May 3, 2022
L-2022-073
10 CFR 50.90

U. S. Nuclear Regulatory Commission
Attn: Document Control Desk
Washington D C 20555-0001

RE: Turkey Point Units 3 and 4
Docket Nos. 50-250 and 50-251
Subsequent Renewed Facility Operating License DPR-31 and DPR-41

Turkey Point Units 3 & 4 Diversity and Defense-In-Depth Evaluation (D3), Framatome Document No. 51-9324096-004

Reference:

1. NRC Standard Review Plan Branch Technical Position 7-19, "Guidance for Evaluation of Defense-In-Depth and Diversity to Address Common Cause Failure Due to Latent Design Defects in Digital Safety Systems," Revision 8, dated January, 2021.

Florida Power and Light (FPL) hereby submits for NRC review, the enclosed Defense-in-Depth and Diversity (D3) Evaluation for Turkey Point Units 3 and 4 (Turkey Point). As discussed during an April 13, 2022 pre-application meeting (ADAMS Accession No. ML22102A198), the D3 evaluation is being submitted in advance of FPL's proposed Reactor Protection System (RPS), Engineered Safety Feature Actuation System (ESFAS) and Nuclear Instrumentation System (NIS) Digital Instrument and Control (I&C) Modernization license amendment request (LAR) for Turkey Point. FPL plans to submit the LAR in the second quarter of 2022.

In Reference 1, the NRC requires licensees to provide a D3 assessment of the proposed digital I&C system which demonstrates that any vulnerabilities to common-cause failures have been adequately addressed. In the enclosed D3 assessment, FPL has evaluated for defense-in-depth and diversity, the applicable design basis events identified in the Turkey Point Updated Final Safety Analysis Report (UFSAR).

Attachment 1 of this letter contains an affidavit from Framatome, Inc., (Framatome), the owner of the D3 Evaluation in Attachment 3, which supports a request for withholding from public disclosure pursuant to 10 CFR 2.390(a)(4). The affidavit sets forth the basis on which the information may be withheld from public disclosure by the Nuclear Regulatory Commission (Commission) and addresses with specificity the considerations listed in paragraph (b)(4) of Section 2.390 of the Commission's regulations. Accordingly, FPL requests that the information which is proprietary to Framatome be withheld from public disclosure pursuant to 10 CFR 2.390(a)(4). Correspondence with respect to the proprietary aspects of this information or the supporting Framatome affidavit should be addressed to Mr. Phillip Opsal, Manager, Product Licensing for Framatome, 3315 Old Forest Road, Lynchburg, Virginia 24501. Attachment 2 contains Framatome Document No. 51-9348245-000, which is the redacted (non-proprietary) version of the D3 Evaluation. Attachment 3 contains Framatome Document No. 51-9324096-004, which is the proprietary version of the D3 Evaluation. Attachment 3 may not be reproduced or copied in whole or in part, shall not be furnished to others without the express written consent of Framatome, and is not to be used in any way which is or may be detrimental to Framatome. Attachment 3 and any copies that may have been made must be returned to Framatome upon request. Attachments 1 and 2 are suitable for public dissemination.

This letter contains no regulatory commitments.

Should you have any questions regarding this submission, please contact Mr. Michael J. Davis, Fleet Licensing Manager, at 319-851-7032.

Timothy Lesniak
General Manager, Regulatory Affairs
Florida Power & Light

cc: USNRC Regional Administrator, Region II
USNRC Project Manager, Turkey Point Nuclear Plant
USNRC Senior Resident Inspector, Turkey Point Nuclear Plant
Ms. Cindy Becker, Florida Department of Health (Attachments 1 and 2 only)

Attachments

1. Affidavit for Attachment 3 to this letter: Florida Power and Light Turkey Point Unit 3 & 4 Diversity and Defense-In-Depth Evaluation (D3), Framatome Document No. 51-9324096-004

2. Florida Power and Light Turkey Point Unit 3 & 4 Diversity and Defense-In-Depth Evaluation (D3), Framatome Document No. 51-9348245-000 (Non-Proprietary Version)

3. Florida Power and Light Turkey Point Unit 3 & 4 Diversity and Defense-In-Depth Evaluation (D3), Framatome Document No. 51-9324096-004 (Proprietary Version)

ATTACHMENT 1:

Affidavit for Attachment 3: Florida Power and Light Turkey Point Unit 3 & 4 Diversity and Defense-In-Depth Evaluation (D3), Framatome Document No. 51-9324096-004

A F F I D A V I T

1. My name is Philip A. Opsal. I am Manager, Product Licensing for Framatome Inc. (formally known as AREVA Inc.), and as such I am authorized to execute this Affidavit.

2. I am familiar with the criteria applied by Framatome to determine whether certain Framatome information is proprietary. I am familiar with the policies established by Framatome to ensure the proper application of these criteria.

3. I am familiar with the Framatome information contained in Framatome Document No. 51-9324096-004, "Diversity and Defense-In-Depth Evaluation Florida Power & Light Co. Turkey Point Unit 3 & 4 Digital Modernization." Information contained in this Document has been classified by Framatome as proprietary in accordance with the policies established by Framatome for the control and protection of proprietary and confidential information.

4. This Document contains information of a proprietary and confidential nature and is of the type customarily held in confidence by Framatome and not made available to the public. Based on my experience, I am aware that other companies regard information of the kind contained in this Document as proprietary and confidential.

5. This Document has been made available to the U.S. Nuclear Regulatory Commission in confidence with the request that the information contained in this Document be withheld from public disclosure. The request for withholding of proprietary information is made in accordance with 10 CFR 2.390. The information for which withholding from disclosure is requested qualifies under 10 CFR 2.390(a)(4) "Trade secrets and commercial or financial information."

6. The following criteria are customarily applied by Framatome to determine whether information should be classified as proprietary:

(a) The information reveals details of Framatome's research and development plans and programs or their results.

(b) Use of the information by a competitor would permit the competitor to significantly reduce its expenditures, in time or resources, to design, produce, or market a similar product or service.

(c) The information includes test data or analytical techniques concerning a process, methodology, or component, the application of which results in a competitive advantage for Framatome.

(d) The information reveals certain distinguishing aspects of a process, methodology, or component, the exclusive use of which provides a competitive advantage for Framatome in product optimization or marketability.

(e) The information is vital to a competitive advantage held by Framatome, would be helpful to competitors to Framatome, and would likely cause substantial harm to the competitive position of Framatome.

The information in this Document is considered proprietary for the reasons set forth in paragraphs 6(b), 6(d), and 6(e) above.

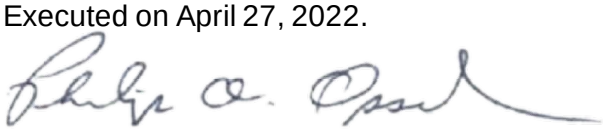
7. In accordance with Framatome's policies governing the protection and control of information, proprietary information contained in this Document has been made available, on a limited basis, to others outside Framatome only as required and under suitable agreement providing for nondisclosure and limited use of the information.

8. Framatome policy requires that proprietary information be kept in a secured file or area and distributed on a need-to-know basis.

9. The foregoing statements are true and correct to the best of my knowledge, information, and belief.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on April 27, 2022.



Philip A. Opsal

ATTACHMENT 2:

Florida Power and Light Turkey Point Unit 3 & 4 Diversity and Defense-In-Depth Evaluation (D3), Framatome Document No. 51-9348245-000 (Non-Proprietary Version)

framatome

Framatome Inc.

ENGINEERING INFORMATION RECORD

Document No.: 51 - 9348245 - 000

Diversity and Defense-in-Depth Evaluation
Florida Power & Light Co. Turkey Point Unit 3&4 Digital Modernization

Diversity and Defense-in-Depth Evaluation
Florida Power & Light Co. Turkey Point Unit 3&4 Digital Modernization

Safety Related? ☒ YES ☐ NO

Does this document establish design or technical requirements? ☒ YES ☐ NO

Does this document contain assumptions requiring verification? ☒ YES ☐ NO

Does this document contain Customer Required Format? ☐ YES ☒ NO

Signature Block

Name and Title/Discipline	Signature	P/LP, R/LR, M, A-CRF, A	Date	Pages/ s Prepared/Reviewed/ Approved or Comments
Jerry Mauck Licensing Engineer	*J MAUCK* *4/28/2022*	LP		All
Ted Quinn Licensing Engineer	*T QUINN* *4/28/2022*	P		All
Taha AbdelNaeem Project Lead/Technical Lead	*TI ABDELNAEEM* *4/28/2022*	LR		All
John DiBartolomeo Independent Design Review (Delegated to Ted Quinn per email)	*T QUINN* *4/28/2022*	R		All
Brian Haynes Licensing Manager	*BM HAYNES* *4/29/2022*	A		All
Georgia Dikeakos Engineering Manager	*G DIKEAKOS* *4/29/2022*	A		All

Note: P/LP designates Preparer (P), Lead Preparer (LP)
M designates Mentor (M)
R/LR designates Reviewer (R), Lead Reviewer (LR)
A-CRF designates Project Manager Approver of Customer Required Format (A-CRF)
A designates Approver/RTM – Verification of Reviewer Independence
N/A if not applicable

Project Manager Approval of Customer References (N/A if not applicable)

Name (printed or typed)	Title (printed or typed)	Signature	Date
Ron Jaworowski	Project Manager	*RO JAWOROWSKI* *4/29/2022*	

Record of Revision

Revision No.	Pages/Sections/ Paragraphs Changed	Brief Description / Change Authorization
000	Entire document	Non-Proprietary version of 51-9324096-004.

Table of Contents

Table of Contents
(continued)

Page

List of Tables

Page

List of Figures

Page

1 EXECUTIVE SUMMARY

The Turkey Point Nuclear Power Plant Unit 3&4 Reactor Protection System (RPS)/Engineered Safety Features Actuation System (ESFAS)/Nuclear Instrumentation System (NIS) upgrade project is currently being completed by Framatome and Florida Power and Light (FPL) under Contract [1]. The digital upgrade replicates the safety functions currently implemented on the analog equipment. The upgrade design and configuration are based on digital control products designed and manufactured by Framatome and its industry partners. However, the installation of digital-based RPS/ESFAS/NIS systems presents a concern that a postulated Software Common Cause Failure (SWCCF) of a common digital safety platform might propagate across multiple trains and channels such that it defeats the required safety functions. The Diversity and Defense-in-Depth (D3) assessment documented herein demonstrates that there will be sufficient defense-in-depth and diversity to cope with a postulated SWCCF to the Triconex PLC (Tricon) digital platform in the RPS/ESFAS/NIS systems. [

]

[ ]

In summary, this Turkey Point Unit 3&4 D3 assessment has followed the applicable guidance provided in BTP 7-19, Rev 8 [3]. Solutions for all transients and accidents when postulating a SWCCF to the RPS/ESFAS Tricon digital platform has been provided as discussed in Sections 4 and 5 of this report. The conclusion section (6) of this report reiterates these findings and provides more details regarding diversity and defense-in-depth.

2 TURKEY POINT UNIT 3&4 DIGITAL UPGRADE PROJECT

2.1 Scope

With the advent of digital technology being implemented as part of safety systems (e.g., the Reactor Protection System and Engineered Safeguard Features Actuation System) in both operating and plants under construction, a concern has been identified that a postulated SWCCF of these software-based safety platforms could propagate across multiple trains and channels in a manner that would defeat the required safety functions. The NRC regulatory guidance for this concern is detailed in BTP 7-19 [3]. FPL is implementing digital technology in the Turkey Point Unit 3&4 RPS and ESFAS. Therefore, Framatome conducted a D3 evaluation and provides documented results herein demonstrating that there will be sufficient defense-in-depth and diversity to cope with a postulated SWCCF to the RPS/ESFAS software based digital platforms.

The guidance within BTP 7-19 [3] is discussed below and demonstrates that, for the replacement digital system, the acceptance criteria of BTP 7-19 [3] are met. [

]

The BTP 7-19 [3] guidance and the assessment process are discussed in the following sections of this report.

[

]

[

]

The Diversity and Defense-in-Depth Evaluation is a SAFETY-RELATED document under the Framatome and Turkey Point Unit 3&4 Quality Programs.

2.2 Objectives

The objective of the D3 assessment is to eliminate potential vulnerabilities of the RPS/ESFAS upgrade to a postulated RPS/ESFAS SWCCF within these systems by [

]

[

]

2.3 Regulatory Position

The Turkey Point Unit 3&4 RPS/ESFAS upgrade project is being designed and implemented to meet current regulatory requirements and guidance. [

]

Based on experience in previous detailed reviews, the NRC staff has established acceptance guidelines for D3 assessments as described in BTP 7-19 [3]. Further guidance was established through the efforts of the Digital Instrumentation and Control (DI&C) Task Working Group No. 2 on D3 with the development of DI&C-ISG-02 [7], "Task Working Group No. 2: Diversity and Defense-in-Depth Issues Interim Staff Guidance," Revision 2. This interim staff guidance (ISG) was developed with extensive review of D3 issues including both internal review within the NRC and external input through public meetings with representatives from industry, vendors, and the public. In addition, NUREG/CR-6303 [6] was published to provide guidance on certain D3 concerns such as diversity. In summary, while the NRC considers a software common cause failure (SWCCF) in digital systems to be beyond design basis, nuclear Power Plants (NPPs) must be protected against the effects of PIEs with a concurrent SWCCF in the digital protection system.

The following Points 1, 2, 3, and 4 of the NRC position in SRM-SECY-93-087 [8] apply to digital system modifications within operating and new plants, and were used by NRC to develop the D3 assessment guidelines in BTP 7-19 [3]:

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

The NRC identified four echelons of defense in NUREG/CR-6303 [6]:

Echelon 1 • Control System – The control system echelon usually consists of equipment that is not safety-related, that is used in the normal operation of an NPP, and routinely prevents operations in unsafe regimes of NPP operations.

Echelon 2 • Reactor Trip System – The Reactor Trip System (RTS) echelon consists of safety-related equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

Echelon 3 • Engineered Safety Features Actuation System (ESFAS) – The ESFAS echelon consists of safety-related equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel and reactor coolant system pressure boundary, and primary containment) and the logic components used to actuate this safety-related equipment, usually referred to as the ESF Actuation System (ESFAS), and controls.

Echelon 4 • Monitoring and Indicator System – The monitoring and indicator system echelon consists of sensors, safety parameter displays, data communication systems, and independent manual controls relied upon by operators to respond to NPP operating events.

SRP Chapter 18, Appendix A, Section 1A [10] states in part:

> *"…The basis for the specific time margin used in the analysis should be justified and documented. Insights from the HFE program, especially the OER and Human Reliability Analysis, should be used. The identification of potential errors, error detection methods, and error recovery paths in event trees may be used to provide estimates of how much margin should be added to the operator response time estimates. For complex situations and for actions with limited margin, such as less than 30 minutes between time available and time required, a more focused staff review will be performed."*

4.3 Spurious RPS/ESFAS Actuations

NUREG-800, Chapter 7, BTP 7-19, [3] states the following concerning postulated spurious actuations caused by a SWCCF:

> *"The evaluation of potential spurious operations is an important part of the overall D3 assessment for a proposed DI&C system to ensure that spurious operations do not lead to events with unacceptable consequences. Although a spurious operation is not always anticipated, it can be detected because this type of failure is normally self-announcing through instrumentation on the actuated system. However, in some circumstances a spurious operation may not occur until a particular signal or set of signals is present. In these cases, rather than occurring immediately upon system startup, the spurious operation would occur only under certain plant conditions. Such a spurious operation is still self-announcing (by the actuated system), even if failure did not occur on initial test…"*

[

]

7 ABBREVIATIONS AND ACRONYMS

Acronyms/Abbreviations	Description
2-o-o-4	Two out of four
2-o-o-3	Two out of three
A/D	Analog to Digital
ADV	Atmospheric Dump Valves
AECL	Atomic Energy of Canada Limited
AFW	Auxiliary Feedwater
AMSAC	ATWS Mitigating System Actuation Circuitry
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
ASD	Atmospheric Steam Discharge
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
B&PV	Boiler and Pressure Vessel
BE	Best Estimate
BIT	Boron Injection Tank
BOL	Beginning of Life
BTP	Branch Technical Position
CCF	Common Cause Failure
CCW	Component Cooling Water
CFCU	Containment Fan Coil Unit
CFR	Code of Federal Regulations
CLOF	Complete Loss of Flow
CR	Control Room
CS	Containment Spray
CVCS	Chemical and Volume Control System
D/A	Digital to Analog
D3	Defense-In-Depth and Diversity Evaluation
[ ]	[ ]
DBA	Design Basis Accident
[ ]	[ ]
DI&C	Digital Instrumentation and Control
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
EAB	Exclusion Area Boundary

Acronyms/Abbreviations	Description
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EMC	Electromagnetic Compatibility
EMI/RFI	Electromagnetic Interference/Radio Frequency Interference
EOL	End of Life
EOP	Emergency Operations Procedure
EPRI	Electric Power Research Institute
EPU	Extended Power Uprate
ESFAS	Engineered Safety Features Actuation System
ETA	External Termination Assembly
FCG	Fatigue Crack Growth
FPL	Florida Power and Light
Framatome	Framatome USA
FT	Foot
FWLB	Feedwater Line Break
GDC	Generic Design Criteria
GL	Generic Letter
GPM (gpm)	Gallons Per Minute
HFE	Human Factors Engineering
HFP	Hot Full Power
HHSI	High Head Safety Injection
HVAC	Heating, Ventilation and Air Conditioning
I&C	Instrumentation and Control
I/A	Intelligent Automation - Foxboro-Schneider
ICW	Intake Cooling Water
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISG	Interim Staff Guidance
LBB	Leak-Before-Break
LBLOCA	Large Break LOCA
LCO	Limiting Condition of Operation
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOL	Loss of Load
LONF	Loss of Normal Feedwater
LOOP	Loss of Offsite Power
LPZ	Low Population Zone

Acronyms/Abbreviations	Description
MCB	Main Control Board
MCC	Motor Control Center
MCR	Main Control Room
mDNBR	Minimum Departure from Nuclear Boiling Ratio
MFW	Main Feedwater
MG	Motor Generator
MOV	Motor Operated Valve
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MSSV	Main Steam Safety Valve
MSS	Main Steam System
MTC	Moderator Temperature Coefficient
MTTF	Mean-Time-To-Failure
NGAID	Next Generation Differential Analog Input
NGDO	Next Generation Digital Output
NIS	Nuclear Instrumentation System
NPP	Nuclear Power Plant
NR	Narrow Range
NRC	United States Nuclear Regulatory Commission
NSR	Non-Safety Related
OTΔT	Overtemperature Delta-T
PA	Postulated Accident
PCT	Peak Clad Temperature
PFD	Probability of Failure on Demand
PIE	Postulated Initiating Event
PLC	Programmable Logic Controller
PLOF	Partial Loss of Flow
PMP	Project Management Plan
PORV	Pilot Operated Relief Valve (definition); or Power Operated Relief Valve
PQP	Project Quality Plan
PRA	Probabilistic Risk Analysis
PRMS	Process Radiation Monitoring System
PRZ	Pressurizer
PSIG	Pounds Per Square Inch Gage
PSV	Pressurizer Safety Valve
Turkey Point Unit 3&4	Plant Turkey Point Nuclear Plant Unit 3&4
QA	Quality Assurance

Acronyms/Abbreviations	Description
QSPDS	Qualified Safety Parameter Display System
RCCA	Rod Cluster Control Assembly
RCP	Reactor Coolant Pump
RCS	Reactor Coolant System
RG	Regulatory Guide
RHR	Residual Heat Removal
RPS	Reactor Protection System
RTB	Reactor Trip Breaker
RTP	Rated Thermal Power
RTS	Reactor Trip System
RWAP	Rod Withdrawal at Power
RWSC	Rod Withdrawal Sub Critical
RWST	Refueling Water Storage Tank
SAR	Safety Analysis Report
SBLOCA	Small Break LOCA
SCMP	Software Configuration Management Plan
SDP	Software Development Plan
SER	Safety Evaluation Report
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SGTR	Steam Generator
SI	Safety Injection
SIA	Structural Integrity Associates
SMT	Surface Mount Technology
SQAP	Software Quality Assurance Plan
SR	Surveillance Requirement
SRP	Standard Review Plan
Std	Standard
SVDU	Flat Panel Display – Safety Video Display Unit
SVVP	Software Verification and Validation Plan
SWCCF	Software Common Cause Failure
SWGR	Switchgear
Tavg	Temperature-Average
TCM	Tricon Communication Module
TI	Test Interval
TLAA	Time-Limited Aging Analysis
TMR	Triple Modular Redundant

Acronyms/Abbreviations	Description
TR	Topical Report (non-EPRI references); or Technical Report
Tricon	Triconex PLC
TS	Technical Specifications
TSAP	Test Specimen Application Program
UF	Under Frequency
UFSAR	Updated Final Safety Analysis Report
UV	Under Voltage
V&V	Verification and Validation
VAC	Volt AC
VCT	Volume Control Tank
WR	Wide Range

8 GLOSSARY OF TERMS

The following definitions are provided for special terms used in this document.

Term	Definition
Anticipated operational occurrence (AOO) (10 CFR Part 50 Appendix A)	Those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of the turbine generator set, isolation of the main condenser, and loss of offsite power.
Common-mode failure (CMF) (NUREG/CR-6303)	Causally related failures of redundant or separate equipment. CMF embraces all causal relations, including severe environments, design errors, calibration and maintenance errors, and consequential failures.
Design basis accident (DBA) (NUREG/CR 6303)	Occurrences that are not expected to occur but are postulated because their consequences would include the potential for the release of significant amounts of radioactive material.
Diverse component or system (IEC 880)	A component or system that duplicates the function of another component or system by employing different physical construction or different principles of operation.
Diversity & Defense-in-Depth (D3)	A concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment.
Echelons of defense (NUREG/CR 6303)	Specific applications of the principle of defense-in-depth to the arrangement of instrumentation and control systems attached to a nuclear reactor for the purpose of operating the reactor or shutting it down and cooling it.
Redundant component or system (IEEE 379)	A piece of equipment or system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function, regardless of the state of operation or failure of the other.

Term	Definition
Single Failure Criterion (IEEE 379)	The safety systems shall perform all required safety functions for a design basis event in the presence of the following: • Any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures. • All failures caused by the single failure. • All failures and spurious actions that cause, or are caused by, the design basis event requiring the safety function. • The single failure could occur prior to, or at any time during, the design basis event for which the safety function is required to function.

9 REFERENCES