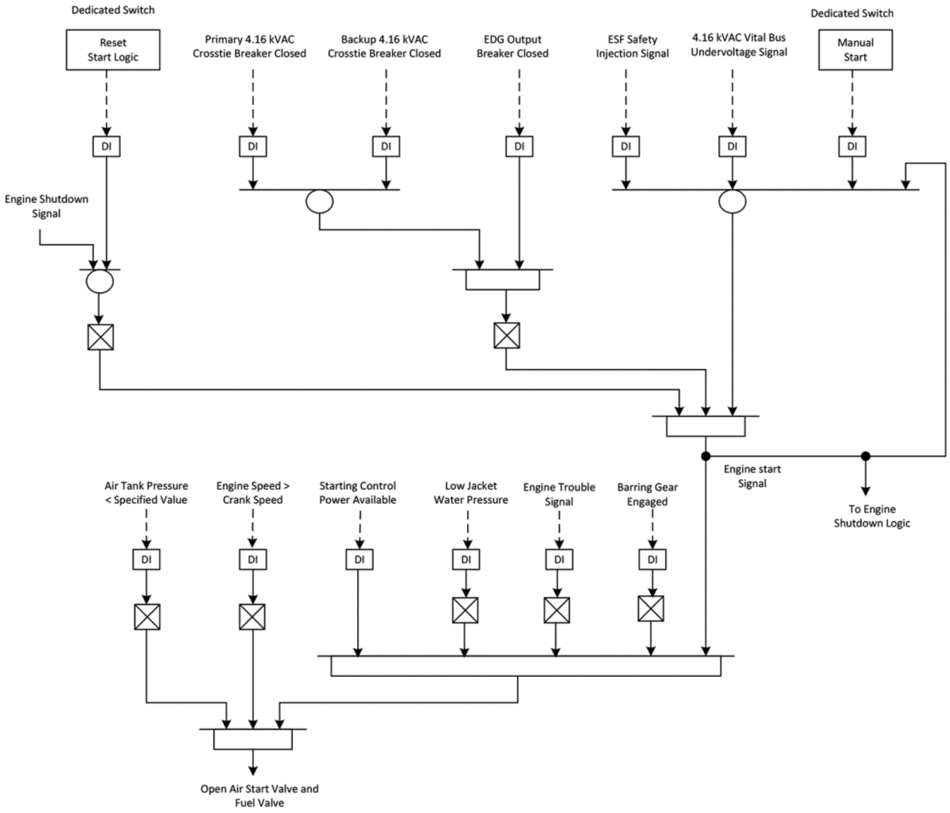
Dedicated Switch
Reset Start Logic
Primary 4.16 kVAC Crosstie Breaker Closed
Backup 4.16 kVAC Crosstie Breaker Closed
EDG Output Breaker Closed
ESF Safety Injection Signal
4.16 kVAC Vital Bus Undervoltage Signal
Dedicated Switch
Manual Start
DI
Engine Shutdown Signal
Engine start Signal
To Engine Shutdown Logic
Air Tank Pressure < Specified Value
Engine Speed > Crank Speed
Starting Control Power Available
Low Jacket Water Pressure
Engine Trouble Signal
Barring Gear Engaged
Open Air Start Valve and Fuel Valve

*Figure 3-2*
*Engine shutdown functional logic*

A representative diesel start functional logic is provided in Figure 3-1. An engine start signal is generated when all of the following conditions are met:

- There is a 4.16-kVac undervoltage signal, engineered safeguard feature actuation signal (ESFAS), or manual start signal.
- The EDG output breaker is open, or the primary 4.16-kVac crosstie breaker is open and the backup 4.16-kVac crosstie breaker is open.
- The manual start reset signal is not active.

The engine start signal is latched in, and the capability must be reset by the operator from the control panel. The engine start signal is an input to the engine shutdown logic.

The air start valve and fuel valve are opened if all of the following conditions are met:

- The engine start signal is active.
- Starting control power is available.
- The jacket water temperature is not low.

- The engine trouble signal is not active.
- The engine speed is not greater than the crank speed.
- The air tank pressure is greater than a specified value.

After the air start valve and the fuel valve are opened, the diesel begins to crank powered from the compressed air supply. If the diesel is successful in starting, the engine speed will exceed the crank speed and the signal to the air start valve and is de-activated to conserve the remaining air supply. If the diesel is not successful in starting, the signal to the air start valve and the fuel valve is de-activated when the pressure in the compressed air tank decreases below a specified value. The pressure setpoint is selected such that there is sufficient compressed air available in the tank for the operator to attempt to manually start the diesel.

The emergency shutdown functional logic is illustrated in Figure 3-2. An engine trouble signal occurs if the manual shutdown reset signal is not active and one of the following conditions is met:

- The lube oil pressure is low.
- The jacket water temperature is high.
- Engine overspeed exists.
- A generator differential current exists.

The engine trouble signal is latched in and must be manually reset by the operator from the control panel. The engine trouble signal is an input to the logic for opening the air start valve and the fuel valve. An engine shutdown signal is generated if the engine trouble signal is active or the manual shutdown signal is active but the engine start signal is not active. The engine shutdown signal opens the fuel shutdown valve and energizes the fuel stop valve.

Figures 3-1 and 3-2 provide representative engine start and shutdown functional logic. Many variations of this logic exist in operating plants. If the decision is made to upgrade the diesel startup and shutdown logic, the plant must first generate the existing functional logic.

## 3.2 EDG Support Systems

The following systems are required to support the operation of the EDGs but are outside the scope of the EDG startup/shutdown logic and this report:

- Voltage regulation
- Diesel engine lube oil system
- Diesel engine combustion air and exhaust system
- Diesel engine cooling system
- Diesel engine fuel oil system

## 3.3 EDG Interface Systems

Figure 3-3 shows the EDG replacement control system interfaces of various plant equipment. These include the following:

- Main control board signalization (indicators and status lights)
- Local control panel signalization (indicators and indications)
- Plant computer
- Plant alarm system
- Local control switches
- Remote control switches
- Diesel process variable inputs
- ESFAS safeguards signal
- 4160-Vac vital bus undervoltage signal
- Non-Class 1E vital bus supply breakers
- EDG output breaker to 4160-Vac vital bus

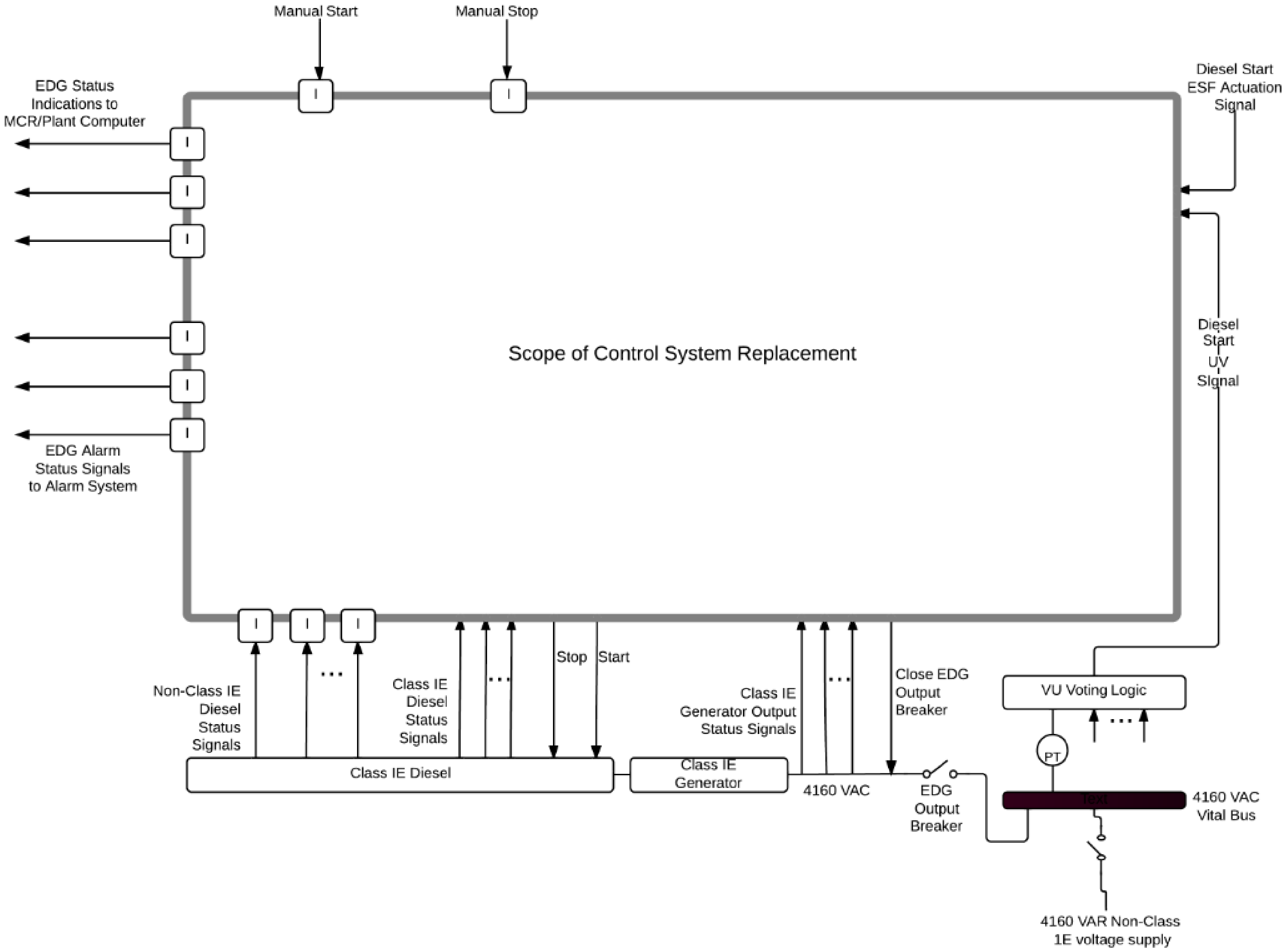
Manual Start
Manual Stop
EDG Status Indications to MCR/Plant Computer
Diesel Start ESF Actuation Signal
I
Scope of Control System Replacement
Diesel Start UV Signal
EDG Alarm Status Signals to Alarm System
Stop
Start
Non-Class IE Diesel Status Signals
Class IE Diesel Status Signals
Class IE Generator Output Status Signals
Close EDG Output Breaker
VU Voting Logic
PT
Class IE Diesel
Class IE Generator
4160 VAC
EDG Output Breaker
Text
4160 VAC Vital Bus
4160 VAR Non-Class 1E voltage supply

*Figure 3-3*
*EDG replacement control system interfaces*

# Section 4: Regulatory Bases

In order to minimize regulatory uncertainty, one goal of an EDG control system I&C replacement project is to maintain the existing plant licensing basis for the functionality of the EDG control systems as much as possible. For example, if the existing plant licensing basis for an EDG unit providing backup Class 1E power supply following a LOOP event were IEEE Std. 387-1977, the guidance provided in that version of the standard should be maintained as the plant licensing basis.

However, for the I&C design aspects of the EDG control system replacement, current regulatory guidance and industry standards must be met. For example, for the safety system design, IEEE Std. 603-1991 (which is referenced in 10CFR50.55a[h]) and all associated daughter standards must be met.

The EDG control system I&C replacement previously described must comply with U.S. regulations, the General Design Criteria (GDC) of Appendix A of 10CFR50, U.S. Nuclear Regulatory Commission (NRC) Regulatory Guides (RGs), industry standards, and other documents used in the design of systems as described in this section. Although this report does not address specific European or other countries' regulatory requirements, the basic principles of minimizing scope, minimizing construction impact, and maintaining existing licensing bases are generically applicable.

This report recommends compliance with the NRC regulatory documents listed in Sections 4.4 and 4.5. However, if a plant's individual design precludes compliance, an alternative analysis must be submitted with the licensing action. As noted, the digital replacement system must meet current regulatory requirements. However, the systems/signals that interface with the EDG are required to meet only the existing plant licensing basis. The boundary of the proposed replacement project must be precisely defined by the utility.

Appendix A contains additional compliance information for each document listed in Sections 4.1–4.6.

## 4.1 10CFR Part 50

The replacement EDG control system must comply with the following NRC Code of Federal Regulations (CFR) documents:

- 10CFR50.55a(a)(1)
- 10CFR50.55a(h)(3)
- 10CFR50.34f(2)(v)
- 10CFR50.59
- 10CFR50.63

## 4.2 10CFR Part 50, Appendix A, GDC

The replacement EDG control system must comply with the following GDC of 10CFR Part 50:

- GDC 1
- GDC 2
- GDC 4
- GDC 5
- GDC 13
- GDC 17
- GDC 18
- GDC 21
- GDC 22
- GDC 23
- GDC 24
- GDC 29
- GDC 33
- GDC 34
- GDC 35
- GDC 38
- GDC 41
- GDC 50

## 4.3 Staff Requirements Memoranda

The replacement EDG control system must comply with SECY 93-087, Sections II.Q and II.T.

## 4.4 Regulatory Guides

The replacement EDG control system must comply with the following NRC RGs:

- RG 1.6
- RG 1.9
- RG 1.22
- RG 1.32
- RG 1.47
- RG 1.53
- RG 1.62
- RG 1.75
- RG 1.81
- RG 1.97
- RG 1.105
- RG 1.118
- RG 1.152
- RG 1.153
- RG 1.155
- RG 1.168
- RG 1.169
- RG 1.170
- RG 1.171
- RG 1.172
- RG 1.173
- RG 1.180
- RG 1.204

## 4.5 NUREG-0800, Branch Technical Positions

The replacement EDG control system must comply with the following NRC Branch Technical Positions (BTPs) under NUREG-0800:

- BTP 7-8
- BTP 7-10
- BTP 7-11
- BTP 7-12
- BTP 7-14
- BTP 7-17
- BTP 7-18
- BTP 7-19
- BTP 7-21

## 4.6 Industry Standards

The replacement EDG control system must comply with the following industry standards:

- Institute of Electrical and Electronics Engineers (IEEE) Std. 308
- IEEE Std. 387
- IEEE Std. 603 and associated IEEE daughter standards
- IEEE Std. 7-4.3.2-2010 and associated IEEE daughter standards

# Section 5: Conformance to IEEE Std. 603

The following is stated in 10CFR50.55a(h)(3), Protection Systems:

> *Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995.*

IEEE Std. 603-1991 has been endorsed by RG1.153, Rev. 1. The scope of IEEE Std. 603-1991 indicates that one of the auxiliary supporting features of a safety system is power sources. In a typical operating NPP, an emergency diesel is provided to supply power to many emergency safeguard feature (ESF) components following a design basis event in coincidence with a LOOP. Also, Section 8.0, Power Source Requirements, of IEEE Std. 603-1991 provides the requirements for electrical power sources. It states the following:

> *Those portions of the Class 1E power system that are required to provide power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std. 309-1980.*

Based on the preceding, the circuitry associated with a diesel generator startup and shutdown logic must meet the requirements of IEEE Std. 603-1991.

The scope of this section is to demonstrate compliance of the diesel startup and shutdown logic to the requirements of IEEE Std. 603-1991.

# Section 6: Conformance to IEEE Std. 7-4.3.2

Section 1.2, Application, of IEEE Std. 603-1991 states the following:

> *The safety system criteria established herein are to be applied to those systems required to protect the public health and safety by functioning to prevent or mitigate the consequences of the design basis events. However, this standard does not apply to all of the systems, structures, and equipment required for complete plant safety, for example, fire protection systems.*
>
> *Guidance on the application of these criteria for safety systems using digital programmable computers is provided in IEEE/ANS 7-4.3.2-1982.*

Since the issuance of IEEE Std. 603 in 1991, the IEEE Working Group has published IEEE Std. 7-4.3.2-2003, which has been endorsed by Regulatory Guide 1.152, Rev. 3. IEEE Std. 7-4.3.2-2003 states the following in clause 5.3.3:

> *The software V&V effort shall be performed in accordance with IEEE Std. 1012-1998. The IEEE Std. 1012-1998 V&V requirements for the highest integrity level (Level 4) apply to systems developed using this standard.*

Therefore, the software associated with the diesel startup and shutdown logic is classified in the highest integrity category as defined in IEEE Std. 1012-1998.

The scope of this section is to demonstrate compliance of the diesel startup and shutdown logic to the guidance provided in IEEE Std. 7-4.3.2-2003.

# Section 7: NRC Interim Guidance DI&C-ISG-04

NRC Interim Staff Guidance (ISG) DI&C-ISG-04, "Task Working Group #4: Highly Integrated Control Rooms—Communications Issues (HICRc)," addresses the design and review of digital systems proposed for safety-related service in NPPs. This guidance document is broken up into three sections: Interdivisional Communications, Command Prioritization, and Multidivisional Control and Display Stations. Interdivisional Communications is not applicable because there is no transmission of data or information among components in different electrical safety divisions nor communications between a safety division and nonsafety-related equipment. The Multidivisional Control and Display Stations section is not applicable because there are no operator workstations used for the control of plant equipment in more than one safety division and for display of information from sources in more than one safety division.

The EDG control system I&C replacement should be designed in accordance with the guidance of the Command Prioritization section. Even though the diesel startup and shutdown logic does not perform intersystem prioritization of commands, the safety significance of the diesel startup and shutdown logic is similar to that of command prioritization. Therefore, this report provides the justification for applying the guidance specified in Section 2 of DI&C-ISG-04 to the diesel startup and shutdown logic. DI&C-ISG-04 states the following:

> *Accordingly the priority modules that combine the diverse actuation signals with the actuation signals generated by the digital system should not be executed in digital system software that may be subject to common-cause failures…*

This report intends to demonstrate that the digital-based system upon which the diesel startup and shutdown logic is implemented is not susceptible to a software common-cause failure (CCF). Additional description of each staff position is provided in Section 9, Diversity Considerations.

# Section 8: NRC Interim Guidance DI&C-ISG-06

NRC guidance document DI&C-ISG-06, "Task Working Group #6: Licensing Process," describes the process that the NRC may use in the review (against licensing criteria—the Standard Review Plan, NUREG-0800) of LARs associated with digital I&C system modifications in operating plants originally licensed under Part 50. This ISG also identifies the information that NRC staff may review for digital I&C equipment and when the information should be provided. License amendment requests for emergency diesel generator control system I&C replacements should be developed to support NRC review under the process described in DI&C-ISG-06.

DI&C-ISG-06 presents a phased approach where critical or fundamental system information is initially vetted through the NRC staff prior to undertaking subsequent steps in the digital I&C system development and the licensing process. The NRC staff encourages public meetings prior to submittal of the LAR in order to discuss issues regarding the system development scope. The intent of this activity is to reduce regulatory uncertainty through the early resolution of major issues that could challenge the staff's ability to assess the system's compliance with NRC regulations. Licensees planning EDG control system I&C replacement should follow the phased approach described in DI&C-ISG-06. This EPRI report describes the information that licensees will provide in Phase 0 and Phase 1. Table 8-1 denotes whether the DI&C-ISG-06 required documentation should be submitted by the utility or the vendor.

*Table 8-1*
*DI&C-ISG-06 required documents to be submitted by the utility or vendor*

| DI&G-ISG-06 Encl. B | DI&G-ISG-06 Tier | | | DI&G-ISG-06 Section Name | Submitted Documents | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | | Utility | Vendor |
| 1.1 | X | X | X | Hardware Architecture Descriptions | | X |
| 1.2 | | | X | Quality Assurance Plan for Digital Hardware | X | X |
| 1.3 | X | X | X | Software Architecture Descriptions | | X |
| 1.4 | X | X | X | Software Management Plan | X | X |
| 1.5 | X | X | X | Software Development Plan | | X |
| 1.6 | X | X | X | Software QA Plan | X | X |
| 1.7 | X | X | X | Software Integration Plan | | X |
| 1.8 | X | X | X | Software Safety Plan | X | X |
| 1.9 | X | X | X | Software V&V Plan | X | X |
| 1.10 | X | X | X | Software Configuration Management Plan | X | X |
| 1.11 | X | X | X | Software Test Plan | | X |
| 1.12 | X | X | X | Software Requirements Specification | X | X |
| 1.13 | X | X | X | Software Design Specification | | X |
| 1.14 | | X | X | Equipment Qualification Testing Plans (Including Electromagnetic Interference, Temperature, Humidity, and Seismic) | | X |
| 1.15 | X | X | X | Diversity and Defense-in-Depth (D3) Analysis | X | X |
| 1.16 | X | X | X | Design Analysis Reports | | X |
| 1.17 | X | X | X | System Description (to block diagram level) | | X |
| 1.18 | | X | X | Design Report on Computer Integrity, Test and Calibration, and Fault Detection | | X |
| 1.19 | X | X | X | System Response Time Analysis Report | | X |
| 1.20 | | X | X | Theory of Operation Description | | X |
| 1.21 | X | X | X | Setpoint Methodology | X | X |
| 1.22 | | | X | Vendor Software Plan | X | X |
| 1.23 | | X | X | Software Tool Verification Program | X | X |
| 1.24 | X | X | X | Software Project Risk Management Program | | X |
| 1.25 | | X | X | Commercial-Grade Dedication Plan | | X |
| 1.26 | X | X | X | Vulnerability Assessment | X | X |
| 1.27 | X | X | X | Secure Development and Operational Environment Controls | X | X |

DI&C-ISG-06 describes three different tiers of applications for approval of I&C system modifications. Tier 1 is applicable to LARs proposing to reference a previously approved topical report for a digital I&C platform or component(s). Tier 2 is applicable to LARs proposing to reference a previously approved topical report with deviations to suit the plant-specific application. Tier 3 is applicable to LARs proposing to use a new digital I&C platform or component(s) with no generic approval. Depending on the vendor selected, the guidance for the appropriate tier should be followed.

## 8.1 Phase 0: Pre-Application

The first regulatory interaction is the Phase 0 meeting described in DI&C-ISG-06. The purpose of this meeting is for the licensee to provide the overall design concept for the digital upgrade to the NRC prior to submittal of the LAR. From DI&C-ISG-06:

> *Prior to submittal of a LAR for a digital I&C upgrade, it is beneficial to have an overall design concept that adequately addresses NRC regulatory requirements and policy with regard to key issues (e.g., communication independence, defense-in-depth and diversity, demonstration of deterministic behavior, etc.). To this end, the NRC staff intends to use the public meeting process to engage licensees in a discussion of how their proposed digital I&C upgrade LAR should addresses: (1) key issues, such as defense-in-depth and diversity, (2) significant variances from current guidance, (3) NRC's determination of the appropriate "Tier" of review, and (4) other unique or complex topics associated with the proposed design.*

The simplicity of the FPGA and the emergency diesel generator application makes it relatively straightforward to address the key NRC regulatory topics referenced in this DI&C-ISG-06 section. Regarding communications independence, there are no interdivisional communications and no nonsafety-related data diodes. See Section 8.2.6 for a discussion of D3. The present report concludes that the EDG control system I&C replacement is not susceptible to software common-cause failures and therefore requires neither a diverse actuation system nor diverse manual actions.

## 8.2 Phase 1: Initial Application

The LAR should address all of the regulatory and design requirements necessary to allow the NRC to make a safety finding. From DI&C-ISG-06:

> *Once a licensee believes it has a design that adequately addresses NRC criteria, including, for example: (1) independence/redundancy, (2) defense-in-depth and diversity, (3) deterministic behavior, (4) variances to existing guidance, and (5) any unique or complex design features, it should prepare and submit a LAR (e.g., see Enclosure B, Information to Be Provided with the LAR). It is incumbent upon the licensee to identify any design features and concepts that may impact the NRC staff's preliminary assessment made during Phase 0. These features and concepts may adversely impact the NRC staff's acceptance of the LAR for review.*

> *To the extent possible, the LAR should address the criteria associated with the following areas, which are discussed in further detail in the referenced sections:*
> *– System Description (Section D.1)*
> *– Hardware Development Process (Section D.2)*
> *– Software Architecture (Section D.3)*
> *– Software Development Process (Section D.4)*
> *– Environmental Equipment Qualifications (Section D.5)*
> *– Defense-in-Depth & Diversity (Section D.6)*
> *– Communications (Section D.7)*
> *– System, Hardware, Software, and Methodology Modifications (Section D.8)*
> *– Compliance with IEEE Std. 603 (Section D.9)*
> *– Conformance with IEEE Std. 7-4.3.2 (Section D.10)*
> *– Technical Specifications (Section D.11)*
> *– Secure Development and Operational Environment (Section D.12)*

### *8.2.1 System Description (Section D.1)*

From DI&C-ISG-06:

> *The licensee's submittal should provide sufficient documentation and descriptions to allow the NRC staff to identify the hardware being used, how the hardware items function, how the various hardware items are interconnected, and any software in the system. The digital hardware items should be identified to the revision level. In those cases where the hardware, software, or their integration has previously been described by the vendor and evaluated by the NRC staff, the licensee should provide reference to the description and evaluation, including the ADAMS accession numbers if available. All changes to previously approved aspects should be evaluated (see Section D.8).*
>
> *The documentation and description should be on two levels. First, the individual channels or divisions should be described, including a description of the signal flows between the various hardware items. Second, there should be a description of the overall system, with particular emphasis on additional hardware items not included in the description of the channels or divisions, such as voters, communications with workstations or non-safety systems, bypass functions/switches, and diverse actuation systems.*

See Section 3.1 for a description of the EDG startup/shutdown system. This section of the license amendment request should describe the overall architecture of the emergency diesel generator control system replacement and identify the FPGA platform and any previous NRC reviews or safety evaluations (SEs). If there are changes to the applicability of the system as described in the NRC's SE, they should be identified and evaluated.

The description should confirm that the replacement does not include interdivisional communications, voting logic, communications with workstations or nonsafety-related systems aside from existing communications to plant systems, or diverse actuation systems.

### 8.2.2 Software Architecture (Section D.3)

From DI&C-ISG-06:

> *Reviewing the software architecture of the digital I&C system allows the NRC staff to understand how the high-level coded functions of the system interact to accomplish the safety function(s)…*
> *Some digital technologies, such as a field-programmable gate arrays (FPGAs), do not utilize software while the system is in operation (BTP 7-14 should be used to review the associated development process). Instead, these systems use software to generate a hardware layout to be implemented in the FPGA. In these situations, the NRC staff's review of the software tools used to generate, implement, and maintain the FPGAs should be guided by IEEE Std. 7-4.3.2- 2003 Clause 5.3.2.*

### 8.2.3 Defense-in-Depth and Diversity (Section D.6)

See Section 9 of the present report.

### 8.2.4 Compliance with IEEE Std. 603 (Section D.9)

See Section 5 of the present report, pertaining to conformance to IEEE Std. 603.

### 8.2.5 Conformance with IEEE Std. 7-4.3.2 (Section D.10)

See Section 6 of the present report, pertaining to conformance to IEEE Std. 7-4.3.2.

### 8.2.6 Technical Specifications (Section D.11)

There are no changes to the Technical Specifications as described in the standard technical specification NUREGs.

# Section 9: Diversity Considerations

The use of the same FPGA-based platform in the implementation of both trains of an EDG start-stop control system requires the plant to demonstrate that the FPGA-based system is not susceptible to a software common-cause failure. The regulatory guidance that should be followed is contained in NUREG-0800, Chapter 7, BTP 7-19; DI&C-ISG-04; and NUREG/CR-6303. The following sections assess how an FPGA-based EDG start/stop system conforms to each applicable criterion in those reports.

## 9.1 Conformance to BTP 7-19, Section B

Conformance to each of the design criteria discussed in BTP 7-19 is provided below.

### *9.1.1 Echelons of Defense*

The EDG start-stop system is considered to be part of the engineered safety features. This system is required to provide power to the ESFAS systems following a postulated loss of off-site power to the ESFs required for the mitigation of design basis events analyzed in Chapter 15 of the safety analysis report (SAR).

In addition, several parameters associated with the EDG start-stop system are monitored to indicate the status of the system post-event. These parameters could include the diesel's on/off status, the diesel cooling water jacket temperature, diesel speed, generator output voltage, frequency and current, and so on. The diesel is automatically started on one or more ESF system-level actuation signals (such as safety injection) or a LOOP signal. In order to meet the requirement of IEEE Std. 603-1991, clause 6.2, manual on/off controls are provided at the local EDG control panel and in the main control room.

### *9.1.2 Plant Critical Safety Functions*

This topic is not applicable to the EDG start-stop system upgrade.

### *9.1.3 Combining Reactor Trip System and ESFAS*

This evaluation assumes that the reactor trip system/ESF and EDG start-stop system are implemented on diverse platforms.

### 9.1.4 Four-Point Position

Point 1: The purpose of the Diversity Assessment section is to assess the diversity and defense-in-depth of the proposed EDG start-stop system digital replacement and its vulnerability to software CCFs.

Point 2: In this evaluation, it is assumed that the two trains of the EDG start-stop system shall be designed such that they are not susceptible to a software CCF. No diverse system will be installed to address any identified software CCFs.

Point 3: The EDG start-stop system digital replacement will not be susceptible to a software CCF. Accorindgly, no diverse system or functions shall be added.

Point 4: Manual controls exist on the EDG local panel and the MCR to start and stop the diesel. EDG parameters and status indications are monitored to assess the status of the system following a design basis accident. The parameters and status indications are displayed in the MCR and the local control panel. Because the EDG start-stop system is shown not to be susceptible to a postulated software CCF, the controls and monitored parameters are not required to be diverse from the digital replacement system.

### 9.1.5 Manual Initiation of Automatically Initiated Protective Actions Subject to CCFs

Manual dedicated controls are located on the local EDG panel and in the MCR to start and stop the diesel. These signals from the manual controls are input to the EDG start-stop system digital replacement module.

### 9.1.6 D3 Assessment

This section provides the D3 assessment of the EDG start-stop system digital replacement. This is accomplished by evaluating the compliance to BTP 7-19, ISG-04, and NUREG/CR-6303.

### 9.1.7 Diverse Means

The EDG start-stop system digital replacement shall be designed such that it is not susceptible to a software CCF.

### 9.1.8 Potential Effects of CCF: Failure to Actuate and Spurious Actuation

The EDG start-stop system digital replacement shall be designed such that it is not susceptible to a software CCF.

### 9.1.9 Design Attributes to Eliminate Consideration of CCFs

The FPGA-based emergency diesel generator start-stop system I&C replacement shall be designed with the following three key attributes, based on the guidance provided in DI&C-ISG-04:

- Simple logic.
- 100% testability. All software paths will be tested, and all combinations of inputs and outputs will be tested.
- Unused inputs will be grounded to preclude unwarranted interaction.

Details are provided in the evaluation of conformance to DI&C-ISG-04.

### 9.1.10 Conformance to DI&C-ISG-04, Section 2

Section 2 of DI&C-ISG-04 was originally written to address the design criteria of a priority logic module. A priority logic module is generally used to prioritize the commands from up to three subsystems, one of which may be non-Class 1E. Generally, one priority module exists for each ESF component. The output of the priority module is transmitted to the ESF component control logic. If a postulated failure occurs in a priority logic module, either no command signal or a degraded command signal would be transmitted to the ESF component. Similarly, for the EDG start-stop logic, if a postulated failure occurs in the control logic, either no command signal or a degraded command signal would be transmitted to the diesel; the worst consequence would be that the diesel would not start upon demand. If the failure occurred coincident with a LOOP event, the consequence would be an SBO.

Therefore, this report assumes that the EDG start-stop system has the same safety significance as a priority logic module—that is, a failure of the block could result in the loss of command to an ESF component. In the case of a priority logic module, a specific ESF component would not receive a signal. In the case of the EDG start-stop system, the diesel would not receive a start signal.

The conclusion is then reached that the staff positions specified in DI&C-IOSG-04 can also be applied to the EDG start-stop system. Conformance to each of the staff positions in DI&C-ISG-04 is covered in report Sections 9.1.10.1–9.1.10.10.

#### 9.1.10.1 Safety-Related Device

The EDG start-stop system is identified as a safety-related device or software function, is classified as Class 1E, and must meet all of the applicable requirements. The design process shall meet the 10CFR50 Appendix A and Appendix B requirements applicable to safety-related devices and software.

#### 9.1.10.2 Independent

The EDG start-stop system digital replacement shall not be installed on an FPGA-based platform in which other protective functions are implemented. Only the EDG start-stop system shall be installed on the digital devices.

#### 9.1.10.3 Safe State

This position is not applicable to the EDG start-stop system digital replacement.

#### 9.1.10.4 One or More Components

There shall be one FPGA device for each EDG train that is independent from the other train.

#### 9.1.10.5 Communication Isolation

There are no communication paths associated with the EDG start-stop system digital replacement. All input and output signals are hardwired to the device.

#### 9.1.10.6 Conformance to IEEE Std. 7-4.3.2

All software development in the design of the EDG start-stop system logic shall be developed in accordance with the guidance provided in IEEE Std. 7-4.3.2, Regulatory Guide 1.152, and BTP 7-14.

#### 9.1.10.7 Software Classification

The software associated with the EDG start-stop system shall be classified as Level 4 according to the guidance in IEEE Std. 1012-1998. The EDG start-stop system will meet all requirements applicable to Level 4 safety-related software.

#### 9.1.10.8 Development Testing

The following describes the testing strategy that should be used to meet the 100% testing criteria provided for the prioritization logic module. See Appendix B for a detailed example of the testing strategy applied to the EDG start-stop system logic.

DI&C-ISG-04 states the following in Section 2, Item 6, Command Prioritization:

> *Validation testing of the design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.*

The approach that should be taken is similar to the Technical Specification overlap testing currently used for analog safety systems. The priority logic module should be subdivided into software blocks. For example, one block may include the process variable input signals to the EDG start-stop logic that are logically combined in an OR gate. The output of the software block would be the output of the logical OR gate. The block would be tested for every possible combination of inputs. The output would be verified to be correct for each possible combination.

The logical OR output signal is the input to the next software block. Because all combinations of the inputs for the first software block have been verified, the input to the second software block has to be tested only for a logic 1 or logic 0, the two possible states of the output signal of the first software block.

The EDG start-stop logic would be subdivided into a finite number of software blocks, and each block would be tested as previously described. This approach would test all combinations of input signals and the states of all interior logic states, and the output signal(s) of each software block would be verified for all possible combinations of input signals. By performing this type of software overlap testing, the guidance provided in DI&C-ISG-04 is met. This testing strategy is not difficult to implement for a system that has relatively simple functional logic, which is true for the EDG start-stop logic. See Appendix B, Software Development Testing Methodology According to DI&C-ISG-04.

#### 9.1.10.9 Automatic Testing

There will be no continuously running self-diagnostic tests associated with the EDG start-stop system digital replacement module. Upper-level diagnostic indications will exist that monitor the status of the support systems, including one or more of the following conditions: loss of voltage to the cabinet, high cabinet temperature, and door-open indication.

The EDG start-stop logic shall be subjected to periodic manual testing at the frequency prescribed in the plant’s technical specifications.

#### 9.1.10.10 Separation

There shall be one EDG start-stop system logic per train and one EDG start-stop system logic per diesel. There are no interfaces between the logic elements of redundant trains. The logic associated with one train receives only input signals from that train.

### *9.1.11 Conformance to NUREG/CR-6303, Section 3*

Conformance to each of the guidelines identified in NUREG/CR-6303 is described in Sections 9.1.11.1–9.1.11.14.

#### 9.1.11.1 Guideline 1: Choosing Blocks

Because of the simplicity of the EDG start-stop system logic, the logic is encompassed in only one block. This standalone block has no interaction with any other train. The block's outputs are transmitted only to the diesel associated with that train.

#### 9.1.11.2 Guideline 2: Determining Diversity

The following assumptions are used in determining diversity:

- The EDG start-stop system is implemented on a platform that is diverse from the reactor trip system and the system-level ESF logic.
- The EDG start-stop system is implemented on an FPGA digital device.
- Both trains of the EDG start-stop system are implemented on independent FPGA digital devices.

NUREG/CR-6303 lists six different diversity features to investigate when determining the degree of existing diversity: design, equipment, functional, human, signal, and software. Based on the previous assumptions, no diversity exists between the two trains of the EDG start-stop system. However, BTP 7-19, Section 1.9, states the following:

> ***1.9 Design Attributes to Eliminate Consideration of CCF***
> *Many system design and testing attributes, procedures, and practices can contribute to significantly reducing the probability of CCF. However, there are two design attributes, either of which is sufficient to eliminate consideration of software logic based CCF:*
>
> *Diversity or Testability*
> 1. *Diversity – 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.*
> 2. *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).*

As covered in DI&C-ISG-04, Item 8, the EDG start-stop system logic is 100% tested due to the small number of logic gates and the relatively simple logic. Therefore, the conclusion can be drawn that the EDG start-stop system is not susceptible to a software CCF.

### 9.1.11.3 Guideline 3: System Failure Types

Guideline 3 describes three types of system failures, as follows:

- **Type 1: interaction between echelons of defense**. This type of failure is not applicable to an EDG start-stop system instrumentation and control replacement project because a failure in the control system echelon and the RT/ESF echelon of defense does not directly result in the generation of an EDG start-stop signal.
- **Type 2: failure of the safety I&C system to respond upon demand**. There is one EDG start-stop system per train and one EDG start-stop system per diesel. As demonstrated in the Guideline 2 analysis, the EDG start-stop system I&C replacement is not susceptible to a postulated software common-cause failure because of the simplicity of the logic and the capability to perform 100% testability. Therefore, a software CCF cannot result in the loss of both trains of the EDG start-stop system. One train might be lost due to a postulated single failure, but only one train is required for mitigation of plant SAR Chapter 15 design basis accidents.
- **Type 3: failure of sensors to detect abnormal conditions**. The EDG start-stop system receives diverse signals for starting the EDGs. These include an undervoltage signal on the 4.16-kVac vital buses and an automatic ESFAS. The ESFAS is generated by various process protection signals, which can include pressurizer pressure, steamline pressure, containment pressure, steamline flow, steamline differential pressure, reactor coolant system temperature, and so on. Accordingly, sufficient diversity exists in the signals that result in the generation of a diesel start signal.

### 9.1.11.4 Guideline 4: Echelon Requirements

For the purposes of this evaluation, it is assumed that the EDG start-stop system is implemented only on an FPGA digital device. The control systems, the reactor trip system, the remaining portion of the ESF system, and the monitoring system are implemented on one or more diverse platforms.

### 9.1.11.5 Guideline 5: Method of Evaluation

It is assumed in this evaluation that the EDG start-stop system logic in each train is composed of only one block of software. The block can either fail low (not respond upon a demand signal to start the diesel) or high (generate a spurious diesel start signal); there are no other credible failure modes within the block of firmware. For a postulated low failure, the diesel does not start on demand. However, the independent EDG start-stop system in the other train is not degraded by the assumed failure. Only one diesel is required for accident mitigation. For a postulated high failure, the diesel spuriously starts. Because an undervoltage signal is not generated from the 4.16-kVac vital buses, the EDG output breaker is not closed, and the operator is required only to manually stop the diesel.

#### 9.1.11.6 Guideline 6: Postulated Common-Mode Failure of Blocks

As demonstrated in the Guideline 2 analysis, the EDG start-stop system is not susceptible to a postulated software CCF. As such, a failure of both trains of the EDG start-stop system does not need to be postulated as a result of a postulated single failure or postulated software CCF. Only one train is assumed to fail due to a postulated single failure, as required by IEEE Std. 603-1991, clause 5.1.

#### 9.1.11.7 Guideline 7: Use of Identical Hardware and Software Modules

For the purposes of this evaluation, the software block in a train of the EDG start-stop system is identical to the software block in the other train. However, based on the Guideline 2 evaluation, the blocks are not susceptible to a software CCF.

#### 9.1.11.8 Guideline 8: Effect on Other Blocks

There is only one EDG start-stop system software block per train; therefore, its failure cannot be propagated to other downstream blocks.

#### 9.1.11.9 Guideline 9: Output Signals

Because the Guideline 2 evaluation demonstrated that the EDG start-stop system software block is not susceptible to a software CCF, the failure of the block is due solely to a postulated single failure in which one block would fail at a time. Therefore, one train of EDG start-stop logic would still be available for mitigation of design basis accidents.

#### 9.1.11.10 Guideline 10: Diversity for Anticipated Operational Occurrences

Because the Guideline 2 evaluation demonstrated that the EDG start-stop system logic is not susceptible to a software CCF, at least one train of diesel start-stop logic is available for anticipated operational occurrence (AOO) mitigation.

#### 9.1.11.11 Guideline 11: Diversity for Accidents

Because the Guideline 2 evaluation demonstrated that the EDG start-stop system logic is not susceptible to a software CCF, at least one train of diesel start-stop logic is available for design basis accident mitigation.

#### 9.1.11.12 Guideline 12: Diversity Among Echelons of Defense

As specified in the assumptions applied to this evaluation, the EDG start-stop system is assumed to be implemented on a diverse platform. Therefore, the EDG start-stop system platform is diverse from the platforms upon which the other echelons of defense are implemented.

### 9.1.11.13 Guideline 13: Plant Monitoring

The monitoring (status light, indication, alarm) signals associated with the EDG start-stop system are the same as those used for the currently installed system. The EDG start-stop system status signals (status lights, indications, alarms) are hardwired to the existing plant monitoring systems. No changes are made to the signals being monitored, and the plant interfaces with the EDG start-stop system. No changes are made to the presentation of the EDG start-stop system information in the MCR and the local control panel.

### 9.1.11.14 Guideline 14: Manual Operator Action

The EDG start-stop system receives hardwired 4.16-kVac vital bus undervoltage signals and one or more ESFAS automatic actuation signals, which automatically start the diesels. In addition, manual controls for starting and stopping the diesel are located on the local diesel control panel and in the MCR.

# Section 10: Failure Modes and Effects Analysis

A detailed failure modes and effects analysis (FMEA) must be performed on the plant's specific diesel startup and shutdown digital-based replacement system. Digital-based systems may introduce failure modes different from those addressed for an analog-based system.

In addition, a hazard analysis must be performed on digital-based systems to demonstrate that no postulated software-related failure could result in the system not meeting the single-failure criteria. The hazard analysis should be incorporated into the system FMEA.

The objectives of performing an FMEA on a plant's specific diesel startup and shutdown digital replacement system are to demonstrate that the hardware single-failure criterion is met and that no postulated single failure in the software could occur that would result in the system not meeting the single-failure criterion.

# Section 11: References and Bibliography

## 11.1 References

1. *Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems.* EPRI, Palo Alto, CA: 2011. 1022983.

## 11.2 Bibliography

Title 10 Code of Federal Regulations, Part 50 (10CFR50), Domestic Licensing of Production and Utilization Facilities. U.S. Nuclear Regulatory Commission, Washington, D.C.

10 CFR Part 50.34, "Contents of applications; technical information." U.S. Nuclear Regulatory Commission, Washington, D.C.

10 CFR Part 50.63, "Loss of all alternating current power." U.S. Nuclear Regulatory Commission, Washington, D.C.

10 CFR Part 50 Appendix A, General Design Criteria for Nuclear Power Plants. U.S. Nuclear Regulatory Commission, Washington, D.C.

IEEE Std. 603, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronic Engineers, Piscataway, NJ: 2009.

IEEE Std. 7-4.3.2-2010, IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Institute of Electrical and Electronics Engineers, Piscataway, NJ: 2010.

IEEE Std. 308, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronic Engineers, Piscataway, NJ: date based on plant licensing basis.

IEEE Std. 387, IEEE Standard Criteria for Diesel-Generator Units Applied as Standby Power Supplies for Nuclear Power Generating Stations, Institute of Electrical and Electronic Engineers, Piscataway, NJ: date based on plant licensing basis.

DI&C-ISG-04, Digital Instrumentation and Controls Task Working Group #2, Highly Integrated Control Rooms – Communications Issues, Interim Staff Guidance, Revision 1, US Nuclear Regulatory Commission, Washington, D.C.: 2009. http://www.nrc.gov/reading-rm/doc-collections/isg/digital-instrumentation-ctrl.html

DI&C-ISG-06, Digital Instrumentation and Controls Task Working Group #6, Licensing Process, Revision 1, US Nuclear Regulatory Commission, Washington, D.C.: 2009. http://www.nrc.gov/reading-rm/doc-collections/isg/digital-instrumentation-ctrl.html*Guideline on Licensing Digital Upgrades –TR-102348 Revision 1 – NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule*. EPRI, Palo Alto, CA: 2002.

NUREG/CR-6303, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems. U.S. Nuclear Regulatory Commission, Washington, D.C.: December 1994.

Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.53, Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.75, Physical Independence of Electric Systems. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.97, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.118, Periodic Testing of Electric Power and Protection Systems. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.152, Criteria for Programmable Digital Computers in Safety Systems of Nuclear Power Plants. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.153, Criteria for Safety Systems. U.S. Nuclear Regulatory Commission, Washington, D.C.

Regulatory Guide 1.155, Station Blackout. U.S. Nuclear Regulatory Commission, Washington, D.C.

# Appendix A: Compliance with Regulatory and Industry Standards and Guidance

The four tables in this appendix list the applicable regulations and compliance details for 10CFR50, including its General Design Criteria (see Table A-1); the NRC's Regulatory Guides (see Table A-2); NUREG BTPs (see Table A-3); and IEEE standards (see Table A-4).

*Table A-1*
*Compliance with regulations*

| Regulation | Compliance |
|---|---|
| 10CFR50.55a(a)(1) | The EDG control system I&C replacement shall be designed in accordance with 10CFR50.55a(a)(1). The EDG control system I&C replacement is defined as Quality Class Q. The EDG control system upgrade shall be designed, fabricated, erected, constructed, tested, and inspected commensurate with the requirements of 10CFR Part 50, Appendix B. |
| 10CFR50.34f(2)(v) | The EDG control system I&C replacement shall not affect the plant's compliance with 10CFR50.34(f)(2)(v). This is provided by compliance to clause 5.8.2 (system status indication) and clause 5.8.3 (indication of bypasses) of IEEE Std. 603. Information regarding bypassed and inoperable status (BISI) is presented below. The HMI interface with BISI will remain the same. |

*Table A-1 (Continued)*
*Compliance with regulations*

| Regulation | Compliance |
|---|---|
| 10CFR50.59 | The EDG control system I&C replacement shall be evaluated against the criteria in 10CFR50.59 to determine if prior NRC approval is required. Some considerations that should be addressed include, for example, potentially different failure modes of digital equipment versus analog equipment or older digital equipment, the effect of combining functions of previously separate devices into one digital device, and the potential for software CCFs. EPRI TR-1022983/NEI 01-01 provides guidance for performing this evaluation for digital upgrades. |
| 10CFR50.63 | The EDG control system I&C replacement shall be designed in accordance with 10CFR50.63 to meet the existing plant licensing basis. This requires that each light-water-cooled NPP "be able to withstand for a specified duration and recover from a station blackout." The specified station blackout duration shall be based on the following factors:<br>• The redundancy of the on-site emergency ac power sources<br>• The reliability of the on-site emergency ac power sources<br>• The expected frequency of loss of off-site power<br>• The probable time needed to restore off-site power |
| **10CFR Part 50, Appendix A, General Design Criteria (GDC)** | |
| GDC 1 | The EDG control system I&C replacement shall be designed in accordance with GDC 1 and the requirements of 10CFR50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Processing Plants." The vendor's compliance to 10CFR Appendix B is provided in the plant's quality assurance manual. |
| GDC 2 | The EDG control system I&C replacement shall be designed in accordance with GDC 2. Compliance with IEEE Std. 603, clause 5.4, demonstrates that the applicable I&C systems remain operable during and following natural phenomena applicable to the plant site. The EDG control system I&C replacement is designed as Seismic Category I. The EDG control system I&C replacement will be installed in the EDG rooms, which are designed to provide protection against other natural phenomena, such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches. |

*Table A-1 (Continued)*
*Compliance with regulations*

| Regulation | Compliance |
|---|---|
| **10CFR Part 50, Appendix A, General Design Criteria (GDC)** | |
| GDC 4 | The EDG control system I&C replacement shall be designed in accordance with GDC 4 and be capable of withstanding the effects of missiles and environmental conditions associated with normal, abnormal, and post-accident environmental conditions. |
| GDC 5 | The EDG control system I&C replacement shall be designed in accordance with GDC 5. The EDG control system upgrade shall be designed such that there will be no impact on the ability of any shared structures, systems, and components to perform their safety function. |
| GDC 13 | The EDG control system I&C replacement shall be designed in accordance with GDC 13. The EDG control system upgrade shall functionally replicate the existing EDG control system. The replacement EDG instrumentation and control system shall meet the requirements of IEEE Std. 603. |
| GDC 17 | The EDG control system I&C replacement shall be designed in accordance with GDC 17. The EDG control system shall be designed to meet the independence, separation, single failure, and testability at power criteria of IEEE Std. 603-1991.<br>Compliance with GDC 17 is demonstrated through meeting the following guidelines and IEEE standards:<br>• RG 1.6<br>• RG 1.9 (see also IEEE-387)<br>• RG 1.32 (see also IEEE-308)<br>• RG 1.53 (see also IEEE-379)<br>• RG 1.75 (see also IEEE-384)<br>• RG 1.153 (see also IEEE-603)<br>• RG 1.155 (SBO guidelines—see the existing plant licensing basis)<br>• RG 1.204 (see also IEEE-665, 666, 1050, and C62.23)<br>• NUREG/CR-0660 (Generic Letter 79-21) |

*Table A-1 (Continued)*
*Compliance with regulations*

| Regulation | Compliance |
|---|---|
| **10CFR Part 50, Appendix A, General Design Criteria (GDC)** | |
| GDC 18 | The EDG control system I&C replacement shall be tested as part of the integrated EDG system testing in accordance with GDC 18 and plant Technical Specifications. The EDG control system shall be designed with the capability to test periodically (1) the operational and functional performance of the control system and (2) the operability of the integrated system under conditions as close to design as practical the operational sequence from a postulated LOOP to the re-energization of the Class 1E vital buses from the EDG. |
| GDC 21 | The emergency diesel generator control system I&C replacement shall be designed in accordance with GDC 21. The EDG control system I&C replacement reliability must be factored into the overall on-site ac power reliability study as required by 10CFR50.63. The utility is required to demonstrate that the control system replacement supports the reliability goal of the existing on-site ac power system. Further guidance is provided in RG 1.155. |
| GDC 22 | The EDG control system I&C replacement shall be designed in accordance with GDC 22. The safety system should comply with the independence requirements of IEEE Std. 603-1991 and guidance provided in RG 1.153 and RG 1.75. Guidance is provided in RG 1.6 concerning the independence of on-site ac power sources from off-site ac power sources. |
| GDC 23 | The EDG control system I&C replacement shall be designed in accordance with GDC 23. The FMEA for the safety system shall include a failure analysis of the EDG control system. |
| GDC 24 | The EDG control system I&C replacement shall be designed in accordance with GDC 24. Electrical isolation, physical separation, and communication independence shall be maintained between the safety and nonsafety portions of the EDG control system in accordance with the independence requirements of IEEE Std. 603. |

*Table A-1 (Continued)*
*Compliance with regulations*

| Regulation | Compliance |
|---|---|
| **10CFR Part 50, Appendix A, General Design Criteria (GDC)** | |
| GDC 29 | The EDG control system I&C replacement shall be designed in accordance with GDC 29. Following a loss of off-site power, the EDG control system shall be designed to provide power to the ac vital buses to ensure that the protective equipment necessary for the mitigation of an anticipated operational occurrence (AOO) is available. |
| GDC 33 | The EDG control system I&C replacement shall be designed in accordance with GDC 33. Following a loss of off-site power, the EDG control system shall be designed to provide power to the ac vital buses to ensure that the reactor coolant makeup system necessary for the mitigation of an AOO or design basis event is available. |
| GDC 34 | The EDG control system I&C replacement shall be designed in accordance with GDC 34. Following a loss of off-site power, the EDG control system shall be designed to provide power to the ac vital buses to ensure that the residual heat removal system necessary for the mitigation of an AOO or design basis event is available. |
| GDC 35 | The EDG control system I&C replacement shall be designed in accordance with GDC 35. Following a loss of off-site power, the EDG control system shall be designed to provide power to the ac vital buses to ensure that the emergency core cooling system necessary for the mitigation of a design basis event is available. |
| GDC 38 | The EDG control system I&C replacement shall be designed in accordance with GDC 38. Following a loss of off-site power, the EDG control system shall be designed to provide power to the ac vital buses to ensure that the containment heat removal system necessary for the mitigation of a design basis event is available. |

*Table A-1 (Continued)*
*Compliance with regulations*

| Regulation | Compliance |
|---|---|
| **10CFR Part 50, Appendix A, General Design Criteria (GDC)** | |
| GDC 41 | The EDG control system I&C replacement shall be designed in accordance with GDC 41. Following a loss of off-site power, the EDG control system shall be designed to provide power to the ac vital buses to ensure that the containment atmospheric cleanup system (if applicable) necessary for the mitigation of a design basis event is available. |
| GDC 50 | The EDG control system I&C replacement shall be designed in accordance with GDC 50. Following a loss of off-site power, the EDG control system shall be designed to provide power to the ac vital buses to ensure that the reactor containment temperature and pressure are within design basis limits. |
| **Staff Requirements Memoranda** | |
| SECY 93-087<br>Section II.Q | A D3 analysis should be performed according to NUREG/CR-6303 to determine if any diverse design features are required to be added to the plant. See the Diversity Considerations section for additional information. |
| SECY 93-087<br>Section II.T | The plant alarms generated by the EDG control system should remain the same. The design of the plant alarm system is outside the scope of this upgrade. |

*Table A-2*
*Compliance with NRC Regulatory Guides*

| Regulatory Guide | Compliance |
|---|---|
| RG 1.6 | The EDG control system I&C replacement should be designed to meet the guidance of RG 1.6. The logic associated with each EDG control system should be independent from the control system associated with another division/train. |
| RG 1.9 | The EDG control system I&C replacement should be designed to meet the guidance of RG 1.9. The EDG control system I&C should be tested at the frequency specified in the plant's technical specifications. |
| RG 1.22 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.22. The control system I&C shall be tested as part of the integrated EDG system testing in accordance with RG 1.22 and the plant's technical specifications. |

*Table A-2 (Continued)*
*Compliance with NRC Regulatory Guides*

| Regulatory Guide | Compliance |
|---|---|
| RG 1.32 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.32. The EDG control system logic should be tested as part of the on-site ac power system. |
| RG 1.47 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.47. The EDG control system should be designed to provide bypassed and inoperable status indication for the EDGs based upon the existing plant HMI evaluation. |
| RG 1.53 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.53. The safety system should comply with the requirements of IEEE Std. 379-2000 for application of the single-failure criterion. |
| RG 1.62 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.62. The safety system should comply with the system-level manual initiation requirements of IEEE Std. 603-1991, clause 6.2. The design and location of the system-level EDG start-stop controls (such as the MCR and/or local control panel) should be based upon the existing plant human-systems interface evaluation. |
| RG 1.75 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.75. The safety system should comply with the independence requirements of IEEE Std. 384-1992. |
| RG 1.81 | For plants with a shared on-site power system between units, the guidance of RG 1.81 should be met. |
| RG 1.97 | The EDG control system should be designed to comply with the guidance of RG 1.97. The EDG control system status indications provided in the MCR should be determined from the existing plant licensing basis concerning post-accident monitoring instrumentation. |
| RG 1.105 | The EDG control system should be designed to comply with the guidance of RG 1.105. The setpoints associated with the EDG control system should be based upon the existing plant licensing basis. |
| RG 1.118 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.118. The safety system should comply with the requirements of IEEE Std. 338-1987 with respect to periodic testing of electric power and protection systems. |

*Table A-2 (Continued)*
*Compliance with NRC Regulatory Guides*

| Regulatory Guide | Compliance |
|---|---|
| RG 1.152 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.152. The EDG control system I&C replacement shall comply with the requirements of IEEE Std. 7-4.3.2-2003 with respect to the reliability and design requirements for microprocessor-based safety systems. |
| RG 1.153 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.153. The control system shall comply with the design requirements of IEEE Std. 603-1991. |
| RG 1.155 | The EDG control system I&C replacement should be designed to support the reliability goal of the existing on-site ac power system. |
| RG 1.168 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.168. The control system compliance to IEEE Std. 1012-2004 with respect to the verification and validation of safety system software should be described in the software program manual. The EDG control system software should be designed to Level 4 requirements. |
| RG 1.169 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.169. The control system compliance to IEEE Std. 828-2005 with respect to the configuration management plans for safety system software should be described in the software program manual. |
| RG 1.170 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.170. The control system compliance to IEEE Std. 829-2008 with respect to the test documentation of safety system software should be described in the software program manual. |
| RG 1.171 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.171. The control system compliance to ANSI/IEEE Std. 1008-1987 with respect to the unit's testing of safety system software should be described in the software program manual. |

*Table A-2 (Continued)*
*Compliance with NRC Regulatory Guides*

| Regulatory Guide | Compliance |
|---|---|
| RG 1.172 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.172. The control system compliance to IEEE Std. 830-1998 with respect to the preparation of software requirement specifications for safety system software should be described in the software program manual. |
| RG 1.173 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.173. The control system compliance with the requirements of IEEE Std. 1074-2006 with respect to the development processes for safety system software should be described in the software program manual. |
| RG 1.180 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.180 for acceptable methods to address the compatibility and susceptibility of electromagnetic and radio-frequency interference (EMI/RFI) and power surges on safety-related control systems. |
| RG 1.204 | The EDG control system I&C replacement should be designed to comply with the guidance of RG 1.204 for acceptable methods to address lightning protection of plant electric and I&C systems. |

*Table A-3*
*Compliance with NUREG-0800 BTPs*

| Regulatory Guidance Document | Compliance |
|---|---|
| BTP 7-8 | The EDG start-stop control system I&C replacement should be designed in accordance with the guidance of BTP 7-8. The safety system should comply with the requirements of IEEE Std. 603-1991, clauses 5.7 and 6.5. In addition, the safety system should be designed to support surveillance testing as described in the plant's technical specifications. |
| BTP 7-10 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-10. The control system should meet the existing plant compliance to RG 1.97. |

*Table A-3 (Continued)*
*Compliance with NUREG-0800 BTPs*

| Regulatory Guidance Document | Compliance |
|---|---|
| BTP 7-11 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-11. The control system should comply with the requirements of IEEE Std. 603-1991, clauses 4.7 and 5.6. Electrical isolation shall be maintained between the redundant portions of safety systems or between safety and nonsafety systems. |
| BTP 7-12 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-12. The control system should comply with the requirements of IEEE Std. 603-1991, clauses 4.4 and 6.8. The setpoints associated with the EDG control system should be based upon the existing plant licensing basis. |
| BTP 7-14 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-14. The control system software development lifecycle conformance to RG 1.28, 1.152, 1.168, 1.169, 1.170, 171.1, 1.172, 1.173, and NUREG/CR 6101 should be described in the software program manual. |
| BTP 7-17 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-17. The I&C portions of the control system should comply with the requirements of IEEE Std. 603-1991,clauses 5.1 and 5.7. The I&C portions of the control system should be designed to permit periodic testing of the EDG control system with the reactor operating at power or when shut down while retaining the capability of the control system to accomplish its safety functions. |
| BTP 7-18 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-18. The control system should comply with the requirements of RG 1.152, Revision 2. Software tools for developing application software should be qualified to a level commensurate with the system they are designed to support. If a commercial-grade digital control system is used, it should conform to the guidance presented in EPRI report TR-106439. |

*Table A-3 (Continued)*
*Compliance with NUREG-0800 BTPs*

| Regulatory Guidance Document | Compliance |
|---|---|
| BTP 7-19 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-19. A D3 analysis should be performed according to NUREG/CR-6303 to determine if any vulnerabilities to software CCFs need to be addressed. |
| BTP 7-21 | The EDG control system I&C replacement should be designed in accordance with the guidance of BTP 7-21. The control system should comply with the requirements of IEEE Std. 603-1991, clauses 4.4, 4.10, and 6.1. The control system should be designed such that the system response time is no longer than the response time of the existing EDG control system. |

*Table A-4*
*Compliance with industry standards*

| Industry Standard | Compliance |
|---|---|
| IEEE STD. 308 | The EDG control system I&C replacement should be designed in accordance with the guidance of the IEEE Std. 308 version of the standard that is referenced in the existing plant licensing basis. |
| IEEE STD. 387 | The EDG control system I&C replacement should be designed in accordance with the guidance of the IEEE Std. 387 version of the standard that is referenced in the existing plant licensing basis.<br>IEEE Std. 387-1995 supplements IEEE Std. 308-1991, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, in that it amplifies subclause 6.2.4 of that standard (Standby Power Supplies) concerning requirements for EDGs.<br>IEEE Std. 387-1995 provides the principal design criteria, design features, qualification considerations, and testing requirements for EDGs, including auxiliary equipment and controls used in the standby power supply of a nuclear facility. It states the following:<br>*4.5.2.1 Control Modes*<br>*The diesel-generator unit shall be provided with control systems, permitting automatic and manual control.*<br>*4.5.2.2 Automatic Control*<br>*Upon receipt of an emergency start-diesel signal, the automatic control system shall provide automatic startup and automatic adjustment of speed and voltage to a ready-to-load condition.*<br>*a. A start-diesel signal shall override all other generating modes and return control of the diesel-generator unit to the automatic control system.*<br>*b. An emergency start-diesel signal shall not override any manual non-operating modes such as those for repair and maintenance.*<br>The EDG control system I&C replacement must not change the plant's conformance to IEEE Std. 387. |
| | |

*Table A-4 (Continued)*
*Compliance with industry standards*

| Industry Standard | Compliance |
|---|---|
| IEEE STD. 603 and associated daughter standards | 10CFR Part 50.55a(h)(3), Protection Systems, states the following:<br>*Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995.*<br>IEEE Std. 603-1991 has been endorsed by Regulatory Guide 1.153, Rev. 1.<br>The scope of IEEE Std. 603-1991 indicates that one of the auxiliary supporting features of a safety system is power sources. In a typical operating nuclear power plant, an emergency diesel is provided to supply power to many ESF components following a design basis event in coincidence with a LOOP. Also, Section 8.0, Power Source Requirements, of IEEE Std. 603-1991 provides the requirements for electrical power sources. It states the following:<br>*Those portions of the Class 1E power system that are required to provide power to the many facets of the safety system are governed by the criteria of this document and are a portion of the safety systems. Specific criteria unique to the Class 1E power systems are given in IEEE Std. 309-1980.*<br>Based upon the above, the circuitry associated with a diesel generator startup and shutdown logic must meet the requirements of IEEE Std. 603-1991.<br>The scope of this section is to demonstrate compliance of the diesel startup and shutdown logic to the requirements of IEEE Std. 603-1991. |

*Table A-4 (Continued)*
*Compliance with industry standards*

| Industry Standard | Compliance |
|---|---|
| IEEE STD. 7-4.3.2-2010 and associated daughter standards | The EDG control system I&C replacement should be designed in accordance with the requirements of IEEE Std. 603 and the following associated IEEE standards:<br>• IEEE Std. 828-2006<br>• IEEE Std. 829-2008<br>• IEEE Std. 830-1993<br>• IEEE Std. 1012-2004<br>• IEEE Std. 1016-2009<br>• IEEE Std. 1028-2008<br>• IEEE Std. 1074-1995<br>Additional conformance information for IEEE Std. 7-4.3.2 can be found in Section 6 of the present report. |

# Appendix B: Software Development Testing Methodology According to DI&C-ISG-04

This appendix covers the implementation of the 100% testing strategy for the representative diesel startup and shutdown logic diagrams (see Figures 3-1 and 3-2). The following is an example of the 100% testing methodology. Once the representative logic diagrams are finalized (see Figure B-1 for a draft diagram), this section will be revised to describe them.

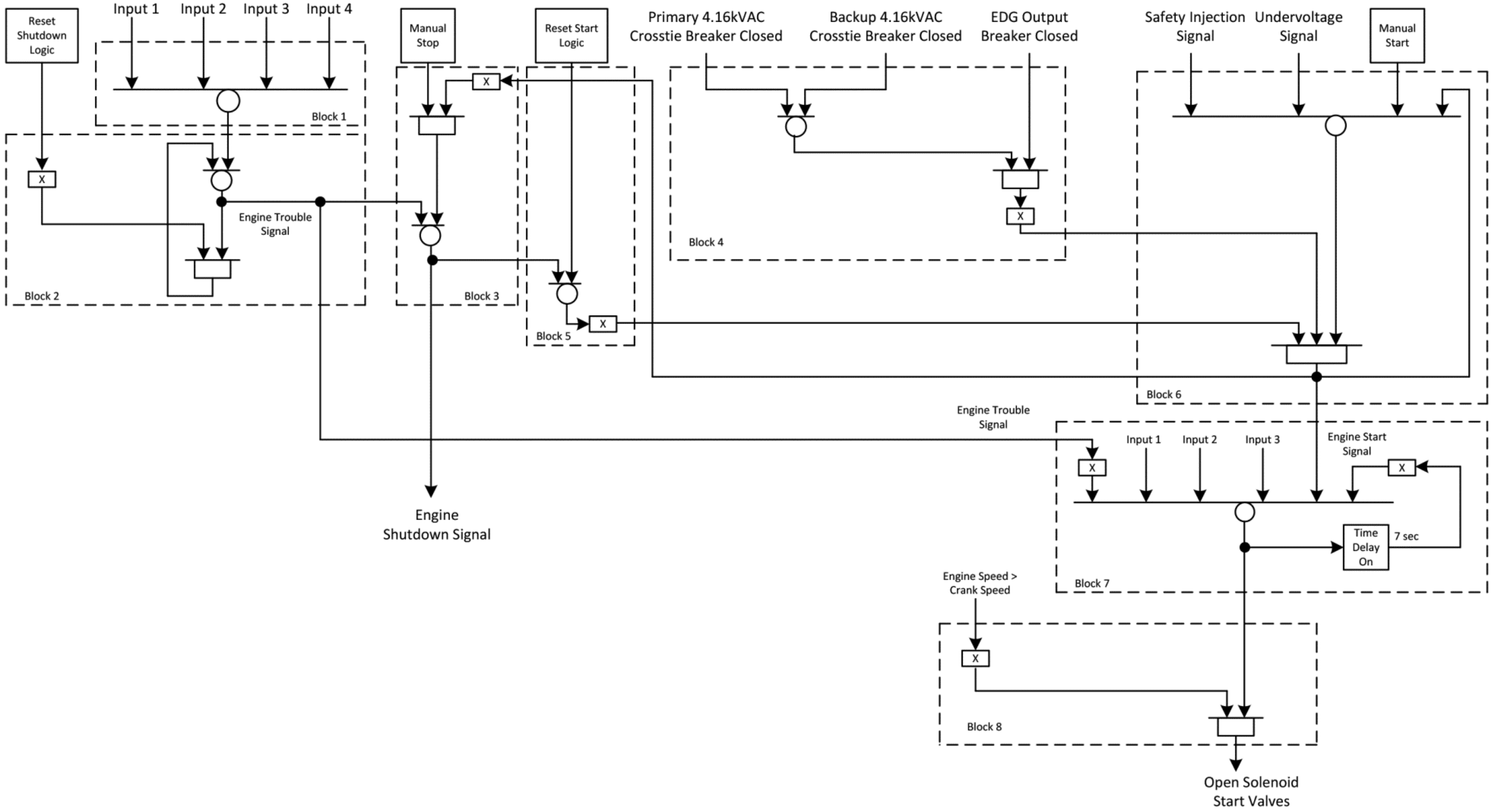

*Figure B-1*
*Example of 100% testability EDG start logic*

## B.1 A 100% Testing Strategy for Diesel Startup and Shutdown Logic

The following discussion provides the strategy for meeting the 100% testability guideline in DI&C-ISG-04 with respect to emergency safeguards diesel starting logic.

### B.1.1 Description of Diesel Startup and Shutdown Logic

Figure 3-1 provides a simplified logic for a typical diesel startup. Essentially, it consists of two sets of logic: a diesel starting logic and an engine shutdown logic.

The engine can be automatically or manually started. The automatic start signals are generally the safety injection actuation signal from the system-level ESFAS logic and an undervoltage signal derived from voltage measurements on the 4.16-kVac vital buses (voting performed in another system). The manual controls are generally located in the MCR and on the diesel local control panel. The automatic and manual signals are interlocked under certain conditions to preclude damage to the diesel upon starting. The crosstie breakers to the 4.16-kVac breaker must be open, and the diesel generator output breaker must be open.

Generally, two non-Class 1E power feeds to the 4.16-kVac vital bus can be used to normally supply voltage to the bus. The diesel generator output breaker must also be open before the diesel can be started. There is one other interlock to preclude the starting of the engine—an engine shutdown signal. This signal will be described. If all feeder and supply breakers to 4.16 kVac are open and an engine shutdown signal does not exist, an engine start signal is generated. This signal also latches in the automatic or manual start signals so that the engine start signal is a maintained signal, even if the initiating signals no longer exist. The operator must manually reset the start signal to return it to logic 0.

Finally, there is an interlock that prevents repetitious attempts to start the engine for the case in which the engine has not started. The start signal is allowed to exist for a predetermined period (for example, 5–8 seconds). If some predetermined engine operating conditions have not been met within this period, the start signal is blocked, and an engine failure signal is generated. If the diesel starts properly, the signal to the solenoid start valves is removed after the engine exceeds a specified setpoint.

An engine shutdown signal is generated if certain operating conditions associated with the engine are exceeded. These could include crankcase pressure, lube oil temperature, or jacket water temperature. If one or more of these conditions exceed defined setpoints, an engine trouble shutdown signal is generated. This signal is latched in such that the engine shutdown signal continues to exist, even if the off-normal operating condition(s) that resulted in the initial signal returns to logic 0. The operator is required to manually reset the engine trouble signal to return it to logic 0. The engine trouble signal is then logically ORed with a manual stop signal to generate the engine shutdown signal. The manual engine stop signal is interlocked with the engine start signal to preclude the operator from manually stopping the engine if an engine start signal exists.

### B.1.2 Regulatory Guidance on 100% Testing

Item 6 of DI&C-ISG-04, Section 2, Command Prioritization, states the following:

> *Software used in the design, testing, maintenance, etc. of a priority module is subject to all of the application guidance in Regulatory Guide 1.152, which endorses IEEE Standard 7-4.3.2-2003 (with comments). This included software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic devices (PLDs, programmable gate arrays, or other such devices. Section 5.3.2 of IEEE 7-4.3.2-2003 is particularly applicable to this subject. Validation of design tools used for programming of a priority module or a component of a priority module is not necessary if the device directly affected by these tools is 100% tested before being released for service. 100% testing means that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. The testing should not involve the use of the design tool itself. Software-based prioritization must meet all requirements (quality requirements, V&V, documentation, etc.) applicable to safety-related software.*

Item 8 of Section 2 further states:

> *Note that it is possible that logic devices within the priority module include unused inputs: assuming those inputs are forced by the module circuitry to a particular known state, those inputs can be excluded from "all possible combinations" criterion. For example, a priority module may include logic executed in a gate array that has more inputs than are necessary. The unused inputs should be forced to either "TRUE" or "FALSE" and then can be ignored in the :all possible combinations" testing.*

### B.1.3 A 100% Testing Strategy

As previously stated, the engine starting and shutdown logic essentially consists of two parts: the startup logic and the shutdown logic. As illustrated by Figure B-1, each part of the logic is a relatively simple logic that consists of fewer than 10 logic gates. However, the number of inputs can be greater than 10, depending on the plant's specific engine logic. To simplify the task of testing the engine logic 100%, the logic is tested by subdividing the logic into blocks. For example, the logic for the engine trouble shutdown signal is composed of a logical OR gate that could have many (more than five) inputs. The input signals are In1, In2, In3, and In4. The output is the output of the logical OR gate. All combinations of inputs to this logic OR will be tested, with the output of the logic OR verified for all combinations of input signals. In Figure B-1, this is identified as Block 1.

For example, assume that there are four inputs to the logic OR gate. Table B-1 shows the combinations of input signals that would be tested and the output signal verified.

*Table B-1*
*Block 1 testing combinations*

| Input Signals for Block 1 | | | | |
|---|---|---|---|---|
| **Input 1** | **Input 2** | **Input 3** | **Input 4** | **Logical OR Expected Output** |
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 |

After all combinations of inputs are tested for Block 1, the logic for the latch circuit is then tested (Block 2). Because the OR logic gate has been tested for all combinations, Block 2 testing is not required to test all combinations of inputs to Block 1. Concerning the four inputs (In1–In4), the testing assumes that all of the inputs are logic 0 and that one or more of the inputs are logic 1. Testing of Block 2 essentially reduces to testing two input signals and one output signal. The inputs are the Block 1 output and the reset shutdown logic control. The output signal is the engine trouble shutdown signal. However, the state of the feedback path will also be verified for each input combination.

Table B-2 shows the combinations of input signals that would be tested and the output signal verified. Because there is a latch in the logic, the conditions in Table B-2 are time-sequenced.

*Table B-2*
*Block 2 testing combinations*

| Input Signals for Block 2 | | Expected Feedback State | Engine Trouble Signal Expected Output |
|---|---|---|---|
| Reset Input | Block 1 Output | | |
| 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 0 |

The last step to testing the engine shutdown logic is to test the combined engine shutdown signal logic (Block 3). Block 3 essentially consists of three input signals and one output signal. The input signals are the engine trouble shutdown signal, the manual stop control signal, and the engine start signal. The output is the engine shutdown signal.

Table B-3 shows the combinations of inputs signals that are tested and the output state verified.

*Table B-3*
*Block 3 testing combinations*

| Input Signals for Block 3 | | | Engine Shutdown Signal Expected Output |
|---|---|---|---|
| Engine Trouble Shutdown Signal | Manual Stop Control Signal | Engine Start Signal | |
| 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 0 | 0 | 0 | 0 |

By conducting the three block tests shown in Tables B.1 through B.3, all combinations of the engine shutdown will have been tested. Intermediate software states have also been verified during the tests, such as the feedback signal in Block 2.

The next step is to test the engine start signal logic. The engine start logic is subdivided into five blocks. Block 4 tests the logical OR gate that has three inputs: primary 4.16-kVac crosstie breaker closed status, backup 4.16-kVac crosstie breaker closed status, and the diesel generator output breaker closed status. Block 4 has one output—a signal that indicates either that the crosstie breakers are not closed or the diesel generator output breaker is not closed.

Table B-4 shows the combinations of inputs signal that are tested and the output state verified.

*Table B-4*
*Block 4 testing combinations*

| Input Signals for Block 4 | | | |
|---|---|---|---|
| **Primary 4.16-kVac Crosstie Breaker Closed** | **Backup 4.16-kVac Crosstie Breaker Closed** | **Diesel Generator Output Breaker Closed** | **Expected Output** |
| 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 |
| 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 |

The next step is to test Block 5. Block 5 has two inputs: the reset start logic control signal and the engine shutdown signal (which was tested in Block 3). Block 5 has one output signal—a signal indicating that there are no conditions present to preclude starting the engine.

Table B-5 shows the combinations of inputs signals that are tested and the output state verified.

*Table B-5*
*Block 5 testing combinations*

| Input Signals for Block 5 | | Expected Output |
|---|---|---|
| **Engine Shutdown Signal** | **Reset Start Logic Control** | |
| 0 | 0 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 1 | 1 | 0 |

The next step is to test Block 6. The output of Block 6 is the engine start signal. There are five inputs to Block 6: an output signal of Block 5, output signal of Block 4, safety injection signal, undervoltage signal, and manual start control signal.

Table B-6 shows the combinations of input signals that are tested and the output state verified.

*Table B-6*
*Block 6 testing combinations*

| Input Signals for Block 6 | | | | | Engine Start Signal Expected Output |
|---|---|---|---|---|---|
| **Block 4 Output** | **Block 5 Output** | **Safety Injection Signal** | **Undervoltage Signal** | **Manual Start Control Signal** | |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 1 |
| 1 | 1 | 0 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 0 | 1 | 1 |
| 0 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |

The next step is to test Block 7. Block 7 performs the logic to generate a start failure signal. There are several process variable inputs to Block 7 that are indicative of an engine trouble that could generate a start failure signal. Typical signals that indicate engine starting problems include jacket water pressure, engine speed, and starting control module power. For this example, it is assumed that there are three process variable inputs to the logic. There are then five inputs to Block 7, as follows:

- Engine trouble shutdown signal (output of Block 2)
- Engine start signal (output of Block 6)
- In1
- In2
- In3

The output of Block 7 is the output of the logic and gate. This block of logic includes a time-delayed feedback path. Therefore, the sequence of the testing steps must be conducted as specified. The expected state of the feedback path is also specified in Table B-7 because the feedback is internal to the block. The purpose of the time-delayed feedback path is to automatically remove the engine start signal if the diesel has not attained certain running conditions within 7 seconds. This logic provides the operator the opportunity to manually start the diesel after the apparent problem has been rectified. Table B-7 shows the combinations of input signals that are tested and the output state verified.

*Table B-7*
*Block 7 test combinations*

| Input Signals for Block 7 | | | | | Expected Outputs | |
|---|---|---|---|---|---|---|
| **Engine Trouble Shutdown Signal** | **Engine Start Signal** | **In1** | **In2** | **In3** | **Expected Feedbac k State** | **Logical and Gate Expected Output** |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 1 | 0 | 1 | 0 |

*Table B-7 (Continued)*
*Block 7 test combinations*

| Input Signals for Block 7 | | | | | Expected Outputs | |
|---|---|---|---|---|---|---|
| **Engine Trouble Shutdown Signal** | **Engine Start Signal** | **In1** | **In2** | **In3** | **Expected Feedback State** | **Logical and Gate Expected Output** |
| 0 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 0 | 1 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 0 (within 7 sec) | 0 (within 7 sec) | 0 (within 7 sec) | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 0 (within 7 sec) | 1 (within 7 sec) | 1 (within 7 sec) | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 1 (within 7 sec) | 0 (within 7 sec) | 1 (within 7 sec) | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 1 (within 7 sec) | 1 (within 7 sec) | 0 (within 7 sec) | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 1 (within 7 sec) | 1 (within 7 sec) | 0 (within 7 sec) | 1 | 0 |

*Table B-7 (Continued)*
*Block 7 test combinations*

| Input Signals for Block 7 | | | | | Expected Outputs | |
|---|---|---|---|---|---|---|
| Engine Trouble Shutdown Signal | Engine Start Signal | In1 | In2 | In3 | Expected Feedback State | Logical and Gate Expected Output |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 1 (within 7 sec) | 0 (within 7 sec) | 1 (within 7 sec) | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 0 (within 7 sec) | 1 (within 7 sec) | 1 (within 7 sec) | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 (after 7 sec) | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 0 (after 2 sec) | 1 | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 1 | 0 (after 2 sec) | 1 | 1 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 (for 7 sec) | 1 |
| 1 | 1 | 1 | 1 | 0 (after 2 sec) | 1 | 0 |

The last step in the testing process is to test Block 8. The output of Block 8 is the open solenoid start valve signal. Block 8 has two inputs: the engine speed signal and Block 7 output signal.

Table B-8 shows the combinations of input signals that are tested and the output state verified.

*Table B-8*
*Block 8 testing combinations*

| Input Signals | | Open Solenoid Start Valve Signal |
|---|---|---|
| Engine Speed Signal | Block 7 Output Signal | |
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 0 |
| 1 | 1 | 0 |

## B.2 Summary

By dividing the engine shutdown and engine start logic into blocks, it is possible to test all combinations of inputs, all software states, and all outputs with approximately 120 test cases. The engine shutdown logic and engine start logic include feedback paths and a time delay, which necessitates additional test cases to cover all logic states. However, 120 test cases is not an unreasonable number of tests to perform to demonstrate 100% testability.

# Appendix C: Overview of the FPGA Technology

The guidance in this report builds on the information developed on FPGA applications in nuclear power plants documented in the EPRI report *Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems* [1]. This section will contain an overview of the FPGA technology and its advantages over microprocessor-based control systems in simple component-control types of applications.

# Appendix D: Model LAR

This section will provide a model LAR for utilities to adapt to their individual plant's licensing and design basis. It will be written in the style of the Consolidated Line Item Improvement Process model LARs used for the last several years by the Technical Specification Task Force (TSTF) for their generic LARs accompanying NRC-approved TSTF Travelers. The LAR will follow the guidance provided in the NRC/NRR Office Instruction LIC-101, "License Amendment Request Review Procedures," and in DI&C-ISG-06, "Licensing Process."

**Export Control Restrictions**

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful.  Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

**The Electric Power Research Institute Inc.,** (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

***Program:***

Instrumentation and Control

© 2013 Electric Power Research Institute (EPRI), Inc.  All rights reserved. Electric Power Research Institute, EPRI, and TOGETHER...SHAPING THE FUTURE OF ELECTRICITY are registered service marks of the Electric Power Research Institute, Inc.

3002002098

**Electric Power Research Institute**
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com