Duke Energy®

DAVE BAXTER
Vice President
Oconee Nuclear Station

Duke Energy Corporation
ONO1VP/7800 Rochester Highway
Seneca, SC 29672

864-885-4460
864-885-4208 fax
dabaxter@dukeenergy.com

January 31, 2008

U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Attention: Document Control Desk

Subject: Duke Power Company LLC d/b/a Duke Energy Carolinas, LLC
Oconee Nuclear Station, Units 1, 2, and 3
Docket Numbers 50-269, 50-270, and 50-287
License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change Number 2007-09

Pursuant to Title 10, Code of Federal Regulations, Part 50, Section 90 (10 CFR 50.90), Duke Power Company LLC d/b/a Duke Energy Carolinas, LLC (Duke) proposes to amend Appendix A, Technical Specifications, for Facility Operating Licenses DPR-38, DPR-47 and DPR-55 for Oconee Nuclear Station (ONS), Units 1, 2, and 3. Duke plans to replace the current analog based Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) with a digital computer based RPS/ESPS. This design change requires a Technical Specification (TS) change. As such, Duke requests the Nuclear Regulatory Commission (NRC) to review and approve the design change and the associated TS change.

Duke met with the NRC on May 25 and December 14, 2006, February 27 and April 30, 2007, by teleconference on July 10, 2007, and December 12, 2007, to discuss and agree on the format and content of the RPS/ESPS License Amendment Request (LAR) and the associated design-related documents that needed to be available at time of submittal and prior to issuance of the safety evaluation report (SER) for this LAR. The format and content of this LAR is consistent with what was agreed upon during these meetings. The NRC documented by Memorandum dated August 1, 2007, that Nuclear Energy Institute (NEI) 06-02 provides adequate guidance for the basic format and content of the LAR and that Regulatory Guide (RG) 1.206 provides adequate guidance for the technical portion of

Enclosures 1, 2 (not including Attachments 1 and 2), and 6 to this letter contain proprietary information.
Withhold From Public Disclosure Under 10 CFR 2.390.
Upon removal of the enclosures, this letter is uncontrolled.

A001
NRR

the LAR. Duke and the NRC also agreed that software quality assurance was more appropriately addressed by Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14.

The format and content of the information provided in this LAR is consistent with basic format and content guidelines of NEI 06-02. Enclosure 1 provides an evaluation of the RPS/ESPS design change. The technical evaluation contained in Enclosure 1 is consistent with the guidelines of Regulatory Guide 1.206 Chapter C.I.7, applicable portions of SRP Chapter 7, and SRP BTP 7-14.

The TELEPERM XS (TXS) system, as described in Siemens (FANP) Topical Report EMF-2110 (NP), Revision 1, "TXS: A Digital Reactor Protection System," dated September 1999, will replace the existing ONS RPS and ESPS, as described in ONS Updated Final Safety Analysis Report (UFSAR) Chapter 7. The signal processing, the signal validation, and the protection logic for these systems will now be performed by the TXS system.

The TXS SER dated May 5, 2000, indicates that the TXS System as described in Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," is acceptable for referencing in license applications to the extent specified in the topical report and NRC SER.

The proposed TS change revises TS 1.1, 3.3.1, 3.3.3, 3.3.4, 3.3.5, 3.3.7, and associated TS Bases Sections 3.3.1, 3.3.3, 3.3.4, 3.3.5, 3.3.6 and 3.3.7. This TS change is needed to support implementation of the digital upgrade and to take advantage of design features that support extending the Required Action Completion Times for placing a channel in trip, automating channel checks and extending surveillance intervals for channel functional tests. Enclosure 2 provides a description of the proposed TSs, justification for those changes, TS and Bases markups denoting the changes, and TS and Bases retyped pages.

Regulatory evaluation (including the significant hazards consideration), environmental considerations, and references are provided in Chapters 4, 5, and 6, respectively, of Enclosure 1. Enclosure 3 provides a list of regulatory commitments being made as a result of this LAR.

On January 17, 2008, during a conference call, Duke and NRC agreed on documents that need to be docketed to allow NRC to complete their acceptance review of this LAR. These documents are provided in Enclosure 6. The table at the beginning of Enclosure 6 lists these documents. Information contained in AREVA NP documents has been classified by AREVA NP as proprietary. An affidavit from AREVA NP for those documents considered proprietary is included as Enclosure 5. This affidavit sets forth the basis on which the information may be withheld from public disclosure by the NRC pursuant to 10 CFR 2.390. Duke considers the information provided in the Duke documents included in Enclosure 6 as sensitive information and requests these documents be withheld from public disclosure by the NRC pursuant to 10 CFR 2.390.

The ONS UFSAR has been reviewed. Various sections will require revision due to the RPS/ESPS design change. These revisions will be submitted per 10 CFR 50.71(e).

In accordance with Duke administrative procedures and the Duke Quality Assurance Program Topical Report, these proposed changes have been reviewed and approved by the Plant Operations Review Committee and Nuclear Safety Review Board. Additionally, a copy of this LAR is being sent to the State of South Carolina in accordance with 10 CFR 50.91 requirements.

Duke plans to implement the RPS/ESPS digital upgrade in the fall 2009 refueling outage for ONS Unit 1 with the other two Units to follow in the fall 2010 and 2011 outages. Therefore, Duke requests NRC to review and approve the design change and the associated TS change by January 31, 2009. Duke requests the amendment be made effective prior to startup from the Unit 1 fall 2009 refueling outage.

Enclosures 1 and 2 contain information proprietary to AREVA NP and have been marked as proprietary. An affidavit from AREVA NP is included as Enclosure 4. This affidavit sets forth the basis on which the information may be withheld from public disclosure by the NRC pursuant to 10 CFR 2.390. Attachments 1 and 2 of Enclosure 2 are Non proprietary. Non proprietary versions of Enclosures 1 and 2 have been provided in Enclosure 7 and 8, respectively.

If there are any questions regarding this submittal, please contact Boyd Shingleton at (864) 885-4716.

Very truly yours,

D. A. Baxter, Vice President
Oconee Nuclear Station

Enclosures:

1. Evaluation of Proposed Change - Proprietary
2. Evaluation of Proposed Technical Specification Change - Proprietary
   Attachments:
   1. Technical Specifications – Mark Ups
   2. Technical Specifications - Reprinted Pages
3. List of Regulatory Commitments
4. AREVA NP Affidavit for Enclosures 1 and 2
5. AREVA NP Affidavit for Enclosure 6
6. Documents Needed for Acceptance Review of LAR
7. Evaluation of Proposed Change – Non Proprietary
8. Evaluation of Proposed Technical Specification Change – Non Proprietary

cc: Mr. L. N. Olshan, Project Manager
Office of Nuclear Reactor Regulation
U. S. Nuclear Regulatory Commission
Mail Stop O-14 H25
Washington, D. C. 20555

V. M. McCree, Regional Administrator
U. S. Nuclear Regulatory Commission - Region II
Atlanta Federal Center
61 Forsyth St., SW, Suite 23T85
Atlanta, Georgia 30303

Mr. D. W. Rich
Senior Resident Inspector
Oconee Nuclear Station

S. E. Jenkins, Manager
Division of Radioactive Waste Management
Bureau of Land and Waste Management
Department of Health and Environmental Control
2600 Bull Street
Columbia, SC 29201

D. A. Baxter, affirms that he is the person who subscribed his name to the foregoing statement, and that all the matters and facts set forth herein are true and correct to the best of his knowledge.

D. A. Baxter, Vice President
Oconee Nuclear Site

Subscribed and sworn to me: 1-31-2008
Date

Ruth B Joyner
Notary Public

My Commission Expires: 6/15/2016
Date

SEAL

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 3

List of Regulatory Commitments

The following commitment table identifies those actions committed to by Duke Power Company LLC d/b/a Duke Energy Carolinas, LLC (Duke) in this submittal. Other actions discussed in the submittal represent intended or planned actions by Duke. They are described to the Nuclear Regulatory Commission (NRC) for the NRC's information and are not regulatory commitments.

Commitment	Completion Date
Duke will make documents listed in Table 1-2 of Enclosure 1 available for NRC review.	As stated in Table 1-2
Duke will install a diverse Low Pressure Injection actuation system (DLPIAS).	Concurrent with the RPS/ESPS digital upgrade
Duke will install a diverse High Pressure Injection actuation system (DHPIAS).	Concurrent with the RPS/ESPS digital upgrade
Duke will address functionality requirements for the DLPIAS and DHPIAS in the Oconee Selected Licensee Commitment (SLC) Manual.	Prior to startup after completing the first installation of the RPS/ESPS at ONS

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 4

AREVA NP Affidavit
for Enclosures 1 and 2

AFFIDAVIT

STATE OF VIRGINIA)
) ss.
CITY OF LYNCHBURG)

1. My name is Mark J. Burzynski. I am Manager, Product Licensing, for AREVA NP Inc. and as such I am authorized to execute this Affidavit.

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

3. I am familiar with the AREVA NP information provided to the NRC in Duke Power Company LLC License Amendment Request for Oconee Nuclear Station, Units 1, 2, and 3 (Docket Numbers 50-269, 50-270, and 50-287) entitled, *Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change Number 2007-09*, and referred to herein as the "Document." Information contained in this Document has been classified by AREVA NP as proprietary in accordance with the policies established by AREVA NP 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 AREVA NP 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 AREVA NP to determine whether information should be classified as proprietary:

(a) The information reveals details of AREVA NP'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 AREVA NP.

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

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

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

7. In accordance with AREVA NP'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 AREVA NP only as required and under suitable agreement providing for nondisclosure and limited use of the information.

8. AREVA NP 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.

Mark J Burzynski

SUBSCRIBED before me on this 22nd

day of January, 2008.

NOTARY PUBLIC, STATE OF GEORGIA

KENDRICK SMART
NOTARY PUBLIC, CHEROKEE COUNTY, GA
MY COMMISSION EXPIRES DEC. 15, 2009

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 5

AREVA NP Affidavit
for Enclosure 6

AFFIDAVIT

STATE OF VIRGINIA)
) ss.
CITY OF LYNCHBURG)

1. My name is Mark J. Burzynski. I am Manager, Product Licensing, for AREVA NP Inc. and as such I am authorized to execute this Affidavit.

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

3. I am familiar with the AREVA NP information provided to the NRC in support of a Duke Power Company LLC License Amendment Request for Oconee Nuclear Station, Units 1, 2, and 3 (Docket Numbers 50-269, 50-270, and 50-287) entitled Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change Number 2007-09. The following seven AREVA NP documents are provided and referred to herein as the "Documents."

- AREVA NP Document 51-5055058-06, *Dedication Plan for Absopulse AC/DC Power Supply SYS/ARV-4-Q9418*
- AREVA NP Document 51-9062468-001, *Generic Dedication Task Letter for Absopulse AC/DC Power Supply SYS/PFC-4-Q9418*
- AREVA NP Document 51-9062071-001, *Generic Task Letter for Additional Absopulse Power Supply Module Testing at Absopulse*

- AREVA NP Document 51-5045374-06, *Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade System Architecture*
- AREVA NP Document 51-9029108-003, *Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade TXS System Description for LAR Input*
- AREVA NP Document 51-9054435-002, *Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Requirements Specification*
- AREVA NP Document 51-9010419-005, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Software Verification and Validation Plan*

Information contained in these Documents has been classified by AREVA NP as proprietary in accordance with the policies established by AREVA NP for the control and protection of proprietary and confidential information.

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

5. These Documents have been made available to the U S. Nuclear Regulatory Commission in confidence with the request that the information contained in these Documents 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 AREVA NP to determine whether information should be classified as proprietary:

(a) The information reveals details of AREVA NP'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 AREVA NP.

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

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

The information in these Documents is considered proprietary for the reasons set forth in paragraphs 6(b), 6(c) and 6(d) above.

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

8. AREVA NP 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.

Mark J Burzynski

SUBSCRIBED before me on this 22nd

day of January, 2008.

NOTARY PUBLIC, STATE OF GEORGIA

KENDRICK SMART
NOTARY PUBLIC, CHEROKEE COUNTY, GA
MY COMMISSION EXPIRES DEC. 15, 2009

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 6

Documents Needed for Acceptance Review of LAR

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 4

AREVA NP Affidavit
for Enclosures 1 and 2

AFFIDAVIT

STATE OF VIRGINIA)
) ss.
CITY OF LYNCHBURG)

1. My name is Mark J. Burzynski. I am Manager, Product Licensing, for AREVA NP Inc. and as such I am authorized to execute this Affidavit.

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

3. I am familiar with the AREVA NP information provided to the NRC in Duke Power Company LLC License Amendment Request for Oconee Nuclear Station, Units 1, 2, and 3 (Docket Numbers 50-269, 50-270, and 50-287) entitled, *Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change Number 2007-09*, and referred to herein as the "Document." Information contained in this Document has been classified by AREVA NP as proprietary in accordance with the policies established by AREVA NP 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 AREVA NP 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 AREVA NP to determine whether information should be classified as proprietary:

(a) The information reveals details of AREVA NP'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 AREVA NP.

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

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

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

7. In accordance with AREVA NP'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 AREVA NP only as required and under suitable agreement providing for nondisclosure and limited use of the information.

8. AREVA NP 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.

Mark J Burzynski

SUBSCRIBED before me on this 22nd

day of January, 2008.

NOTARY PUBLIC, STATE OF GEORGIA

KENDRICK SMART
NOTARY PUBLIC, CHEROKEE COUNTY, GA
MY COMMISSION EXPIRES DEC. 15, 2009

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 5

AREVA NP Affidavit
for Enclosure 6

AFFIDAVIT

STATE OF VIRGINIA)
) ss.
CITY OF LYNCHBURG)

1. My name is Mark J. Burzynski. I am Manager, Product Licensing, for AREVA NP Inc. and as such I am authorized to execute this Affidavit.

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

3. I am familiar with the AREVA NP information provided to the NRC in support of a Duke Power Company LLC License Amendment Request for Oconee Nuclear Station, Units 1, 2, and 3 (Docket Numbers 50-269, 50-270, and 50-287) entitled Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change Number 2007-09. The following seven AREVA NP documents are provided and referred to herein as the "Documents."

- AREVA NP Document 51-5055058-06, *Dedication Plan for Absopulse AC/DC Power Supply SYS/ARV-4-Q9418*
- AREVA NP Document 51-9062468-001, *Generic Dedication Task Letter for Absopulse AC/DC Power Supply SYS/PFC-4-Q9418*
- AREVA NP Document 51-9062071-001, *Generic Task Letter for Additional Absopulse Power Supply Module Testing at Absopulse*

- AREVA NP Document 51-5045374-06, *Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade System Architecture*
- AREVA NP Document 51-9029108-003, *Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade TXS System Description for LAR Input*
- AREVA NP Document 51-9054435-002, *Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Requirements Specification*
- AREVA NP Document 51-9010419-005, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Software Verification and Validation Plan*

Information contained in these Documents has been classified by AREVA NP as proprietary in accordance with the policies established by AREVA NP for the control and protection of proprietary and confidential information.

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

5. These Documents have been made available to the U S. Nuclear Regulatory Commission in confidence with the request that the information contained in these Documents 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 AREVA NP to determine whether information should be classified as proprietary:

(a) The information reveals details of AREVA NP'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 AREVA NP.

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

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

The information in these Documents is considered proprietary for the reasons set forth in paragraphs 6(b), 6(c) and 6(d) above.

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

8. AREVA NP 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.

Mark J Burzynski

SUBSCRIBED before me on this 22nd

day of January, 2008.

NOTARY PUBLIC, STATE OF GEORGIA

KENDRICK SMART
NOTARY PUBLIC, CHEROKEE COUNTY, GA
MY COMMISSION EXPIRES DEC. 15, 2009

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 7

Evaluation of Proposed Change

Non Proprietary

IEEE excerpts contained in Section 3.3 of this license amendment request are reprinted with permission from IEEE Std 603-1998 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Copyright 1998, by IEEE.

IEEE excerpts contained in Section 3.4 of this license amendment request are reprinted with permission from IEEE Std 7-4.3.2-2003 IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, Copyright 2003, by IEEE.

Table of Contents

List of Tables

List of Figures

ACRONYMS AND ABBREVIATIONS

2.MAX	2nd maximum
2.MIN	2nd minimum
A/D	Analog/Digital
A/E	Architect/Engineer
AC	Alternating Current
AMSAC	ATWS Mitigating System Actuation Circuitry
ASM	Alphanumeric Service Monitor
ATWS	Anticipated Transient without Scram
BTP	Branch Technical Position
CM	Configuration Management
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRD	Control Rod Drive
CRE	Control Rod Ejection
CROs	Control Room Operators
CTs	Completion Times
D3	Defense in Depth and Diversity
DBE	Design Basis Event
DC	Direct current
DCP	Design Change Package
DCRDCS	Digital Control Rod Drive Control System
DCRM	Document Control Records Management
DCS	Data Communication System
DHPIAS	Diverse High Pressure Injection Actuation System
DLPIAS	Diverse Low Pressure Injection Actuation System
DPRAM	Dual Port Random Access Memory
DSS	Diverse Scram System
Duke	Duke Power Company LLC d/b/a Duke Energy Carolinas, LLC
EDS	Electrical Distribution System
EEPROM	Electrically erasable programmable read-only memory
EFW	Emergency Feedwater
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EOP	Emergency Operating Procedures
ES	Engineered Safeguards
ESF	Engineered Safety Features
ESFAS	Engineered Safety Features Actuation System
ESPS	Engineered Safeguards Protective System
ESTC	Engineered Safeguards Terminal Cabinet
F	Fahrenheit
FAT	Factory Acceptance Testing
FEPROM	Flash erasable programmable read-only memory

FMEA	Failure Modes and Effects Analysis
GDC	General Design Criteria
GSM	Graphical Service Monitor
HFE	Human Factors Engineering
HPI	High Pressure Injection
Hz	Hertz
I&C	Instrumentation And Control
I/O	Input/Output
ICS	Integrated Control System
ID	Identification
IDR	Integrated Design Review
IPs	Instrument Procedures
KHUs	Keowee Hydro Units
KOIC	Keowee Oconee Interface Cabinet
KTA	German Safety Standards
LAR	License Amendment Request
LCO	Limiting Condition For Operation
LEDs	Light Emitting Diodes
LOCA	Loss Of Coolant Accident
LOSCM	Loss Of Subcooling Margin
LPI	Low Pressure Injection
LPSW	Low Pressure Service Water
LQST	Licensing and Quality Steering Team
M&TE	Measuring And Test Equipment
MAC	Media Access Control
MCC	Motor Control Center
MDs	Maintenance Directives
MSI	Monitoring and Service Interface
MTP	Modification Test Plan
NEI	Nuclear Energy Institute
NGD	Nuclear Generation Department
NI	Nuclear Instrumentation
NRC	Nuclear Regulatory Commission
NSDs	Nuclear System Directives (Duke)
NUPIC	Nuclear Procurement Issues Committee
OAC	Operator Aid Computer
OCG	Owner Control Group
OER	Operating Experience Review
OI	Operating Instruction
ONS	Oconee Nuclear Station
OPS	Operations
PDC	Plant Design Criteria
PIP	Problem Investigation Process
PLCs	Programmable Logic Controllers

PT	Periodic Test
QA	Quality Assurance
QAP	Quality Assurance Program
QC	Quality Control
QMM	Quality Management Manual
QMP	Quality Management Plan
RA	Required Action
RAM	Random Access Memory
RB	Reactor Building
RBC	Reactor Building Cooling
RBCU	Reactor Building Cooling Unit
RBS	Reactor Building Spray
RCPPM	Reactor Coolant Pump Power Monitor
RCS	Reactor Coolant System
RFI	Radio-Frequency Interference
RG	Regulatory Guide
RH	Relative Humidity
RO	Relay Output
RPS	Reactor Protective System
RTE	Run Time Environment
S/D	Shutdown
SAT	Site Acceptance Testing
SBLOCA	Small Break Loss of Coolant Accident
SDCR	Software Data Change Request
SDD	Software Design Description
SDQA	Software and Data Quality Assurance
SER	Safety Evaluation Report
SI	Surveillance Interval
SIVAT	Simulation and Validation Tool
SMS	Service Monitor Server
SPACE	Specification and Coding Environment
Square D	Schneider Electric
SRP	Standard Review Plan
SRS	Software Requirements Specification
SSC	Structures, Systems and Components
Std	Standard
SWCMF	Software Common Mode Failure
THD	Total Harmonic Distortion
TLU	Total Loop Uncertainty
TS	Technical Specification
TXS	Teleperm Xs
UFSAR	Updated Final Safety Analysis Report
UV	Undervoltage
V	Volts

V&V	Verification And Validation
VAC	Volts Alternating Current
VDC	Volts Direct Current
WPM	Work Process Manual
WR	Wide Range

1. Summary Description

Duke Power Company LLC d/b/a Duke Energy Carolinas, LLC (Duke) is in the process of implementing a design change to replace the existing analog based Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) at the Oconee Nuclear Station (ONS) with a TELEPERM XS (TXS) digital protection system. The upgraded ONS systems will be referred to as the digital RPS/ESPS throughout this License Amendment Request (LAR).

The NRC issued a Safety Evaluation Report (SER) on May 5, 2000 (Reference 1) for the TXS system that is being credited by Duke for the ONS RPS/ESPS digital upgrade. The NRC affirms in the cover letter, that Topical Report EMF-2110(NP), Revision 1 (Reference 2), "TELEPERM XS: A Digital Reactor Protection System" is acceptable for referencing in license applications to the extent specified in the topical report and NRC SER. The SER states that the TXS system is acceptable for use in the development, installation, and operation of safety-related systems in nuclear power plants, subject to plant specific action items that must be performed by an applicant when requesting NRC approval for installation of a TXS system. The plant specific actions are addressed in Chapters 2 and 3 of this Enclosure as indicated in Table 1-1.

The TXS platform, which will replace equipment originally manufactured by Bailey Meter Company, will provide the signal processing, signal validation, and protection logic function for these systems. The TXS platform will process the existing sensor inputs associated with the RPS and ESPS. Replacement is necessary to resolve obsolescence issues associated with the existing equipment. The new system is needed to assure continued reliable station operations and will provide on-line self-testing and diagnostic functions to improve the availability of the system and reduce maintenance burdens. All functions currently performed by the RPS and the ESPS will be maintained. The new equipment will meet or exceed the design requirements of the existing equipment.

Technical Specification (TS) changes are needed to support implementation of the digital upgrade and to take advantage of design features that support extending the Required Action (RA) Completion Times (CTs) for placing a channel in trip, automating channel checks and extending surveillance intervals for Channel Functional Tests (CFTs). Enclosure 3 describes the proposed TS changes, provides justification for those changes as well as TS and Bases markups denoting the changes, and Retyped pages.

Duke met with the NRC on May 25 and December 14, 2006, February 27 and April 30, 2007, by teleconference on July 10, 2007, and December 12, 2007, to discuss and agree on the format and content of the RPS/ESPS LAR and the associated design-related documents that need to be available at time of submittal and prior to issuance of the SER for this LAR. The format and content of this LAR is consistent with what was agreed upon during these meetings. The NRC documented by Memorandum dated August 1, 2007 (Reference 3), that Nuclear Energy Institute (NEI) 06-02 provides adequate guidance for the basic format and content of the LAR and that Regulatory Guide (RG) 1.206 Section C.I.7 provides adequate guidance for the technical portion of the LAR. Duke and the NRC also agreed that Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14 more appropriately addressed software quality assurance. The NRC Staff stated that in those instances where RG 1.206 and the SRP provide different guidance, the guidance of the SRP should be followed.

Table 1-2 lists design-related documents that the NRC Staff stated were needed to perform a review of the ONS RPS/ESPS LAR. The design-related documents listed in Table 1-2 are the same as those identified in a January 11, 2006 letter from the NRC (Reference 4) associated with an earlier RPS/ESPS LAR for this design change that was withdrawn. Duke added documents 16a, 16b, 44 and 45 for completeness. Table 1-2 denotes when each document will be available for NRC review.

The format and content of the information provided in this LAR is consistent with basic format and content guidelines of NEI 06-02. The technical evaluation contained in this enclosure is consistent with the guidelines of RG-1.206 Chapter C.I.7, applicable portions of SRP Chapter 7, and SRP BTP 7-14.

A description of the proposed design change is provided in Chapter 2, "Detailed Description," of this Enclosure. This chapter provides information needed by the NRC to perform a review of the RPS/ESPS digital upgrade consistent with that described in RG 1.206, Sections C.I.7.2, "Reactor Trip System," C.I.7.3, "Engineered Safety Feature Systems," and C.I.7.8, "Diverse Instrumentation and Control Systems."

Chapter 3, Technical Evaluation, provides information consistent with RG 1.206, Section C.I.7, Instrumentation and Controls, guidelines. This chapter addresses compliance of the ONS digital RPS/ESPS design to IEEE Standard (Std) 603-1998 and IEEE Std 7-4.3.2-2003. The chapter also describes testing performed or planned for the digital RPS/ESPS, provides a summary of the Failure Modes and Effects Analysis (FMEA) performed for the digital RPS/ESPS, and addresses the operations, maintenance, and support aspects of the new system to date.

Regulatory evaluation, environmental considerations, and references are provided in Chapters 4, 5, and 6, of Enclosure 1 respectively. Enclosure 3 provides a list of commitments associated with this LAR.

Duke requests approval of this amendment by January 31, 2009, to support the first implementation of this design change on Unit 1 during the fall 2009 refueling outage. As such, Duke requests the NRC make the amendment applicable prior to startup from the fall 2009 outage. Duke plans to implement this design change on Units 3 and 2 in the fall 2010 and 2011 refueling outages respectively.

The term ESPS is primarily used at ONS, however, because ESFAS is the industry generic term for this system, the majority of AREVA documents generated for the digital upgrade project use ESFAS. Either term is considered acceptable.

Table 1-1 TXS SER Plant-Specific Action Items

Note: Plant-specfic action items indicating that the licensee needs to conform to 10 CFR 50.34 (f) are not applicable since Oconee was licensed prior to February 16, 1982. However, where appropriate, Duke has provided a response.

SER Plant-Specific Action Item	Location of Response
1. The licensee must demonstrate that the generic qualification bounds the plant specific condition (i.e., temperature, humidity, seismic, and electromagnetic compatibility) for the locations(s) in which the TXS equipment is to be installed. The generic qualification data must comply with EPRI qualification requirements specified in EPRI TR-107330 and TR-102323-R1 (see SER Sections 2.1.2.1, 2.1.2.2, and 2.1.2.3).	Section 3.3.4 Section 3.4.4
2. The licensee's plant-specific software development V&V activities and configuration management procedures must be equivalent to industry standards and practices endorsed by the NRC (as referenced in SRP BTP HICB-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems") (see SER Sections 4.4, 2.2.3, 2.2.4).	Section 3.4.3 Section 3.6.4
3. If the licensee develops a TXS auxiliary feedwater control system, the licensee must include automatic initiation and flow indication (TMI Action Plan Item II.E.1.2). The licensee needs to confirm that the plant-specific application conforms to the requirements of 10 CFR 50.34 (f)g(2)(xii) (see Section 5.0).	The ONS Digital RPS/ESPS does not replace the existing auxiliary feedwater control system; therefore this SER action item is not applicable.

Table 1-1 TXS SER Plant-Specific Action Items (continued)

4. If the licensee replaces existing accident monitoring instrumentation (TMI Action Plan Item II.F.1) display capabilities with a TXS system, including the bypass and inoperable status information, the licensee needs to confirm that the new system provides equivalent sampling and analyzing features, and meets the requirements of 10 CFR 50.34 (f)(2)(xvii) (see Section 5.0).	As part of the design change, the Wide Range (WR) Nuclear Instrumentation (NI) Monitoring Equipment required to meet RG 1.97, Rev 2 is being relocated to a new cabinet. The ONS Digital RPS/ESPS provides equivalent cabinet mounting and physical location for this equipment as was provided by the original ONS Analog RPS/ESPS. Seismic qualification is maintained for the WR NI Monitoring Equipment. Power source independence and breaker coordination is maintained. The ONS Digital RPS/ESPS equipment qualification is maintained with the inclusion of the WR NI Monitoring Equipment in the cabinetry. Likewise, the WR NI Monitoring Equipment is not adversely impacted by the location of RPS/ESPS equipment.
5. If the licensee installs a TXS inadequate core cooling detection system, the licensee needs to confirm that the new system conforms to the requirements of 10 CFR 50.34 (f)(2)(xviii) (see Section 5.0).	The ONS Digital RPS/ESPS does not replace the existing inadequate core cooling detection system; therefore this SER action item is not applicable.
6. If the licensee installs a TXS containment isolation system (TMI Action Plan Item II.E.4.2), the licensee must verify that the plant-specific application conforms to the requirement of 10 CFR 50.34 (f)(2)(xiv) (see Section 5.0).	The ONS Digital RPS/ESPS performs and provides equivalent functions and functionality to the previous ONS Analog RPS/ES and continues to meet Duke's commitments under the NUREG-0737, TMI Action Plan Item - II.E.4.2.
7. For monitoring plant conditions following core damage, the licensee must verify that the TXS system meets the processing and display portions of the requirements of 10 CFR 50.34(f)(2)(xix)(see Section 5.0).	The ONS Digital RPS/ESPS does not replace existing systems for monitoring plant conditions following core damage; therefore this SER action item is not applicable.
8. If the licensee installs a TXS system for monitoring reactor vessel water level during post-accident conditions, the licensee must provide plant-specific verification of the ranges, and confirm that human factors issues have been addressed, as required by 10 CFR 50.34 (f)(2)(xxiv)(see Section 5.0).	The ONS Digital RPS/ESPS does not replace existing systems for monitoring reactor vessel water level during post-accident conditions; therefore this SER action item is not applicable.

Table 1-1 TXS SER Plant-Specific Action Items (continued)

SER Applicant Action Item	Location of Response
9. If the licensee installs a TXS reactor protection system, the licensee must provide confirmation that the TXS is diverse from the system for reducing the risk from anticipated transients without scram (ATWS), as required by 10 CFR 50.62. If the licensee installs a TXS ESFAS, the licensee must provide confirmation that the diversity requirements for plant systems (feedwater, auxiliary feedwater, turbine controls, etc.) are maintained (see SER Section 5.0)	Section 2.4
10. Setpoints will be evaluated on a plant-specific basis. The licensee must ensure that, when the TXS system is installed, overly conservative setpoints that may occur due to the elimination of analog system drift are not retained, as this would increase the possibility that the TXS equipment may be performing outside the vendor specifications. The licensee must provide the staff with a revised setpoint analysis that is applicable to the installed TXS system(s) (see SER Section 4.0).	Section 3.3.16.8
11. The licensee must evaluate plant-specific accident analyses to confirm that a TXS reactor trip system (RTS) includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown (safety analysis confirmation for accuracy and time response) consistent with the accident analysis presented in Chapter 15 of the plant safety analysis report (see SER Section 4.3).	Section 3.3.16.8, 3.5.3, 3.5.4
12. The staff requires that each licensee ensure that the plant-specific TXS application complies with the criteria of defense against common-mode failures in digital instrumentation and control systems (see SER Section 4.1).	Section 3.2.3
13. The licensee should propose plant-specific Technical Specifications including periodic test intervals (see SER Section 4.2)	Section 3.6.5 Enclosure 2
14. The licensee should demonstrate that the power supply to the TXS system complies with EPRI TR-107330 requirements (see SER Section 2.1.2.4)	Section 3.3.18
15. The licensee should demonstrate that the qualification of the isolation devices was performed in accordance with EPRI TR-107330 requirements (see SER Section 2.1.3).	Section 3.3.4

Table 1-1 TXS SER Plant-Specific Action Items (continued)

SER Applicant Action Item	Location of Response
16. The licensee should demonstrate that Siemens (AREVA system) TXP (control systems) or other manufacturer's control systems satisfy the acceptance guidance set forth in Section 4.1 of this safety evaluation (see SER Section 4.1).	Section 2.4.
17. The licensee should address the need for a requirement traceability matrix (RTM) for enumerating and tracking each system requirement throughout its life cycle, particularly as part of making future modifications (see SER Section 4.4).	See Table 1-2, Item 2 The RTM is a living document which will be maintained throughout the life cycle of the ONS TXS software development process and will be turned over to Duke, as part of the engineering design change documentation process. At that point ONS will control the requirements utilizing the Duke design change and configuration control processes.

Table 1-2 Technical Documents

Document Name	Document Number	Comment
1. Detailed System Architecture	AREVA NP Document No. 51-5045374	Available for NRC review
2. Oconee 1 RPS&ESFAS Requirements Traceability Matrix	AREVA NP Document No. 51-9002060	Pre-FAT version available for NRC review Post-FAT version available approximately 2 months after FAT
3. TELEPERM XS Product Information on Release 3.0.7A of TXS Software	2005/26	Available for NRC review
4. Oconee Nuclear Station TXS RPS/ESPS Replacement System Cabinet Design: 1PPSCA0005	AREVA NP Document No. 38-5069821	Available for NRC review
5. Oconee Nuclear Station TXS RPS/ESPS Replacement System Cabinet Design: 1PPSCA0006	AREVA NP Document No. 38-5069822	Available for NRC review
6. FMEA	AREVA NP Document No. 51-5023886	Available for NRC review
7. ONS 1, 2, & 3 RPS/ESF Controls Upgrade Design Specification for Key Locks and Key Switches	AREVA NP Document No. 51-5045379	Available for NRC review
8. Software Requirements Specification, ONS-1 RPS/ESF Software Requirements Specification (QA1)	AREVA NP Document No. 51-9054435	Available for NRC review
9. ONS Unit 1: RPS and ESFAS Replacement Project Open Item Form, "HW Typicals for CRD (Control Rod Drive) UV (under voltage) Test Jacks, Doc Step 3.12	Not applicable	Open Item closed – necessary changes incorporated into appropriate documents
10. ONS 1, 2, & 3 RPS/ESF Controls Upgrade Hardware Design Solutions	AREVA NP Document No. 51-5052833	Available for NRC review

Table 1-2, Technical Documents (continued)

Document Name	Document Number	Comment
11. ONS Unit 1 – RPS & ESFAS Configuration Management Plan	AREVA NP Document No. 51-9006444	Available for NRC review
12. Oconee Nuclear Station, Units 1, 2, & 3 RPS/ESF Controls Upgrade ID Coding Concept	AREVA NP Document No. 51-5058134	Available for NRC review
13. ONS Units 1, 2, & 3 RPS/ESFAS Controls Upgrade Verification and Validation Plan	AREVA NP Document No. 51-9010419	Available for NRC review
14. ONS Unit 1 RPS/ESFAS Controls Upgrade Software Design Description	AREVA NP Document No. 51-5065423	Available for NRC review
15. ONS Unit 1 RPS/ESFAS Controls Upgrade Software Requirements Review Report	AREVA NP Document No. 51-5066516	Available for NRC review
16. ONS Unit 1 – RPS & ESFAS Factory Acceptance Test Plan a. Factory Acceptance Test Procedures b. Factory Acceptance Test Results Report	AREVA NP Document No. 51-9052960 a. TBD b. TBD	Available for NRC review a. TBD b. TBD
17. Dedication Package for Absopulse Power Supply a. Procedure b. Report	 AREVA NP Document No. 51-5055058 AREVA NP Document No. 51-9062468 & 51-9062071	 Available for NRC review Available for NRC review
18. ONS Units 1, 2, & 3 RPS/ESFAS Controls Upgrade Software Safety Plan	AREVA NP Document No. 51-9005043	Available for NRC review
19. ONS Units 1, 2, & 3 RPS/ESFAS Controls Upgrade Software Installation Plan	N/A	No longer exists as a separate document. This document was incorporated into the AREVA NP Software Program Manual (Reference 11) that was submitted to the NRC for review and approval on 12/21/2006.
20. TXS Supplemental EQ (Equipment Qualification) Summary Test Report	AREVA NP Document No. 66-5015893	Available for NRC review

Table 1-2, Technical Documents (continued)

Document Name	Document Number	Comment
21. ONS RPS/ESFAS Replacement Project Equipment Qualification Report	AREVA NP Document No. 66-5065212	Available for NRC review
22. TUV Certificate on Communication Processor	968/K 110/02	Available for NRC review
23. TUV Documentation on SCP2 Testing	968/K 110.01/02	Available for NRC review
24. TUV Certificate on Processing Module	968/K 109/02	Available for NRC review
25. FANP (Framatome ANP) Report, "TELEPERM XS Simulation – Concept of Validation and Verification	NGLP/2004/en/0094	Available for NRC review
26. Configuration Management	NSD 106 & NSD 800	Available for NRC review
27. Software and Data Quality Assurance (SDQA) Program	NSD 800	Available for NRC review
28. Reactor Building Narrow Range Pressure Instrument Loop Accuracy Calculation (ESFAS)	OSC-2495	Available for NRC review
29. Wide Range RCS Pressure Uncertainty, (ESFAS HPI & LPI setpoints)	OSC-8829 (formerly OSC-2759)	Available for NRC review
30. RPS Main Feedwater Pump Pressure Instrument Loop Accuracy Calculation	OSC-3395	Not changed as a result of this design change.
31. RPS Flux/Flow Ratio Uncertainty Evaluation	OSC-8857 (formerly OSC-3416)	Available for NRC review
32. Reactor Building (RB) Pressure Instrument Loop Accuracy Calculation (ESFAS & RPS)	OSC-3446	Not changed as a result of this design change.
33. RPS RCS Pressure & Temperature Trip Function Uncertainty Analysis and Variable Low Pressure Safety Limit	OSC-8828 (formerly OSC-4048)	Available for NRC review
34. Power-Imbalance Safety Limits and Tech. Spec. Setpoints Using Error-Adjusted Flux/Flow Ratio of 1.094	OSC-5604 (to be revised prior to O3C24)	Only change to this document is due to changes in the other calculations. Available for NRC review – July 2009

Table 1-2, Technical Documents (continued)

Document Name	Document Number	Comment
35. RPS High Flux and Pump/Power Monitor Trip Function Uncertainty Analysis	OSC-8856 (formerly OSC-7237)	Available for NRC review
36. ONS Unit 1 – RPS & ESFAS System Functional Description	OSC-8623	Available for NRC review
37. Engineered Safeguard Feature Actuation System (ESFAS) Replacement Project Specification	OSS-0311.00-00-0012	Available for NRC review
38. Reactor Protection System (RPS) Replacement Project Specification	OSS-0311.00-00-0013	Available for NRC review
39. Duke Power Company, Oconee Nuclear Station, "Nuclear Instrumentation RPS Removal from and Return to Service for Channels A, B, C and D, Rev. 031, ETQS No. RPS-Q-ENTRY	Procedure No. IP/0/A/0305/015 (to be superseded by several new procedures)	Available for NRC review in October 2009
40. Documentation of Software Requirements and SDQA for RPS/ESFAS System Replacement	SDQA-10143-ONS	Available for NRC review
41. SIVAT LSELS Specifications, Job 4310002, Outputs: EFHV0037	Various	Available for NRC review Instead of a test case, Duke will make the SIVAT test procedures available for NRC review.
42. TELEPERM XS Function Blocks, Version 2.60 FB-ADDON, Version 1.2	TXS-1003-76-V10.0/01.04	Available for NRC review
43. SIVAT-TXS Simulation Based Validation Tool, Version 1.4.0 (now rev. 1.5.1)	TXS-1047-76-V2.0/01.04	Available for NRC review
44. Site Acceptance Test (SAT) Plan a. SAT Procedures b. SAT Results Report	TBD TBD TBD	August 1, 2008 a. TBD b. TBD
45. U1 Parameter Calc	OSC-8695	Available for NRC review

2. Detailed Description

2.1 Introduction

The RPS/ESPS design change replaces the analog controls originally manufactured by Bailey Meter Company with a TELEPERM XS (TXS) digital system manufactured by AREVA NP. The fail-safe designs of both systems are maintained in that the RPS fails to the tripped state on a loss of power and the ESPS fails to the non-actuated state on a loss of power.

The scope of the digital RPS/ESPS design change includes the following major components:

- Four RPS Protective Channels (A, B, C and D) for Reactor Trip functions. These channels also provide information to the control board and the Integrated Control System (ICS) (non-safety related functions).
- One RPS Channel (E) for providing information to the control board and the Integrated Control System (ICS) (non-safety related functions).
- Modification to the existing Reactor Coolant Pump Power Monitor (RCPPM) circuitry to resolve concerns with redundancy.
- Two redundant ESPS subsystems that share the same field sensor inputs:
  - Three ESPS Channels (ESPS Input Instrumentation Channels A2, B2 and C2) associated with a set of Odd/Even Voters (ESPS Voters Odd-2 and Even-2) capable of initiating all eight actuation output channels.
  - Three ESPS Channels (ESPS Input Instrumentation Channels A1, B1, and C1) associated with a set of Odd/Even Voters (ESPS Voters Odd-1 and Even-1) capable of initiating all eight actuation output channels. The ESPS Input Instrumentation Channels of this subsystem share the same TXS processors and some hardware with RPS Protective Channels A, B, and C.
- Two ESPS Component Status Cabinets and Component Status Panels for acquiring and display of status checkback information from ESPS field components.
- One Monitoring and Service Interface (MSI) unit (implemented using the same hardware as RPS Channel E), for transferring data to the TXS Gateway and the OAC and to and from the TXS Service Unit.

[ ]

- One TXS Service Unit
- One TXS Gateway
- One TXS Test Machine for use in performing initial tests of RPS/ESPS prior to the field devices being connected to the systems.
- One Diverse Low Pressure Injection Actuation System (DLPIAS)

- One Diverse High Pressure Injection Actuation System (DHPIAS)
- Limited changes to the control room as a result of the RPS/ESPS design change

This design change does not include a stand alone data communication system (DCS). All data communications occur within the RPS/ESPS. A simplified overview of the digital RPS/ESPS and additional components is shown in Figure 2.1-1 and 2.1-2.

Figure 2.1-1 Typical ONS Digital RPS/ESPS Network Architecture

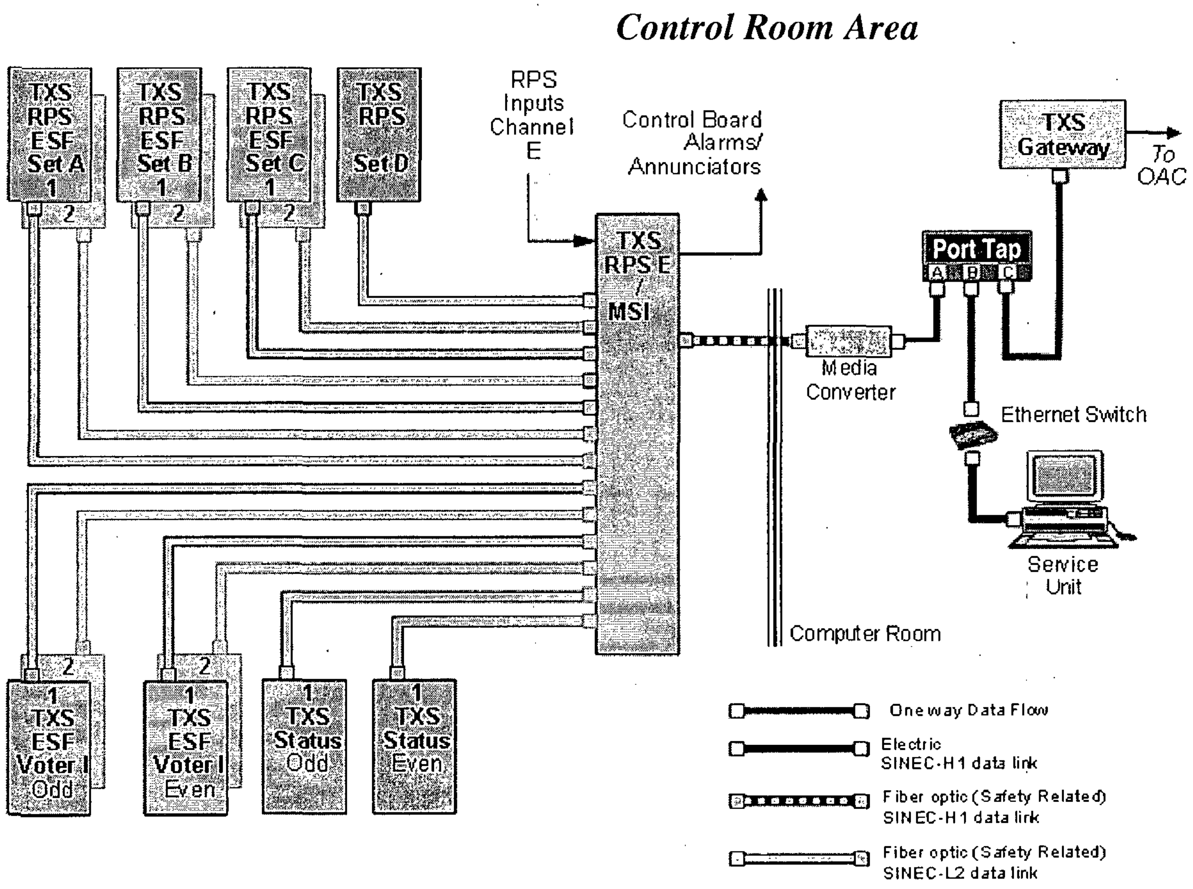
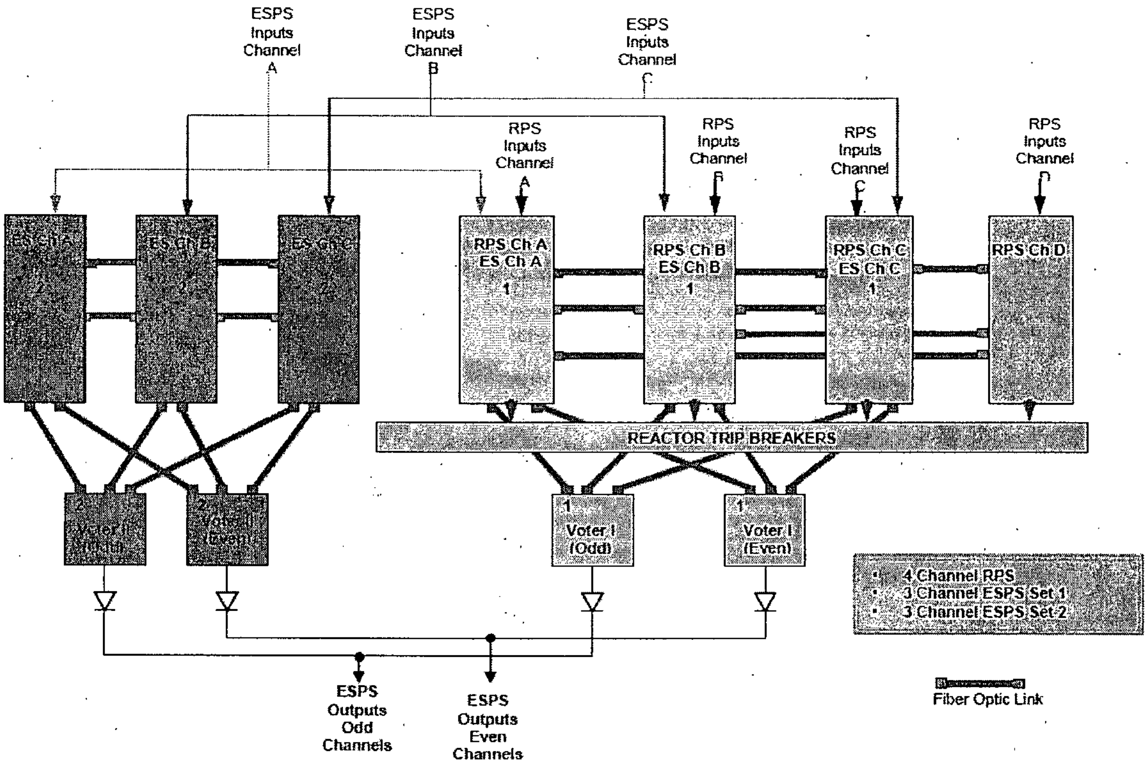


Figure 2.1-2 Typical ONS Digital RPS/ESPS Interchannel Communication Architecture



2.2 Reactor Protective System

The RPS consists of four redundant nuclear safety related protection channels (A, B, C and D) that perform reactor trip functions. A fifth RPS channel (channel E) does not perform a reactor trip function but provides non-safety related monitoring functions and signal outputs to the ICS.

The RPS is designed to monitor selected plant parameters related to safe plant operation and to generate reactor trip signals to protect the fuel and fuel cladding, the Reactor Coolant System (RCS) and the reactor building (RB) from damage. A reactor trip also limits energy input to the RB following a small break loss of coolant accident (SBLOCA) or a steam line break.

The RPS accomplishes its primary function by tripping the Control Rod Drive (CRD) breakers to shut down the reactor when any of the monitored parameters exceed predetermined trip set points. The following Reactor Trip functions are provided:

- Nuclear Overpower (Neutron Flux) Trip
- Nuclear Overpower Flux/Flow/Imbalance Trip
- RCS High Pressure Trip
- RCS Low Pressure Trip
- RCS Variable Low Pressure Trip
- RCS High Outlet Temperature Trip
- Reactor Building High Pressure Trip
- Loss of Both Main Feedwater Pumps Anticipatory Trip
- Loss of Main Turbine Anticipatory Trip
- Reactor Coolant Pump Power/Flux Trip

The RPS portion of the digital RPS/ESPS is shown in Figure 2.1-2.

2.2.1 RPS Channels A, B, C, and D

All RPS functions are implemented by sensors, instrument strings, logic strings and action devices that combine to form the four protection channels. Redundant protection channels and their associated elements are electrically independent and packaged to provide physical separation. Each RPS channel consists of two cabinets containing equipment for:

- Signal processing, conditioning and isolation,
- Direct current (DC) power supplies,
- Processing of the logic functions,
- Two-out-of-four relay logic for actuation of a reactor trip, and
- Communications between the different RPS channels and to the MSI and the Operator Aid Computer (OAC).

Each RPS channel also includes the following nuclear instrumentation:

- Linear amplifiers,
- Summing amplifier,
- Power range test module,
- Bipolar power supply, and
- Detector power supply..

The existing Gamma-Metrics Source Range and Wide Range Nuclear Instrumentation are being removed from the existing cabinets and installed in the new digital RPS Channels A, B, C, and D cabinets. No changes to the Gamma-Metrics equipment circuit design or functions have been made.

Each RPS protective channel has its own transmitters and contact inputs that provide process input signals. For transmitter 4-20 mA inputs, SAA1 Analog Signal Modules are used to convert the current signal to a voltage signal. Voltage signals from the SAA1 modules are supplied to two separate circuits. One circuit is the TXS S466 Analog Input Modules which converts the voltage input signals to digital counts for processing by the TXS SVE2 Processing Modules. TXS software A-MRC Function Blocks convert the input signal digital counts to engineering units. This circuit processes the field inputs and analyzes them to perform the reactor protective function. The second circuit, which receives the voltage output of the SAA1 module, is the SNV1 module. The TXS SNV1 Signal Multiplier Modules provide isolated analog outputs which are independent of the TXS processors. These isolated outputs provide signals to control board indicators, recorders, and to the non-safety Integrated Control System (ICS). This design allows actions such as placing an RPS Channel in Manual Bypass without affecting signals to indicators or to the ICS. It also prevents activities within the non-safety ICS from affecting the signals to the protective system. A similar design is used for power range detector NI flux signals in that the signals are processed separately into the TXS SVE2 processor and via SNV1 modules to provide isolated signals to indicators, recorders, and to the ICS.

For process signal contact inputs, the RPS supplies 120 volts alternating current (VAC) wetting voltage to the contact. This binary voltage signal from the contacts (~0 VAC when contact is open or ~120VAC when closed) is then converted to a 24 volts direct current (VDC) binary signal (~0 VDC or ~24 VDC) by an Optocoupler for the input to the digital input (S430) modules where inputs and status information are processed and sent to the SVE2 Processing Modules.

Each RPS protective channel exchanges the process variables obtained via fiber-optic data links. This enables each protective channel to perform validation checks, on-line signal monitoring and signal selection when processing the RPS functions. The SVE2 Processing Modules analyze the incoming signals and calculate the protective function outputs via the TXS application software. Each RPS channel powers four reactor trip relays associated with that channel but physically located one per cabinet in RPS channels A, B, C, and D (Refer to Figure 2.2-1). During normal operation these relays are energized by 24 VDC signals provided by a TXS S451 Digital Output Module to the coils of the relays.

2.2.1.1 RCPPM Design Change Description

The Reactor Coolant Pump Power Monitoring (RCPPM) circuit will be modified as part of the RPS/ESPS design change. The existing RCPPM circuitry does not have the needed redundancy to allow Duke to credit the pump monitors during flow coast-down events. Therefore, the existing RCPPM equipment is modified to provide the desired redundancy and is qualified via testing. Each RCPPM channel is modified to include the following new redundant components:

- Two new AC watt transducers,
- Two new electronic trip modules, and
- Two new time delay relays (adjustable).

The existing output/isolation relays in each RCPPM will be used to provide inputs to the RPS. Each of the 4 RCPPM channels provides an input to each of the 4 RPS channels. Therefore, each RPS channel receives a contact input providing information on the status of each of the 4 reactor coolant pumps and each of these inputs now has sufficient redundancy to prevent a single failure within a RCPPM channel from providing false information to all 4 RPS channels.

2.2.1.2 Process Input Signal Selection

Each RPS channel receives hardwired analog and binary (contact) process signal inputs. These process signals are provided to the other RPS channels over fiber optic communications links. The fiber optic links provide the desired 1E isolation so that the channels are electrically isolated to prevent undesirable electrical interaction due to equipment failures. Because the channels share input information, each channel can utilize 2.MIN or 2.MAX analog signal selection and two-out-of-four coincidence logic for binary input signals.

Refer to Section 3.4.6 of this Enclosure for explanation of why sharing of input information between safety related channels does not inhibit the performance of the safety function.

2.2.1.3 Analog Process Signal Selection Using 2.MIN/2.MAX

The digital RPS uses 2.MIN or 2.MAX Function Blocks for analog process input signal selection and signal validation. For signal selection, each protective channel uses the second lowest measurement to compare with the low set point value and then determines the partial trip status of that channel for a "low trip" parameter. Similarly, it uses the second highest measurement to compare with the high set point value and then determines the partial trip status of that channel for a "high trip" parameter. This TXS function will reject the outlying signal in the process measurement and thereby minimize inadvertent trips.

2.2.1.4 Binary Contact Process Signal Logic

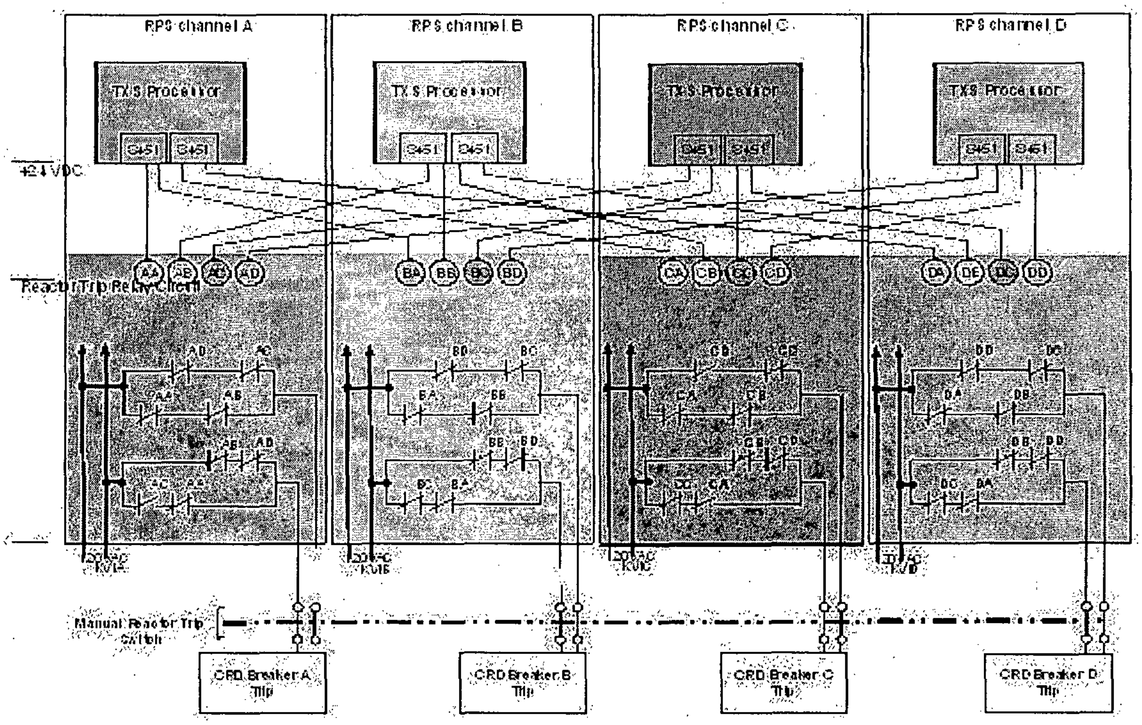
The digital RPS uses two-out-of-four logic Function Blocks to provide coincidence logic for RPS trip functions that utilize process contact inputs (e.g., pressure switches, RCPPM relays).

2.2.2 Reactor Trip Relay Circuits Description

Each RPS channel contains four physically separated relays, each powered from and actuated by the logic of a different RPS channel. When a particular RPS channel determines that a trip condition has been reached, a trip output is generated by that channel and the four trip relays associated with that channel are de-energized. For example, if channel A senses a trip condition, relays AA, BA, CA, and DA will all be de-energized. Refer to Figure 2.2-1.

The output contacts of the four reactor trip relays are wired to provide two-out-of-four coincidence logic to de-energize the under-voltage trip coils and energize the shunt trip coils in order to trip the CRD breaker associated with each RPS channel. Each breaker under-voltage circuit is monitored by a shunt trip relay as a back-up RPS trip. If the under-voltage power is removed due to either an RPS automatic or manually initiated trip, the shunt relay will cause the shunt trip coil to be energized and trip the breaker. The reactor trip relays located in RPS Channel A cabinet provide the two-out-of-four relay logic to trip CRD breaker A. The reactor trip relays in RPS Channel B trip CRD breaker B and so on. If two or more channels of RPS indicate a valid trip condition, all four CRD breakers will trip. For the safety related trip function, the CRD breakers operate in a one-out-of-two-taken twice configuration to remove power to the CRD mechanisms, thus tripping the reactor.

Figure 2.2-1 Typical Digital RPS Protection Channel and Reactor Trip Relay Logic



NOTE: The reactor trip relays are shown in the energized state therefore their relay contacts are shown closed. Contact shelf state is open.

2.2.3 Manual Reactor Trip

The existing ONS design provides a Manual Reactor Trip Pushbutton on the main control board. When pushed, the Manual Reactor Trip Pushbutton de-energizes the undervoltage relays and the interposing relays to the shunt trip coils of the CRD breakers. This causes the CRD breakers to trip thereby de-energizing the CRD motors. When the motors are de-energized, control rods drop into the reactor core. In this manner, the Manual Reactor Trip Pushbutton gives Control Room Operators (CROs) the capability to initiate a reactor trip at any time independent of the status of the RPS. This feature is not affected by the RPS/ESPS replacement and will continue to function and be utilized without impact from the design change.

2.2.4 RPS Channel E (Non-Safety Related Functions)

RPS Channel E performs non-safety related monitoring and provides non-safety related signals to the ICS. This channel performs no reactor protective functions. No functional changes to the relationship between the safety related reactor protective function and to RPS Channel E are made by this design change. RPS Channel E resides in cabinet 16. The field devices providing signals to RPS Channel E are separate and independent from those supplying signals to RPS Channels A, B, C, and D. Signals within the RPS Channel E cabinet are processed similar to those in the protective system channels. Field signals are conditioned and converted and input into a TXS SVE2 processor. This processor provides alarm information related to the Channel E signals to the OAC via the Monitoring and Service Interface. The Channel E signals are also supplied to indicators and to the ICS via SNV1 modules.

RPS Channel E application software runs on one of the four processors used for MSI communications. RPS Channel E functions are not safety related; however, the processor and all related TXS hardware are considered safety related due to the MSI communications isolation function.

2.3 Engineered Safeguards Protective System

The digital ESPS consists of two redundant nuclear safety related subsystems each consisting of three input channels (A, B, and C) and eight actuation logic channels grouped into an Odd Voter (Channels 1, 3, 5, and 7) and Even Voter (Channels 2, 4, 6, and 8). The input sensors are shared between subsystems. Either subsystem can perform the required safety function.

The ESPS is designed to mitigate the effects of various postulated accidents (see Chapter 15 of the ONS UFSAR) by:

- Injection of coolant into the primary system if reactor coolant system (RCS) pressure becomes low, and
- Isolation and cooling of the Reactor Building (RB) if RB pressure becomes high.

ESPS protective functions are listed below. Each function is executed by redundant and independent Engineered Safeguards (ES) equipment trains.

- High Pressure Injection (HPI) and RB Non-Essential Isolation function is initiated if RCS pressure < Low Limit or RB Pressure > High Limit.
- Low Pressure Injection (LPI) is initiated if RCS pressure < Low-Low Limit or RB Pressure > High Limit.
- RB Cooling and RB Essential Isolation function is initiated if RB Pressure > High Limit.
- RB Spray function is initiated if RB Pressure > High-High Limit.

The ESPS portion of the digital RPS/ESPS is shown in Figure 2.1-2.

2.3.1 ESPS Channels A, B, and C

The digital ESPS consists of two subsystems. Each subsystem consists of three Instrument Input Channels (A1, B1, C1 and A2, B2, C2). Each pair of ESPS channels shares process variable sensors. For example, the same RC pressure transmitter input to channel A1 is also provided to channel A2 (See Figure 2.1-2).

Subsystem 1 (channels A1, B1 and C1) is located in the same cabinets used for RPS Protective Channels A, B and C. Subsystem 1 functions are implemented by the same TXS processors as the RPS functions. ESPS Subsystem 2 includes channels A2, B2 and C2. Subsystem 2 functions are implemented by processors physically located in separate cabinets that are not used by the RPS. Each channel in Subsystems 1 and 2 contains the following:

- Signal processing, conditioning and isolation equipment for each plant variable and control signal monitored.
- AC/DC power supplies.
- Equipment to process the plant variables to determine if a protective action is required.
- Equipment to provide outputs to the control room Statalarm system.
- Communication links with the other ESPS channels and voters of this subsystem and the MSI.

Analog inputs from transmitters are supplied to ESPS Subsystem 2 cabinets. The transmitter 4-20 mA signals are input to TXS SAA1 modules which are used to convert the current signal to a voltage signal. Voltage signals from the SAA1 modules are supplied to two separate circuits within a channel of this subsystem. One circuit is the TXS S466 Analog Input Modules which converts the voltage input signals to digital counts for processing by the TXS SVE2 Processing Modules. TXS software A-MRC Function Blocks convert the input signal digital counts to engineering units. This circuit processes the field inputs and analyzes them to perform the safety related engineered safeguards protective function. The second circuit, which receives the voltage output of the SAA1 module, is the SNV1 module. The TXS SNV1 Signal Multiplier Modules provide isolated analog outputs, which are independent of the TXS processors. These isolated outputs provide signals for recorders. The same transmitter signal that is supplied to an ESPS Subsystem 2 channel is also supplied to its respective Subsystem 1 channel via an SNV1 module.

For process signal contact inputs, ESPS Subsystem 2 supplies 120 VAC wetting voltage to the contact. This binary voltage signal from the contacts (~0 VAC when contact is open or ~120 VAC when closed) is then converted to a 24 VDC binary signal (~0 VDC or ~24 VDC) by an Optocoupler for the input to an S430 Digital Input Module where inputs and status information are processed and sent to the SVE2 Processing Modules. The incoming process contact input signal that is input to an ESPS Subsystem 2 channel is also paralleled to the respective ESPS Subsystem 1 channel on the 120VAC side.

Each ESPS input channel receives hardwired analog and binary (contact) process signal inputs. These process signals are provided to the other ESPS input channels within the same subsystem over fiber optic communications links (see Figure 2.1-2). The fiber optic links provide the desired 1E isolation so that the channels are electrically isolated to prevent undesirable electrical interaction due to equipment failures. Because the channels share input information, each channel can utilize 2.MIN or 2.MAX analog signal selection and two-out-of-three coincidence logic for binary input signals.

The ESPS uses 2.MIN or 2.MAX Function Blocks for analog process input signal selection, on-line signal monitoring and signal validation. For signal selection, each ESPS channel uses the 2nd lowest measurement to compare with the low set point value and then determines the partial trip status of that channel for a "low trip" parameter. Similarly, it uses the 2nd highest measurement to compare with the high set point value and then determines the partial trip status of that channel for a "high trip" parameter. This TXS function will reject the outlying signal in the process measurement and thereby minimize inadvertent trips.

The ESPS uses two-out-of-three logic Function Blocks to provide coincidence logic for ESPS protective actuation functions that utilize process contact inputs (i.e., RB pressure switches). These binary inputs are also compared for deviations/faults.

Each channel monitors RCS pressure and RB pressure and will issue a demand to the Voters via fiber optic data link for ESPS protective functions if the values violate set point limits. The ESPS voters monitor for the required coincident logic (two-out-of-three) to initiate the system level protective actions (initiation of an output actuation channel). The ESPS channels and their associated elements are electrically isolated, functionally independent, and packaged to provide physical separation.

In addition to the protective actions performed, the following functions are implemented on the ESPS channels indicated:

- Provide an isolated wide range analog RCS pressure signal to the Transient Monitoring system and a chart recorder from either ESPS Channel A2 or B2. If power to Channel A2 fails, the redundant signal from Channel B2 automatically aligns to the circuit via a transfer relay. Or, if preferred, the alternate Channel B2 signal can be selected manually.

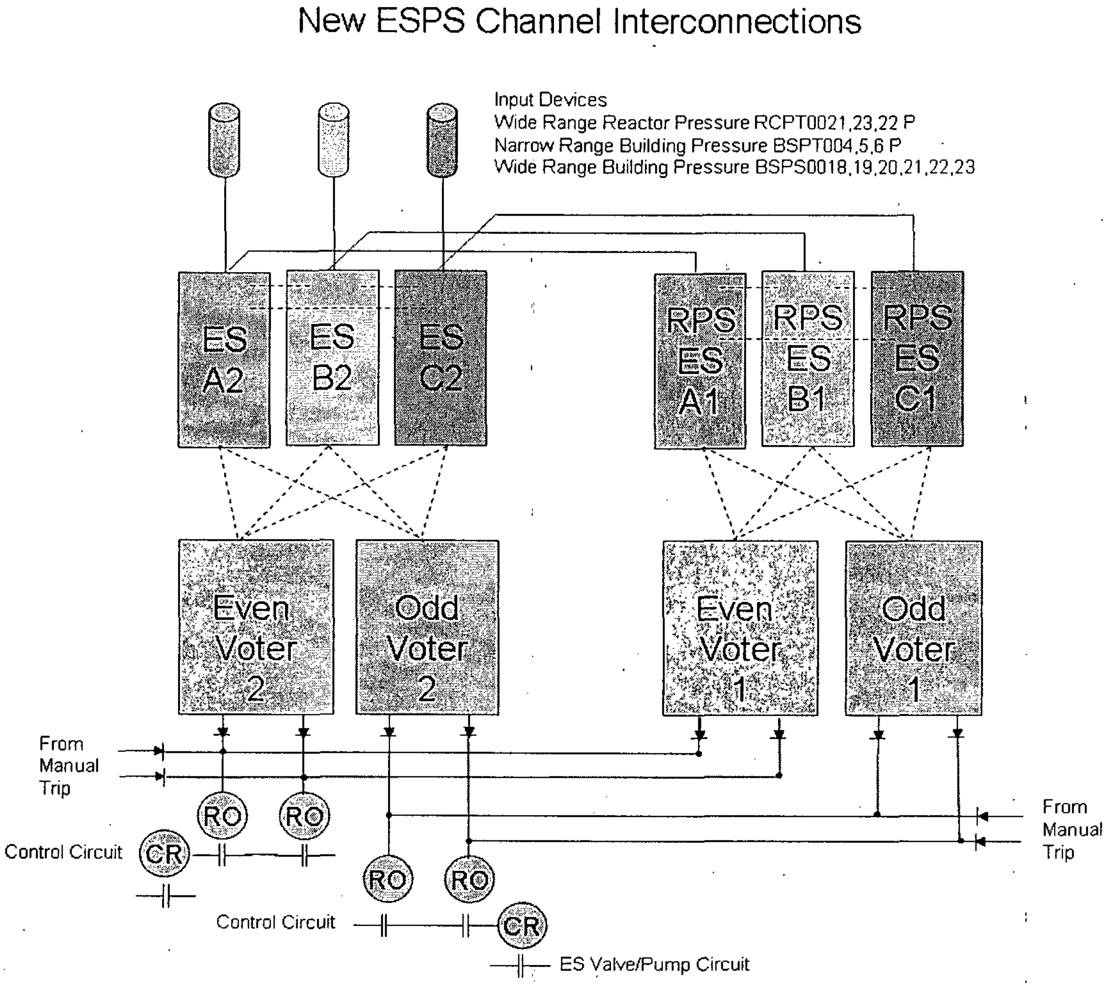
- Channels A1 and A2 provide an isolated output contact to drive the HPI Bypass Enable Statalarm. The contacts are wired in an "or" configuration so either subsystem can drive the Statalarm indication.

- Channels A1 and A2 provide an isolated output contact to drive the LPI Bypass Enable Statalarm. The contacts are wired in an "or" configuration so either subsystem can drive the Statalarm indication.

- Channels A1 and A2 provide an isolated contact output to the ICS system. The signal indicates degraded building pressure. The contacts are wired in an "or" configuration so either subsystem can provide the signal to the ICS.

- The Odd Voters provide an interlock permissive signal to Reactor Coolant System to Low Pressure Injection (RCS/LPI) Isolation valve LPVA0001. This valve is the first LPI valve off of the RCS and is interlocked to prevent inadvertent opening during normal operation. When RC pressure decreases below 400 psig, an OPEN interlock permissive signal to LPVA0001 is supplied by a voted signal out of the TXS. Either ESPS subsystem (1 or 2) may provide the interlock output from its respective Odd voter (Odd-1 or Odd-2).

Figure 2.3-1 Typical New ESPS Channel Interconnections



2.3.2 Odd & Even Voters and Actuation Channels 1 Through 8

Each ESPS voter subsystem (Odd-1, Odd-2, Even-1, and Even-2) is equipped with two TXS SVE2 Processing Modules, operating in a Master/Checker configuration.

The Master/Checker processors acquire the same input information, operate in a synchronized mode, and execute the same application function. At the end of each processing cycle, prior to sending the output commands to the output modules, the Master and Checker compare their results. If the results agree, the required output command is sent to the output modules of the Voter.

If a calculation mismatch occurs between the Master/Checker processors, the respective subsystem automatically disables all of its output modules by shutting down the power supply to the output modules, generates an alarm, and initiates a reboot of the Voter subsystem. The Master/Checker operation is designed to prevent spurious actuations.

The remaining Voter subsystems remain operable, as each Voter can actuate its respective output channel and components independently. This is achieved by wiring the binary output signals of the Even Voters in a "wired-or" configuration. The Odd Voter channels are wired similarly.

Each ESPS Voter subsystem uses two outputs from separate binary output (S451) modules to actuate each ESPS actuated device. ESPS actuated devices are actuated by two relays connected in series. To actuate a device, TXS must send a "high" signal from both binary output modules to close the actuation relays. Each system generates signals to the Statalarms (control board indicators).

The ESPS Voters monitor for the required coincident logic (two-out-of-three) to initiate the system level protective actions (actuation channel initiation). The actuation channels and the plant variables required to initiate the protective function are shown in Table 2-1.

Table 2-1 Channel Protective Function(s) Initiated and Plant Variables Monitored

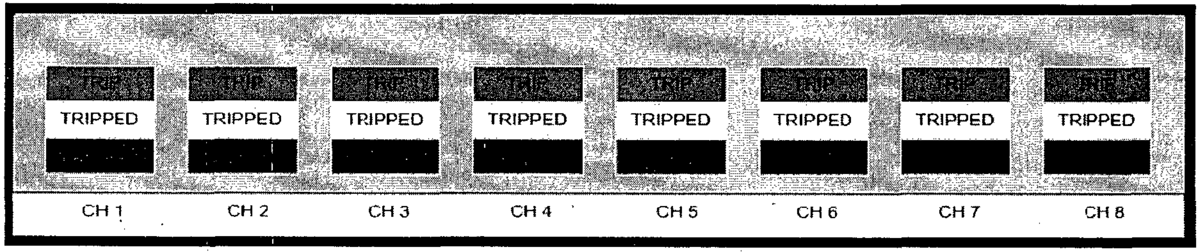
Channel	Protective Function(s) Initiated	Plant Variable Monitored
Channel 1	Odd - HPI and RB Non-essential Isolation, Keowee Start, Load Shed and Standby Breaker 1 Input, and Keowee Standby Bus Feeder Breaker Input	High RB Pressure or Low RC Pressure
Channel 2	Even - HPI and RB Non-essential Isolation, Keowee Start, Load Shed and Standby Breaker 2 Input, and Keowee Standby Bus Feeder Breaker Input	High RB Pressure or Low RC Pressure
Channel 3	Odd – LPI and Low Pressure Service Water	High RB Pressure or Low-Low RC Pressure
Channel 4	Even – LPI and Low Pressure Service Water	High RB Pressure or Low-Low RC Pressure
Channel 5	Odd – RB Cooling and RB Essential Isolation	High RB Pressure
Channel 6	Even – RB Cooling and RB Essential Isolation	High RB Pressure
Channel 7	Odd – RB Spray	High-High RB Pressure
Channel 8	Even – RB Spray	High-High RB Pressure

In addition to the above ESPS actuation signals, the Odd Voters are used to provide an interlock permissive signal to the RCS Pressure/LPI Isolation valve. This valve is the first LPI valve off of the RCS and is interlocked to prevent inadvertent opening during normal operation. When RCS pressure decreases below 400 psig, an open interlock permissive signal to the RCS/LPI isolation valve is supplied by a voted signal out of the TXS, from contact outputs in the Odd Voter cabinet (Cabinet 13). Either ESPS subsystem (1 or 2) may provide the interlock output from its respective Odd voter (Odd-1 or Odd-2). Although credit is taken in the safety analysis for the ability to open the RCS Pressure/LPI isolation valve as a secondary boron dilution flow path, this is not an ES required function and thus the interlock circuit does not have to meet the single failure criteria.

2.3.3 Manual Channel Trip and Reset

The existing ESPS Trip/Reset pushbutton switches will be replaced by new devices powered from the TXS system (24 VDC). The pushbuttons allow each actuation channel (1 through 8) to be manually tripped from the Manual Trip pushbuttons on the Unit Board. Manual trip is independent of the TXS software and can be initiated during any mode of operation. Each actuation channel (1 through 8) can be manually reset from the Reset pushbuttons on the Unit Board following either automatic or manual actuation of the channel. Use of Manual Trip pushbuttons is controlled by Operations procedures.

Figure 2.3-2 Typical Actuation Channel Trip Pushbuttons



2.3.4 Auto/Manual Pushbuttons

The Auto/Manual function is an existing feature of the ESPS. Following an event where the ESPS has actuated, the CRO uses these switches to apply or remove the actuation signal to each ESPS actuated component. With the switch in Automatic, the ESPS signal is applied to the component to maintain it in its ESPS position. Selecting Manual causes the relay contact for each actuated component in the associated output logic channels (Channels 1 through 8) to go open. This permits the operator manual control of the individual components from the normal component control switches. In the existing ESPS system, selecting Auto/Manual is an action that must be taken for each component at its RZ module.

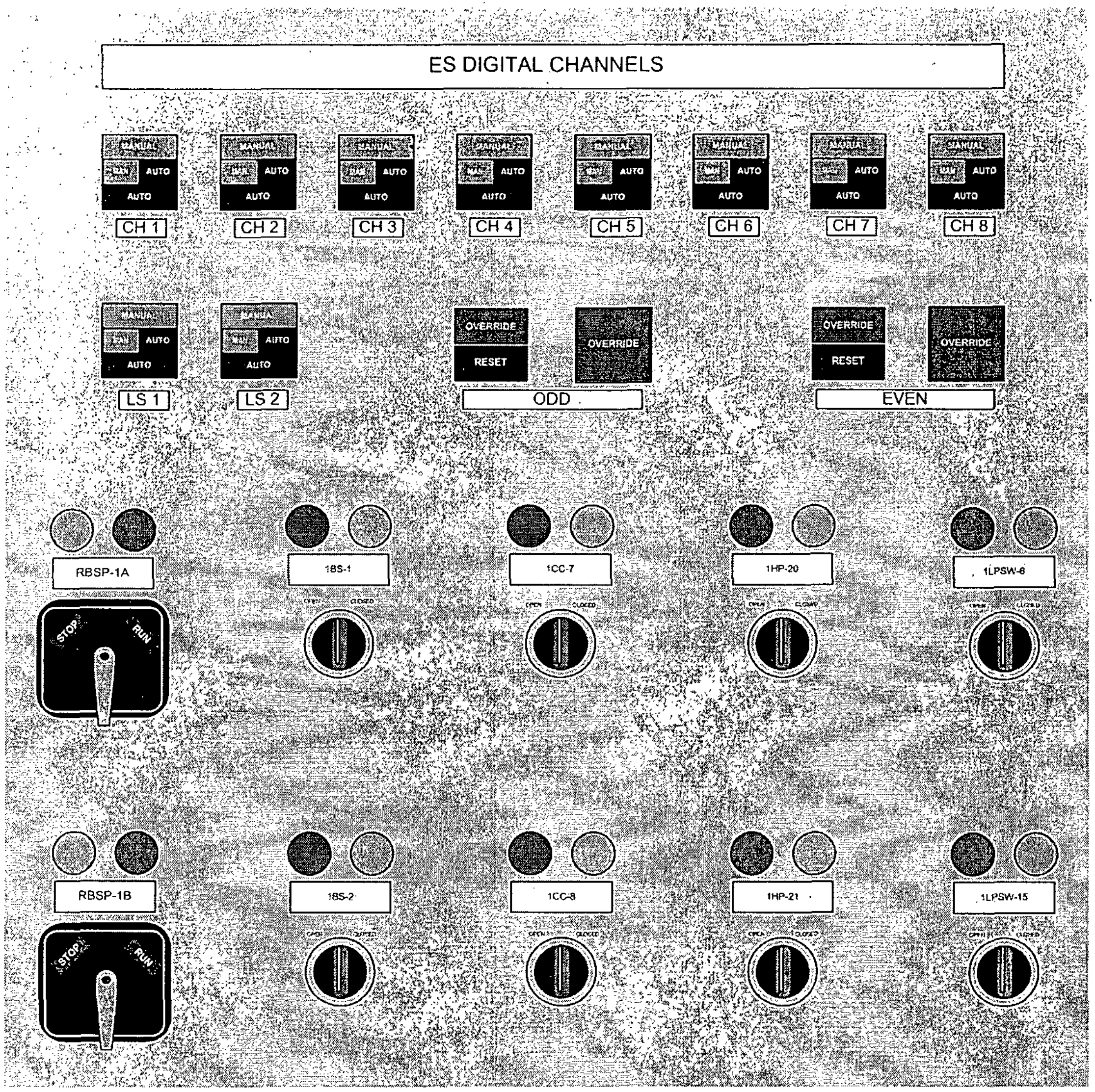
The existing individual component function will be replaced with a new ESPS individual logic channel "level" Auto/Manual function. Each of the eight ESPS logic channels will have an individual auto/manual pushbutton selector switch. These new switches will be installed on the UB2 control board. Each pushbutton switch will include LEDs to indicate that either the Auto or Manual mode is selected. If an ESPS actuation signal (automatic or manual) is not present, the Auto/Manual pushbutton switches have no control function and the indicating light emitting diodes (LEDs) will be off. Once an ESPS actuation signal is initiated, either from an automatic system demand actuation or by operator manual initiation actuation, the Auto light will be illuminated and the Auto/Manual pushbutton functions may then be selected from this control point.

With the Auto/Manual pushbutton in Auto, the ESPS operates in the safeguards control mode. However, if it is desired to take manual control of the ESPS channel or the individual associated actuated components for that channel, the Manual mode can be selected. When the Manual mode is selected, the individual actuation components in that associated channel may then be operated from the normal component control switch. If Manual has been selected and the operator wishes to place the channel components back in the ES position, the operator can push the Auto pushbutton and the channel components will go to the ES position. Once an ESPS channel has been reset using the Reset pushbutton, the Auto/Manual LEDs for that channel will go out and the Auto/Manual pushbuttons will no longer respond.

ESPS Actuation Output Logic Channels 1 and 2 provide a signal to the Load Shed logic in addition to actuating High Pressure Injection Pumps and RB Non-Essential Isolation. While no changes are being made to the functionality of the Load Shed circuitry as part of this design change, a brief description of the intent of Load Shed is provided. The emergency power source for ONS is provided by Keowee Hydro Units (KHUs) 1 and 2. In the event that offsite power sources to ONS are lost and the emergency power source is demanded, one KHU will start and provide power to ONS via an overhead power path to the 230KV switchyard, and then to the respective startup transformer of each ONS unit to the main feeder buses. If this is successful, this KHU and the capacity of the startup transformers are capable of supplying the needed shutdown loads (4 kV and less) of the ONS units. The other KHU will also start and provide power to ONS via an underground power path through the CT4 transformer. If power is available on the ONS main feeder buses via the other KHU to the overhead path, breakers between the CT4 transformer and the ONS main feeder buses (designated the Standby breakers - each ONS unit has a pair of Standby breakers between CT4 and the main feeder buses) do not close. However, if a failure of the overhead power path to provide power occurs, the under voltage condition that is sensed on the ONS main feeder buses will close the Standby breakers. Additionally if one of the ONS units has a condition which has caused the ESPS to actuate Channels 1 and 2, that unit's Standby breakers will close in to provide power to that unit faster than for the other 2 ONS units because of the presence of the ESPS signal. The most limiting factor for power to the ONS units in this situation is the capacity of the CT4 transformer. Since the CT4 transformer does not have the capacity of the startup transformers, non-essential loads are shed from the main feeder buses prior to closing the Standby breakers. This is done by Load Shed circuitry. During an actuation of ESPS actuation output logic channels 1 and 2, signals are supplied to start the KHUs and signals are supplied to the Load Shed circuitry and the Standby breakers. If power is available on the main feeder buses via the startup transformers, the ESPS loads are powered via the startup transformers. KHUs are started by ESPS but they operate in standby if the startup transformer power sources are available. Likewise, ESPS actuation alone does not initiate Load Shed. However, if power is not available on the main feeder buses via the normal or startup transformer sources during the ESPS actuation, the Load Shed circuitry is initiated and ESPS loads are supplied from a KHU via CT4. The presence of the ESPS signal provides a seal-in circuit for the Load Shed actuation in this case.

Load Shed logic Channels 1 and 2 will have separate Auto/Manual pushbutton selector switches from the switches used to select Manual for the balance of the ESPS Channel 1 and 2 components. The Load Shed 1 and 2 switches are installed on UB2 control board below the Auto/Manual switches for ESPS logic channels 1 and 2. These selector switches will allow the Load Shed & KHU Emergency Start permissive logic to remain enabled even if the operator places the ESPS Channels 1 or 2 Auto/Manual switches in the MANUAL mode. This gives the operator the ability to take manual control of the ESPS Channel 1 or 2 components while maintaining the Load Shed & KHU emergency start logic in an actuated state if only the CT4 power source is available. Allowing separate action to take manual control of ESPS Channel 1 or 2 components versus taking manual control to clear the Load Shed & Keowee Emergency Start signal from ESPS is consistent with the actions that are required for the existing ESPS.

Figure 2.3-3 Typical ESPS Related Devices



The following ESPS related devices shown in Figure 2.3-3 will be installed on the Unit 1 control boards. These changes are typical of changes being made for Units 2 and 3.

- First row in Figure 2.3-3 - Channel 1 through 8 Auto/Manual selector switches
- Second row in Figure 2.3-3 - Load Shed Channel 1 and 2; Odd and Even Voter Emergency Override switches and indicator lights
- Third row in Figure 2.3-3 - RBSP-1A, 1BS-1, 1LPSW-6, 1CC-7, 1HP-20 (Control switch and indicating lights for 1 HP-20 will be moved from existing location on 1UB1 to new location on 1UB2.)
- Fourth row in Figure 2.3-3 - RBSP-1B, 1BS-2, 1LPSW-15, CC-8, 1HP-21

2.3.5 ESPS Emergency Override

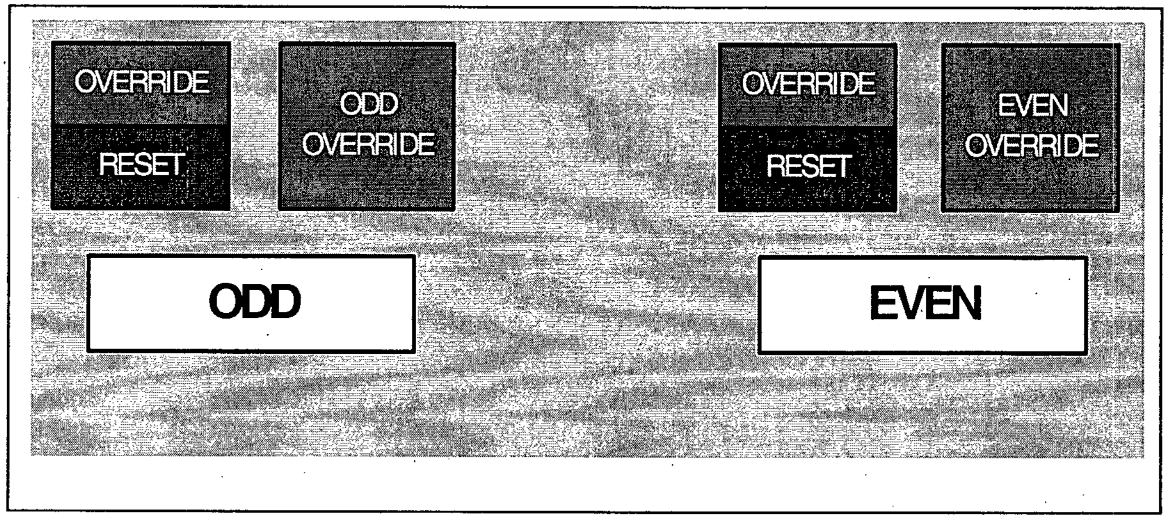
The RPS/ESPS digital upgrade adds a new ESPS Emergency Override feature that ensures the CRO is capable of taking control of all ESPS devices should there be an inadvertent ESPS actuation resulting from a failure of the TXS system (e.g. common mode software failure). Two new Emergency Override pushbuttons (one Odd and one Even) will be installed on the unit board near the new ESPS Auto/Manual pushbuttons.

Actuation of the ESPS Emergency Override switch will de-energize the automatic outputs to all ESPS actuated field devices. Manual control by the CRO using the Auto/Manual pushbuttons will still be possible. A Reset pushbutton is also provided to allow that Voter's output boards to be re-energized following return of the digital ESPS to normal operation.

Operation of either Override is indicated to the control room through separate Statalarm windows and via a red light located next to each pushbutton.

The Override only affects the automatic system. It does not affect the ability of the operators to manually actuate the channels via the Manual Trip pushbuttons or the ability of the Diverse Low Pressure Injection Actuation System (DLPIAS) or Diverse High Pressure Injection Actuation System (DHPIAS) to actuate channels. Override pushbuttons are equipped with flip covers to prevent inadvertent operation (Reference Figure 2.3-4).

Figure 2.3-4 Typical Emergency Override Pushbuttons



2.3.6 ES Odd and Even Device Status Panels

The existing RZ Module control/status indication panels are replaced as part of this design change. The RZ modules provide indication to the operator of component (valve, pump, etc.) status following an ESPS actuation. The RZ modules are arranged to provide indication by actuation channel (1 through 8). For some ESPS actuated components, the RZ modules provide status indication only and the control switches for the associated components are located separately on the control board. For other ESPS actuated components, the RZ modules provide status indication and also include the control switches that are used to operate the associated components manually. For other ESPS actuated components, the RZ modules provide both status indication and control capability for the components and each component has an additional switch located elsewhere on the control board that can be used to operate the component when ESPS is not actuated.

The RZ Module status indicating equipment of the existing ESPS will be replaced with new ES Device Status Panels that will indicate the status of each device actuated by the ESPS arranged by channel. These Status Panels provide status indication only. For those ESPS actuated components which had control switches located only on the RZ modules, new control switches are added to the control boards so that for each ESPS actuated component, there will be a consistent method for operating the components. The new control switches will be mounted on control boards VB2 or on UB2 as follows:

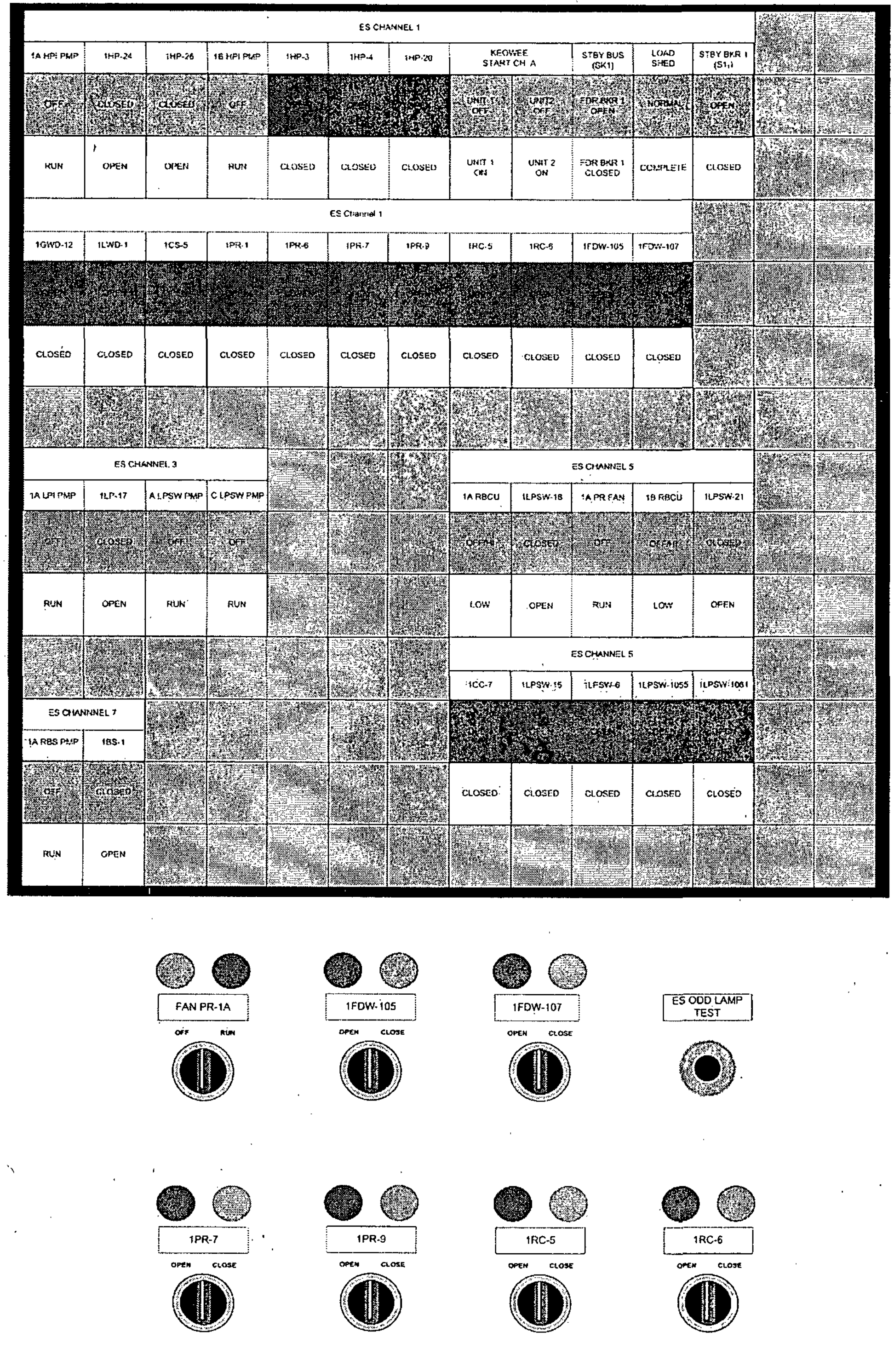
- The following ESPS Odd Channel components will have new control switches installed on VB2 below the new ESPS Odd Channel Status Panel – PR Fan A, Valve 1FDW-105, Valve 1FDW-107, Valve 1PR-7, Valve 1PR-9, Valve 1RC-5, and Valve 1RC-6.
- The following ESPS Even Channel components will have new control switches installed on VB2 below the new ESPS Even Channel Status Panel – PR Fan B, Valve 1FDW-106, Valve 1FDW-108, Valve 1PR-3, Valve 1PR-8, Valve 1PR-10, and Valve 1RC-7.
- The following ESPS components will have new control switches installed on UB2 below the selector switches for ESPS Channel 1-8 Auto/Manual Control - RB Spray Pump 1A, RB Spray Pump 1B, Valve 1BS-1, Valve 1BS-2, Valve LPSW-6, Valve LPSW-15, Valve 1CC-7, Valve 1CC-8, Valve 1HP-20, and Valve 1HP-21 (Control switch for 1HP-20 is re-located from UB1 to UB2).

The existing RZ modules receive their power from Motor Control Centers 1XS1 or 1XS2 through control power transformers. The new status panels use LEDs powered from the RPS/ESPS (24 VDC from Absopulse Power Supplies which receive their power from battery/inverter backed vital power panel boards). When a logic channel of ESPS is actuated, either automatically or with the trip pushbutton switch, the associated ES position light for the device on the status panel will begin to flash on and off. Once the device has reached its ES position, the light will stop flashing and stay on. The new status panel will have an external push button that can be used to test all the lamps on the status panel. Pushing the test push button will provide a 24 VDC signal to each of the status panel LEDs from the TXS equipment.

The Odd ES Component Status processor receives data from output Channels 1, 3, 5 and 7. The Even ES Component Status processor receives data from output Channels 2, 4, 6 and 8. Status of ES components (in ES position or in non-ES position) is received at the Component Status cabinets via hardwired contacts. Status indication is converted from a 120 VAC signal to a 24 VDC signal and sent to the appropriate Component Status processor and to the ES Device Status Panels. The Component Status processor sends status information to the MSI for transmission to the OAC via the TXS Gateway computer.

Figure 2.3-5 Typical Device Status Panel Arrangements on 1VB2

ODD CHANNELS



2.4 Diverse Instrumentation & Control (I&C) Systems

2.4.1 Existing Diverse Systems

Duke evaluated existing ONS plant control systems, manual controls, and Anticipated Transient Without Scram (ATWS) systems to confirm diversity between them and the TXS based RPS and ESPS as part of the Defense in Depth and Diversity (D3) assessment described in Section 3.2.3 of this Enclosure. This evaluation is provided in sections 2.4.1.1, 2.4.1.2, and 2.4.1.3 below.

2.4.1.1 Plant Control Systems

ONS plant control systems listed in Section 6.3 of the D3 assessment (Reference 5) were evaluated to confirm diversity between them and the TXS based RPS and ESPS as part of the D3 assessment described in Section 3.2.3 of this Enclosure. None of these ONS control systems are part of this digital design change or TXS based. As a result, the diversity between the control systems and the RPS and ESPS will be ensured. If plant control systems are modified in the future then the diversity arguments presented in the D3 assessment will be applied and re-evaluated as part of the design change at that time.

The KHUs, which are the emergency power sources for ONS, use a TXS system in the KHU governor control system. BTP 7-19 defines the control system echelon as consisting of non-safety equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is used in the normal operation of the reactor. As such, the safety related KHUs were not considered a control system and their failure was not postulated concurrent with a SWCMF of the RPS/ESPS nor was this failure scenario considered credible.

2.4.1.2 Manual Controls

Manual controls and displays supporting CRO actions to place the nuclear plant in a hot shutdown condition, and to perform reactivity control, core heat removal, reactor coolant inventory control, containment isolation, and containment integrity actions were verified as adequate as part of the D3 analysis described in Section 3.2.3. In summary, manual controls and displays needed to shut down the plant are not affected by a postulated software common mode failure (SWCMF) that is assumed to render the RPS/ESPS inoperable in the D3 assessment.

The D3 design features conform to the guidance of SRP Chapter 7, BTP HICB-19, Revision 4, "Guidance for Evaluation of Defense-in-Depth & Diversity in Digital Computer-Based Instrumentation and Control Systems." Refer to Section 3.2.3 of this Enclosure for more detail regarding this subject.

2.4.1.3 Anticipated Transient without Scram (ATWS) Mitigation System

The ONS ATWS Mitigation System is composed of two parts; the ATWS Mitigating System Actuation Circuitry (AMSAC) and the Diverse Scram System (DSS). AMSAC was installed to comply with 10 CFR 50.62 requirements to improve the capability to mitigate an ATWS event. The DSS was installed to comply with 10 CFR 50.62 requirements to improve the capability to mitigate a primary system overpressure event, such as a Loss of Main Feedwater ATWS event. These systems share the same hardware and software and consist of two Programmable Logic Controllers (PLCs) for the logic control circuits and two Uninterruptible Power Sources. Inputs from the Control Oil System for both Main Feedwater Pump Turbines monitor the turbines for operation. Inputs from the Feedwater system monitor Feedwater pump discharge pressure. Isolated inputs from the Wide Range (WR) RCS Pressure sensors monitor the RCS for high pressure. The WR RCS Pressure signals are derived from the Reactor Vessel Level Indication System and are not associated with the RCS Pressure inputs to either RPS or ESPS. These inputs are wired to the PLCs and outputs to the final actuation devices are wired using interfacing relays. The PLCs are manufactured by Square D (Schneider Electric) and are SY/MAX Model 400 PLCs. The AMSAC and DSS are independent and diverse from the TXS Protection System and will continue to meet all requirements of 10 CFR 50.62. The PLCs use straight forward ladder logic programming software proprietary to the Square D product line. As required by 10 CFR 50.62, these systems are not affected by a common mode failure (hardware or software) or loss of power to the RPS/ESPS.

The following ONS AMSAC and DSS systems' attributes were evaluated to confirm diversity between them and the TXS based RPS/ESPS: design, human, equipment, software, functional, and signal.

The following are the major differences between the TXS and the ONS AMSAC and DSS:

- The design architectures are completely different.
- The design organization, management, designers, programmers, and testing engineers are different.
- The central processing unit (CPU) modules, input/output circuit boards and bus structure are different.
- The power supplies are different.
- The software operating systems are different.
- The software development tools are different.
- The software validation tools are different.
- The software algorithms, logic, program architecture, timing, and order of execution are different.
- The application programs are functionally diverse.

The design architecture diversity attribute is a very powerful type of diversity because this forces different configurations and functionality with different compilers, linkers, and other auxiliary programs to be used. The organizational diversity attribute also has a significant effect on diversity because management controls the resources applied and the corporate culture under which designers and programmers work. The ONS design for the ATWS systems, which consist of non-safety related digital equipment installed over 15 years ago, is clearly diverse and independent from the TXS platform. As such, the ONS ATWS design continues to meet the ATWS Rule with the replacement TXS based RPS/ESPS. If ATWS systems are modified in the future then the diversity arguments presented here will be applied and re-evaluated.

2.4.2 New Diverse Systems

Duke will install a Diverse Low Pressure Injection Actuation System (DLPIAS) concurrent with the RPS/ESPS digital upgrade to mitigate a postulated large break LOCA concurrent with a RPS/ESPS SWCMF that the D3 assessment concluded could not be mitigated by manual operator actions. The DLPIAS is described in more detail in Section 2.4.2.1 below.

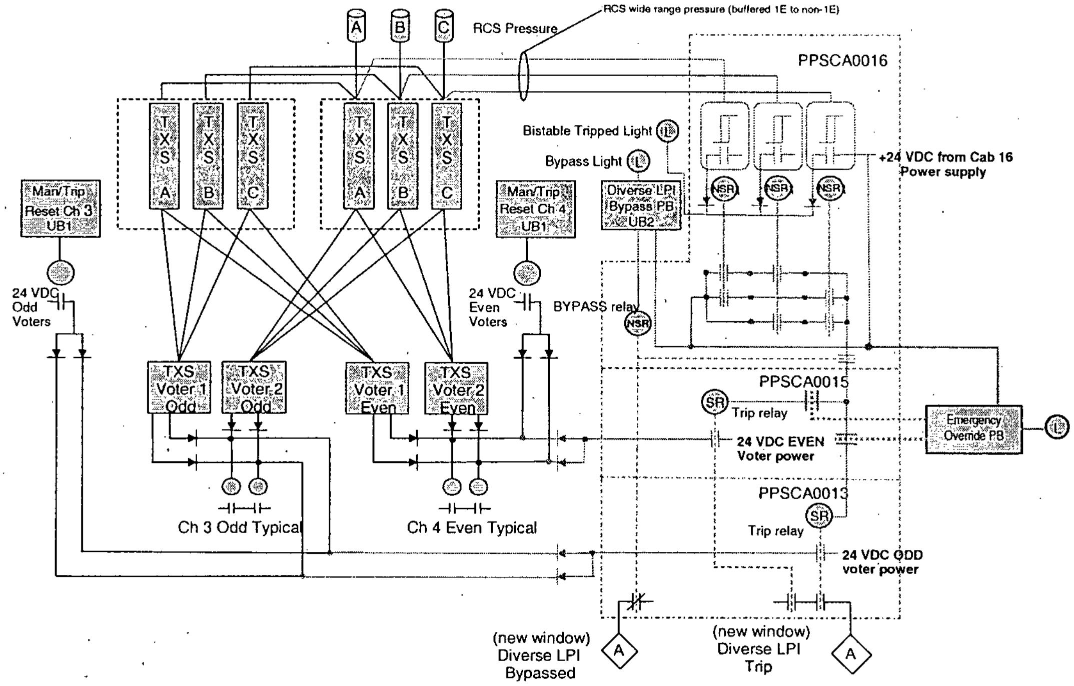
Additionally, during a telephone conversation between Duke (Ron Jones and Larry Nicholson) and NRC (Jim Dyer, et al) on April 6, 2006, Duke agreed to install a Diverse High Pressure Injection Actuation System (DHPIAS) concurrent with the RPS/ESPS digital upgrade to eliminate NRC concerns regarding one redundant set of ESPS channels sharing processors with RPS Channels A, B, and C. The DHPIAS is described in more detail in Section 2.4.2.2 below.

Duke will address functionality requirements for the DLPIAS and DHPIAS in the Oconee Selected Licensee Commitment (SLC) Manual. There are no interactions between these diverse actuation systems and the digital RPS/ESPS that would impact the operability of the RPS/ESPS.

2.4.2.1 Diverse Low Pressure Injection Actuation System

The DLPIAS will use conventional analog bistable trip units and two-out-of-three logic actuated on low RCS pressure. See Figure 2.4-1.

Figure 2.4-1 Typical Diverse LPI Actuation System



Compliance to Identified Design Requirements for DLPIAS:

The DLPIAS design requirements, which are based on existing non-safety related ATWS design requirements, are listed below. These requirements are considered appropriate because SRP HICB-19 (B.1) states diverse means may be a non-safety system, automatic, or manual if the system is of sufficient quality to perform the necessary function under the associated event conditions and within the required time. Where appropriate, a statement of how the DLPIAS will comply with these design requirements is made.

1. The system shall be of sufficient quality to perform the necessary function under the associated event conditions and within the required time (BTP HICB-19 B.1)

    - The proposed system will be a combination of safety and non-safety related components. The interface with the LPI actuation circuit and the Diverse LPI trip relay will be safety related. The bistable devices, two-out-of-three logic relays, annunciator circuits will be supplied as non-safety related and wired per ONS design requirements for separation and isolation. The power for the bistables and relay logic will be non-safety related.

- The quality of the components will be based on selection of known process electrical components that have proven reliability. The relays used for non-safety to safety isolation, the BYPASS ENABLE, and the EMERGENCY OVERRIDE switch selected will be the same as those supplied for the ES actuation circuits. The bistables will be of standard process industry commercial quality.

2. Automatic and manual actuation capability.

   - The DLPIAS will provide for automatic actuation of the ESPS Channel 3 and Channel 4 components. This includes actuation of the LPI System.
   - TXS ESPS manual initiation is accomplished by either the existing ES Trip/Reset buttons located on the main control board or actuation of the individual LPI component control switches/pushbuttons . The logic for the manual trip bypasses the TXS logic and allows the CRO to initiate ES actuation on a per channel basis.
   - DLPIAS initiation, automatic or manual, is downstream of the part of TXS ESPS subject to the SWCMF occurrence.
   - An EMERGENCY OVERRIDE pushbutton is provided to permit a redundant capability to prevent inadvertent operation of the LPI pumps. The LPI pumps must not be allowed to dead-head for an extended period of time to prevent pump damage. Both the BYPASS/ENABLE and EMERGENCY OVERRIDE pushbuttons are capable of preventing inadvertent initiation of DLPIAS.

3. Actuate LPI on low RCS pressure

   - DLPIAS will actuate only on low RCS pressure. The basis for this is the DLPIAS is intended to provide automatic LPI injection to cover the case of the large break LOCA in case the TXS has an SWCMF. The loss of RCS Pressure is the most appropriate indication that a large break LOCA has occurred.

4. Accuracy - Setpoints will be chosen that permit ESPS Actuation prior to DLPIAS actuation including instrumentation loop error.

   - The Setpoint of the DLPIAS will be chosen to allow the ESPS to actuate first. Because the DLPIAS is a specialized backup mitigation system for large break LOCA, the setpoint selected will be based on a suitable margin to permit ESPS the initial actuation opportunity and accuracies of the instrumentation string.

5. Minimize Inadvertent actuation - Use multi-channel logic in "an actuate to initiate" manner. For example; two-out-of-two channels required

   - The two-out-of-three logic will minimize inadvertent actuations. Actuation circuit relays are energized to actuate. Loss of power will not result in actuation.

6. Diverse hardware and software required - both analog and digital applications are acceptable provided diversity is maintained

   - Diverse hardware (bistables) is being provided. No Software is being provided for the DLPIAS.

7. Diverse sensors not required - Follow B&W Owners Group AMSAC/DSS guidance if using existing RPS/ESPS sensors

   - The RCS Pressure signals will be isolated from the safety related signals utilizing the TXS SNV1 signal isolators. Signal isolation is at the input signal conditioning front end of the TXS and does not make use of the analog to digital conversion hardware or software of the TXS computers.

8. Diverse power source to RPS/ESPS not required. Battery backup not required

   - The power will be from the same 120 VAC supplied to Channel E of the RPS. This power is non-safety related. The power is fed from the non-safety 120 VAC Inverter fed power panelboard KI.

9. Physical Separation not required

   - Physical separation will be maintained as it relates to IEEE Std 384-1992 separation criteria between safety related and non-safety related components for hardware located within the RPS/ESPS cabinets. The bistables and relays will be DIN Rail mounted components.

10. Electrical Separation is required. Electrical separation per ONS design requirements.

    - Electrical separation between safety related and non-safety related components will be maintained by the use of qualified isolators and relays.

11. Safety to non-safety isolation required. Isolation required to meet ONS criteria and guidance.

    - Physical separation will be maintained as it relates to IEEE Std 384-1992 separation between safety related and non-safety related components.

12. Equipment must be qualified for its intended location. All logic equipment shall be located in a mild environment.

    - All logic equipment associated with the DLPIAS system with the exception of the existing process system transmitters and cabling (which is environmentally qualified) is located in the Control Room and will be verified acceptable for the intended environment based on manufacturer product specification sheets.

13. Operating bypasses or maintenance bypasses

- Operating and maintenance bypassing is provided on the main control boards.
- Appropriate human factors evaluations performed along with operator training to prevent inadvertent bypassing.
- Administrative procedures are used to control and address Operating and Maintenance bypasses.
- The Diverse LPI BYPASS/ENABLE Switch will be used to bypass the DLPIAS system for both maintenance and operations. The procedures will require that the DLPIAS be bypassed on controlled shutdowns at the same time the ESPS LPI Bypass is initiated.
- The Diverse LPI EMERGENCY OVERRIDE switch will be used to override inadvertent initiation of the LPI pumps. This switch provides a redundant method of preventing inadvertent initiation of LPI to the BYPASS/ENABLE switch.

14. DLPIAS actions go to completion once initiated - reset controlled by procedure. Same as existing ESPS.

- The above criteria and requirements will be met. The Diverse LPI Bypass Switch will be administratively controlled and used to reset the actuated components once the DLPIAS actions have occurred and appropriate assessment of the initiating event permits recovery actions to commence.

15. Information readouts provided in Control Room for operator awareness and system monitoring shall be the same as during normal operation.

- Existing plant process system readouts (indications of RC system pressure, LPI pump status, LPSW pump status, LPI valve position, RPS, ESPS and other appropriate plant systems and equipment) will be utilized. No additional/new indicators will be provided.
- Control Room alarms are provided to alert operators to DLPIAS actuation.
- Control Room indications are provided to indicate the condition of the DLPIAS Bypass/Enable control switch and Emergency Override pushbutton.

16. Augmented quality program (NRC Generic Letter 85-06) is not required. Non-safety related commercial industrial products consistent with application are acceptable.

- There are no unique or special procurement requirements.

17. Software quality assurance

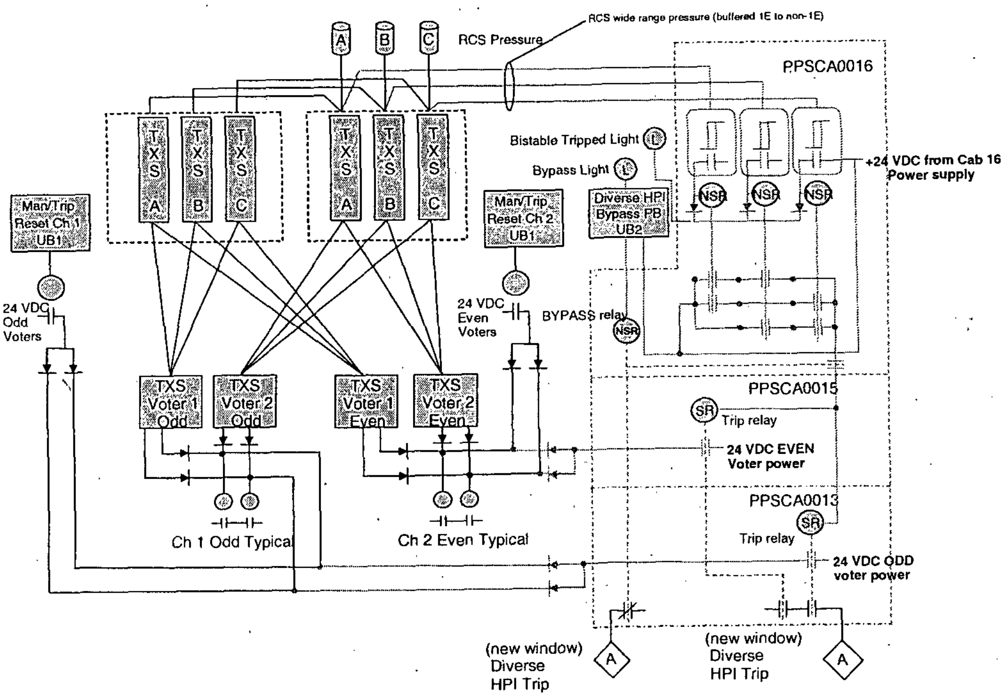
- The DLPIAS design does not require the use of any software.

2.4.2.2 Diverse High Pressure Injection Actuation System

On April 6, 2006, Duke agreed to install a DHPIAS concurrent with the RPS/ESPS digital upgrade to eliminate NRC concerns regarding one redundant set of ESPS channels sharing processors with RPS Channels A, B, and C. The DHPIAS is not required per the D3 analysis as described in Section 3.2.3 of this Enclosure.

The DHPIAS will use conventional analog bistable trip units and two-out-of-three relay logic actuated on low RCS pressure. See Figure 2.4-2.

Figure 2.4-2 Typical Diverse HPI Actuation System



Compliance to Identified Design Requirements for DHPIAS:

The DHPIAS design requirements, which are the same as those listed for DLPIAS, are listed below. Where appropriate, a statement of how the DHPIAS will comply with these design requirements is made.

1. The system shall be of sufficient quality to perform the necessary function under the associated event conditions and within the required time (BTP HICB-19 B.1)

   - The proposed system will be a combination of safety and non-safety related components. The interface with the HPI actuation circuit and the Diverse HPI Trip Relay will be safety related. The bistable devices, two-out-of-three logic relays, and annunciator circuits will be supplied as non-safety related and wired per ONS design requirements for separation and isolation. The power for the bistables and relay logic will be non-safety related.
   - The quality of the components will be based on selection of known process electrical components that have proven reliability. The relays used for non-safety to safety isolation, the BYPASS/ENABLE, and the EMERGENCY OVERRIDE switch selected will be the same as those supplied for the ES actuation circuits. The bistables will be of standard process industry commercial quality.

2. Automatic and manual actuation capability

   - The DHPIAS will provide for automatic actuation of the ESPS Channel 1 and Channel 2 components. This includes actuation of the HPI System.
   - TXS ESPS manual initiation is accomplished by either the existing ES Trip/Reset buttons located on the main control board or actuation of the individual HPI component control switches/pushbuttons. The logic for the manual trip bypasses the TXS logic and allows the Operator to initiate ES actuation on a per channel basis.
   - DHPIAS initiation, automatic or manual, is downstream of the part of TXS ESPS subject to the SWCMF occurrence.

3. Actuate HPI on low RCS pressure

   - DHPIAS will actuate only on low RCS pressure. The basis for this is the DHPIAS is intended to provide automatic HPI injection to cover various cases of the small break LOCA in case the ESPS has an SWCMF. The loss of RCS pressure is the most appropriate indication that a small break LOCA has occurred.

4. Accuracy - Setpoints will be chosen that permit ESPS Actuation prior to DHPIAS actuation including instrumentation loop error.

   - The DHPIAS setpoint will be chosen to allow the ESPS to actuate first. Because the DHPIAS is a specialized backup mitigation system for SBLOCA, the setpoint selected will be based on a suitable margin to permit ESPS the initial actuation opportunity and accuracies of the instrumentation string.

5. Minimize Inadvertent Actuation - Use multi-channel logic in "an actuate to initiate" manner. For example: two-out-of-two channels required

    - The two-out-of-three logic will minimize inadvertent actuations. Actuation circuit relays are energized to actuate. Loss of power will not result in actuation.

6. Diverse hardware and software required - both analog and digital applications are acceptable provided diversity is maintained

    - Diverse hardware (bistables) is being provided. No software is being provided for the DHPIAS.

7. Diverse sensors not required - Follow B&W Owners Group AMSAC/DSS guidance if using existing RPS/ESPS sensors.

    - The RCS pressure signals will be isolated from the safety related signals utilizing the TXS SNV1 signal isolators. Signal isolation is at the input signal conditioning front end of the TXS and does not make use of the analog to digital conversion hardware or software of the TXS computers.

8. Diverse power source to RPS/ESPS not required. Battery backup not required

    - The power will be from the same 120 VAC source supplied to Channel E of the RPS. This power is non-safety related. The power is fed from the non-safety 120 VAC Inverter fed power panelboard KI.

9. Physical separation not required

    - Physical separation will be maintained as it relates to IEEE Std 384-1992 separation criteria between safety related and non-safety related components for hardware located within the RPS/ESPS cabinets. The bistables and relays will be DIN Rail mounted components.

10. Electrical separation is required. Electrical separation per ONS design requirements.

    - Electrical separation between safety related and non-safety related components will be maintained by the use of qualified isolators and relays.

11. Safety to non-safety isolation required. Isolation required to meet ONS criteria and guidance.

    - Physical separation will be maintained as it relates to IEEE Std 384-1992 separation between safety related and non-safety related components.

12. Equipment must be qualified for its intended location. All logic equipment shall be located in a mild environment

    - All logic equipment associated with the DHPIAS system with the exception of the existing process system transmitters and cabling (which is environmentally qualified) is located in the Control Room and will be verified acceptable for the intended environment based on manufacturer product specification sheets.

13. Operating bypasses or maintenance bypasses

    - Operating and maintenance bypassing is provided on the main control boards
    - Appropriate human factors evaluations performed along with operator training to prevent inadvertent bypassing
    - Administrative procedures are used to control and address operating and maintenance bypasses
    - The Diverse HPI Bypass Switch will be used to bypass the DHPIAS system for both maintenance and operations. The procedures will require that the DHPIAS be bypassed on controlled shutdowns at the same time the TXS HPI Bypass is initiated for the ESPS.

14. DHPIAS actions go to completion once initiated - reset controlled by procedure. Same as existing ESPS

    - The above criteria and requirements will be met. The Diverse HPI Bypass Switch will be administratively controlled and used to reset the actuated components once the DHPIAS actions have occurred and appropriate assessment of the initiating event permits recovery actions to commence.

15. Information readouts provided in Control Room for operator awareness and system monitoring shall be the same as during normal operation.

    - Existing plant process system readouts (indications of RCS pressure, HPI pump status, HPI valve position, RPS, ESPS and other appropriate plant systems and equipment) will be utilized. No additional/new indicators will be provided.
    - Control room alarms are provided to alert operators to DHPIAS actuation.
    - Control Room alarms are provided to indicate the condition of the DHPIAS Bypass/Enable control switch.

16. Augmented quality program (NRC Generic Letter 85-06) is not required. Non-safety related commercial industrial products consistent with application are acceptable.

    - There are no unique or special procurement requirements.

17. Software quality assurance

- The DHPIAS design does not require the use of any software.

2.5 *Other Digital RPS/ESPS Related Components and Features*

2.5.1 Monitoring and Service Interface

The MSI provides the interface between the safety related systems (RPS, ESPS, ESPS Voters and ESPS Component Status) and the non-safety related TXS Gateway computer and TXS Service Unit. Electrical isolation between the safety related systems and non-safety related TXS Gateway computer and TXS Service Unit is provided by safety related fiber optic cable (refer to Figure 2.1-1 and Section 3.3.6 of this Enclosure). The MSI provides data isolation (refer to Section 3.4.6 of this Enclosure).

The MSI also provides an interface with RPS Channel E. The communications path within the MSI is divided, with four communication processors handling the communication data links to the safety related TXS processors and a separate communications processor handling communications via an Ethernet link to the TXS Service Unit and TXS Gateway computer.

Communications on the non-safety related side of the MSI is through a restricted access local area network (LAN) that connects the MSI, TXS Service Unit computer, and the TXS Gateway computer. The MSI is designed and programmed to only relay control and maintenance commands that originate from the Ethernet media access control (MAC) address assigned to the TXS Service Unit.

All MSI communications links are via safety related fiber optic cables, thereby assuring electrical isolation between the individual RPS and ESPS channels and the non-safety related components.

The MSI performs the following communications functions:

- Relay of control and maintenance commands from the TXS Service Unit to each of the safety related TXS processors.
- Relay of status information and control command responses from the safety related TXS processors back to the TXS Service Unit.

- Relay of computer point information from the safety related TXS processors to the TXS Gateway computer and from there to the plant OAC.

therefore, a safety related (class 1E) power supply is not required. Data communication independence is discussed in Section 3.4.6 of this Enclosure. On a loss of power, isolation between the safety related TXS processors, the non-safety related TXS Gateway computer, and the TXS Service Unit computer is assured.

2.5.2 TXS Gateway Computer

The TXS Gateway computer provides the communication interface between the digital RPS/ESPS and the OAC.

The TXS Gateway computer is a rack mountable high performance server, which acts as a TXS processor on one side and data acquisition system on the other side. The TXS Gateway is not located within the digital RPS/ESPS cabinets. It is located in the unit OAC computer room. The Gateway does not utilize TXS hardware components although it does run TXS proprietary software. The communication between the RPS/ESPS and OAC is accomplished in a manner such that no credible OAC fault or failure can adversely affect the ability of the RPS/ESPS to accomplish its safety functions when required.

2.5.3 TXS Service Unit

The TXS Service Unit allows authorized personnel to access all functions of the digital RPS/ESPS required to conduct tests for system commissioning as well as design changes, periodic testing and for monitoring the digital RPS/ESPS after installation in the plant. The TXS Service Unit serves the following functions:

- Monitoring the system state,
- Reading and acknowledging on line error and state messages,
- Modifying online parameters,
- Performing periodic tests,
- Error detection and fault diagnosis, and
- Central reloading of software after design changes.

The TXS Service Unit communicates with all TXS processors via the MSI. The TXS Service Unit is non-Class 1E. Effective 1E/non-1E isolation is provided using fiber optic data links.

Since the TXS Service Unit has direct access to the online system; multiple levels of protection against unauthorized use is employed. The description of these design features is considered by Duke to be sensitive information and to be withheld from public disclosure pursuant to 10 CFR 2.390. Duke submitted descriptions of the cyber security features of the RPS/ESPS that demonstrate that the applicable cyber security requirements have been met by letter dated January 30, 2008.

2.5.4 TXS Test Machine

The Test Machine is a portable unit that can be used for performing calibration checks and logic tests on TXS systems. It is not a device that is normally connected to the system. The Test Machine is operated by plain-text scripts, and output data can be logged to disk files for long- term storage of calibration results. For the Oconee RPS/ESPS project, it will be used to perform tests during the Factory Acceptance Test phase and potentially during Site Acceptance Test phase when field devices are not connected to the cabinets. It can also be used to facilitate tests during the initial installation of the RPS/ESPS cabinets into the plant. Once this initial testing is complete, periodic testing of the systems does not require use of the Test Machine. It will be available if needed for testing to support future design changes to the system.

The Test Machine consists of a roll-around cabinet with the necessary I/O and control modules. The I/O boards provide digital outputs, digital inputs, and analog inputs/outputs. Connections are made to the TXS system using prefabricated cables. These cables are connected to I/O connectors in the TXS cabinets. When the cable is inserted into the connector, all field signals are disconnected and signals from the Test Machine I/O modules are applied as inputs.

The Test Machine is considered Measuring and Test Equipment (M&TE). Therefore, the purchase, storage, software configuration management, and any needed calibrations of this equipment will be performed in accordance with the departmental directive for M&TE.

2.5.5 Graphical Service Monitor

The GSM provides a graphical user interface for working with the on-line system. The GSM is a client to the TXS Service Unit. The GSM formats and presents this data in a close-to-real-time manner. Note that the requests for data are a second priority for the RPS/ESPS. Therefore the data is provided only when the RPS/ESPS is not performing its safety function.

The GSM formats and presents the data to the TXS Service Unit. In addition to presenting data, the GSM can also change parameters in the online system and run tests.

The GSM acts as an interactive user-interface for the maintenance and servicing of the digital RPS/ESPS by Operations and Maintenance personnel. Menus and dialog masks enable system monitoring and test execution without requiring a detailed knowledge of the command language of the service monitor. Graphical input options are used in lieu of most of the commands. Visualization of states and events inside the digital RPS/ESPS is enabled by the GSM.

The functions for placing channel inputs into a Trip or Bypass state can be accomplished via the GSM screens. Testing of the digital RPS/ESPS output functions is also possible through the use of GSM dialogs. The GSM is also capable of verifying that the correct software is running on the digital RPS/ESPS.

The GSM will be used only by qualified personnel and controlled by approved procedures. Individuals from different organizations will have different privilege level based on job function. These procedures will allow qualified personnel to perform the following core functions:

- Monitoring the digital RPS/ESPS during operation,
- Modifying parameter settings (an example of this function is changing of the high flux trip setpoint from its full power setpoint to the shut down setpoint),
- Outputting signal values and signal states,
- Performing periodic tests,
- Detecting errors, and
- Diagnosing faults.

2.5.6 Lead/Lag Filters

The Oconee digital RPS/ESPS includes lead/lag filters in the signal processing stream for each analog input. The NRC SER for the TXS Topical Report (Reference 1) does not address lead/lag filters.

All of the lead/lag filter parameters are set in such a manner as to turn off the filter (i.e., pass through filter) with one exception. The only filters that will be switched on are the filters on the differential pressure input signals (used for calculating RCS Flow) received by the RPS for use in the Flux/Flow/Imbalance Trip #3. In the current analog system, the STAR modules receive these same differential pressure signals. The STAR modules currently contain a 594 milliseconds hardware filter on the flow inputs to address signal noise. The digital RPS will use software filters or a combination of hardware (SAA1) and software filter settings on these input signals with a time response delay not to exceed the 594 milliseconds filter delay as exists in the current system. In the current analog RPS, the old Bailey BY pressure transmitters were replaced with new Rosemount 1154 differential pressure transmitters. The 594 milliseconds filter was included in the STAR design in order to address process noise sensed by the new Rosemount 1154 Differential Pressure Transmitters. The inclusion of software filters on analog input signals is merely a proactive design to allow the system to be flexible and address future signal noise that may be encountered due to plant equipment changes (similar to the differential pressure signal noise encountered). These filters are set to operate in the Pass Through mode and will not affect the system response to plant conditions. This will be confirmed via SIVAT testing and FAT testing. The filters are designed into the system in order to allow the system to tolerate signal noise that might be caused by process system conditions.. The filter time constants are addressed and documented in an ONS calculation.

Extensive SIVAT testing is performed on the application software, including the parameters and functionality of the lead/lag filters. These filters were tested in several configurations, including the "Pass Through" configuration. Additional testing on these filters in the final, to-be-installed configuration will be performed during factory acceptance testing. This will include testing by injecting calibrated signals and verifying the accuracy received by the software and response time testing to ensure the system responses are within the allowed time.

The filters were designed and implemented in the proposed digital RPS/ESPS to give flexibility to the system in order to compensate for different signal noise characteristics that may be encountered during the life-cycle of the RPS/ESPS system. As stated above, the only currently known need for an activated filter is for the RCS differential pressure signals. The noise characteristics associated with the RCS differential pressure signals are documented in a Duke calculation. While this calculation is an example of signal noise characteristics that might be encountered, it is not representative of all types of signal noise that might be encountered by the digital RPS/ESPS system due to plant conditions.

Noise suppression before the A/D conversion will be implemented by the SAA1 card and low pass filtered with settings of 47, 94, and 188 milliseconds. Software filtering would only be needed if noise suppression requirements were outside these ranges, as is the case with the RCS differential pressure signals. The system response times are consistent with the existing system.

Should filter setting changes be necessary after installation of the digital RPS/ESPS, they will be controlled by the Oconee design change program to ensure that proper design and licensing reviews of the changes are performed. If a need arises for the filters to be switched on, filter response requirements would be developed to determine what type of filtering is necessary and settings of the SAA1 filter would be determined (as required). The parameter settings for the software system would be calculated, tested with SIVAT, and tested on the actual system before the system settings could be used. This would be performed by ONS personnel.

2.5.7 ESPS Variable Time Delay Function

The digital RPS/ESPS design includes a variable time delay function (0 to 15 minute range) on each output prior to ES device actuation. This is an enhancement to the existing ESPS capabilities. All time delays will be set at 0 to provide the same performance as the current ESPS. These settings will be controlled by approved plant procedures, and subsequent changes to the time delay settings will require a plant design change.

Should a time delay be needed in the future, this variable time delay function minimizes the scope of the design change needed to change load sequencing of ES equipment. Load sequence changes for ES equipment is not within the scope of the RPS/ESPS design change.

Oconee had previously recognized the need to increase the safety related Electrical Distribution System (EDS) bus and equipment terminal voltages at all voltage levels, when an accident occurs. A series of station design changes were implemented to improve the capabilities of the EDS to meet the required demand. These changes were implemented to improve the 600V and 208V motor control center (MCC) transient voltages and MOV terminal voltages by delaying Reactor Building Cooling Unit (RBCU) start until ES continuous-duty motors have started and ES MOVs have completed their stroke.

2.5.8 Power Distribution to RPS/ESPS Cabinets

Four independent class 1E battery backed 120 VAC power panels are used to supply power to the TXS RPS/ESPS channels.

- RPS Channel A, RCPPM Channel A, ESPS Channel A and the Odd Voters are fed from power panel KVIA.
- RPS Channel B, RCPPM Channel B, ESPS Channel B and the Even Voters are fed from power panel KVIB.
- RPS Channel C, RCPPM Channel C and ESPS Channel C are fed from power panel KVIC.
- RPS Channel D and RCPPM Channel D are fed from power panel KVID.

These 120 VAC power sources for the TXS RPS/ESPS are unchanged from those used to supply the current analog Bailey RPS and ESPS.

Power supplied to the cabinet which contains RPS Channel E, the MSI, DLPIAS, and DHPIAS is supplied from a battery backed non-1E 120 VAC power panel 1KI. This 120 VAC power source is unchanged from the source for the current analog Bailey RPS Channel E.

The Gamma-Metrics nuclear instrumentation equipment is removed from the Bailey RPS cabinets and then re-installed in the TXS RPS cabinets as part of this design change. No changes are made to the power sources for the Gamma-Metrics equipment.

The 120 VAC power circuits to the TXS cabinets are routed through breakers within the cabinets in addition to the breakers located at the power panel boards and are available for local isolation of power as needed. Within each TXS cabinet, the 120 VAC power is then supplied to redundant, auctioneered ± 24 VDC Absopulse power supplies. The Absopulse power supplies are used to power the TXS circuitry and the existing field devices such as transmitters and indicators.

The 120 VAC power to ESPS Odd Component Status Cabinet 17 is supplied from the same branch circuit used to power the Odd Voter Cabinets 12 and 13. No Absopulse power supply is located in cabinet 17 so 24 VDC power is fed from the Absopulse power supplies in the Odd Voter Cabinets to the Odd Component Status Cabinet.

The 120 VAC power to ESPS Even Component Status Cabinet 18 is supplied from the same branch circuit used to power the Even Voter Cabinets 14 and 15. No Absopulse power supply is located in cabinet 18 so 24 VDC power is fed from the Absopulse power supplies in the Even Voter Cabinets to the Even Component Status Cabinet.

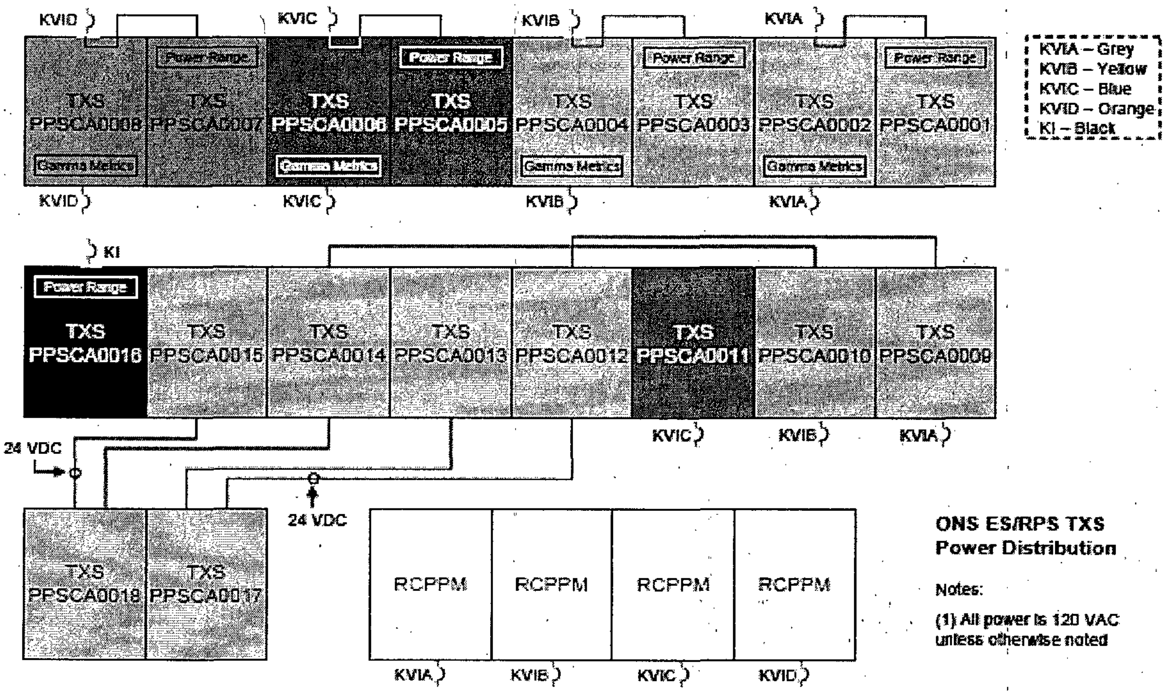
The RZ module indications associated with the Bailey ESPS system are presently powered from sources 208 VAC 1XS1 and 1XS2 MCCs via control power step-down transformers. The indications provided by the RZ modules are replaced with Status Panels as part of the TXS RPS/ESPS installation. The Status Panel indications are powered by 24 VDC from Absopulse power supplies.

Demonstration that the Absopulse power supply complies with EPRI TR-107330 as required by the NRC for a TXS installation (Reference 1, Section 2.1.2.4) is contained in Section 3.3.18 of this Enclosure. Section 3.3.18 also describes activities performed to ensure power source loading and breaker coordination for the RPS/ESPS systems is appropriate.

Power supplied for the TXS Gateway computer and the TXS Service Unit computer are supplied from separate non-1E battery backed 120VAC power panels.

Power to the specific cabinets is reflected in Figure 2.5-1.

Figure 2.5-1 Typical TXS Power Distribution



Note: Arrangement reflects the plan view of the cabinets for ONS Unit 1 Control Room.

2.6 *Overview of RPS/ESPS Cabinets, Location and Layout*

The digital RPS/ESPS will be installed in eighteen cabinets located in the ONS Control Rooms. The cabinet designations, contents, and power sources are listed below.

Table 2-2 RPS/ESPS Cabinets, Location and Layout

ONS Unit #	Cabinet Designation	Functions Performed in these Cabinets	Cabinet Power Source
1/2/3	PPSCA0001	RPS Channel A, ESPS Channel A1	Power Panel KVIA
1/2/3	PPSCA0002	RPS Channel A, ESPS Channel A1	Power Panel KVIA
1/2/3	PPSCA0003	RPS Channel B, ESPS Channel B1	Power Panel KVIB
1/2/3	PPSCA0004	RPS Channel B, ESPS Channel B1	Power Panel KVIB
1/2/3	PPSCA0005	RPS Channel C, ESPS Channel C1	Power Panel KVIC
1/2/3	PPSCA0006	RPS Channel C, ESPS Channel C1	Power Panel KVIC
1/2/3	PPSCA0007	RPS Channel D	Power Panel KVID
1/2/3	PPSCA0008	RPS Channel D	Power Panel KVID
1/2/3	PPSCA0009	ESPS Channel A2	Power Panel KVIA
1/2/3	PPSCA00010	ESPS Channel B2	Power Panel KVIB
1/2/3	PPSCA00011	ESPS Channel C2	Power Panel KVIC
1/2/3	PPSCA00012	ESPS Odd Voter 1	Power Panel KVIA
1/2/3	PPSCA00013	ESPS Odd Voter 2	Power Panel KVIA
1/2/3	PPSCA00014	ESPS Even Voter 1	Power Panel KVIB
1/2/3	PPSCA00015	ESPS Even Voter 2	Power Panel KVIB
1/2/3	PPSCA00016	RPS Channel E, TXS MSI, DLPIAS and DHPIAS	Power Panel KI
1/2/3	PPSCA00017	ESPS Odd Component Status	Power Panel KVIA
1/2/3	PPSCA00018	ESPS Even Component Status	Power Panel KVIB

2.7 Differences Between Topical Report TXS and ONS TXS

The ONS application of the TXS system includes changes to the TXS that were made to take advantage of advancements in technology and increased processing power that have occurred since the TXS platform was approved by NRC SER (Reference 1) dated on May 5, 2000.

2.7.1 Hardware Changes

Because of these advancements, the Oconee TXS RPS/ESPS includes some components that are different than those previously reviewed and approved in the TXS SER (Reference 1). Table 2-3 provides a summary and discussion of changes made to the TXS hardware.

2.7.2 Software Changes

2.7.3 TXS Development Procedure Changes

A summary of changes to the procedures used for TXS development is presented in Table 2-5.

Table 2-3 Summary of TXS Hardware Changes Since TXS SER Issued

Table 2-3 Summary of TXS Hardware Changes Since TXS SER Issued (continued)

Table 2-3 Summary of TXS Hardware Changes Since TXS SER Issued (continued)

Table 2-3 Summary of TXS Hardware Changes Since TXS SER Issued (continued)

Table 2-3 Summary of TXS Hardware Changes Since TXS SER Issued (continued)

Table 2-4 Summary of TXS Software Changes Since TXS SER Issued

Table 2-4 Summary of TXS Software Changes Since TXS SER Issued (continued)

Table 2-4 Summary of TXS Software Changes Since TXS SER Issued (continued)

Table 2-4 Summary of TXS Software Changes Since TXS SER Issued (continued)

Table 2-4 Summary of TXS Software Changes Since TXS SER Issued (continued)

Table 2-5 Summary of TXS Development Procedure Changes Since TXS SER Issued

Table 2-5 Summary of TXS Development Procedure Changes Since TXS SER Issued (continued)

3. Technical Evaluation

3.1 Introduction

This Chapter provides information consistent with RG 1.206, Section C.I.7, Instrumentation and Controls, guidelines.

Specifically, Section 3.2, Digital Instrumentation and Control Systems General Description, includes information on the qualification of the digital system, protection with respect to common-cause failure, and functional requirements of IEEE Std 603 and the General Design Criteria (GDC). Section 3.2 addresses the first four topics (design criteria, instrumentation and control (I&C) design, defense-in-depth and diversity (D3), and functional requirements and commitments) of Appendix C.I.7-A to RG 1.206. The last three topics (life-cycle process planning, life-cycle process requirements, and software life-cycle requirements) are addressed in Section 3.4.3 of this Enclosure, which provides information consistent with Standard Review Plan (SRP) Branch Technical Position (BTP) 7-14 guidelines.

The information included in Section 3.3, Conformance with IEEE Std 603-1998, describes how the ONS design for the new digital RPS/ESPS complies with IEEE Std 603-1998 by addressing the safety system design basis listed in RG 1.206 Appendix C.I.7-B. The design basis items listed in the RG are consistent with the safety system criterion listed in IEEE Std 603-1998, Clauses 5 through 7. For completeness, Section 3.3 also addresses the power source requirements of Clause 8 of IEEE Std 603-1998.

The information included in Section 3.4, Conformance with IEEE Std 7-4.3.2-2003, explains how the design for the new digital RPS/ESPS complies with IEEE Std 7-4.3.2-2003 by addressing the safety system design basis listed in RG 1.206, Appendix C.I.7-C. The design basis items listed in the RG are consistent with the safety system criterion listed in Clause 5 of the IEEE Std 7-4.3.2-2003.

The information provided in Sections 3.3 and 3.4 is consistent with that identified in NRC review guidelines for evaluation of conformance to IEEE Std 603-1998 and IEEE Std 7-4.3.2-2003 contained in SRP Appendix 7.1-C and Appendix 7.1-D, respectively. In those cases where the information provided in Section 3.3 and 3.4 are the same, reference is made to the appropriate section and the information is only provided once.

10 CFR 50.55a(h) requires that Oconee design of protection systems comply with IEEE Std 279 or IEEE 603-1991. However, in this LAR, Duke addresses IEEE 603-1998. The purpose of the revision from IEEE Std 603-1991 to 1998 was to clarify the application of this standard to computer-based safety systems and to

advanced nuclear power generating station designs. The 1998 revision provided an informational annex for the treatment of electromagnetic interference (EMI) and radio-frequency interference (RFI), clarifies definitions (e.g., Class 1E), and updates references. IEEE Std 7-4.3.2-1993 provides additional guidance on applying the safety system criterion specified by this standard for the use of computers as components in safety systems. Duke considers the 1998 revision to IEEE Std 603 more appropriate for referencing since it provided additional criteria and guidance with respect to the application of the standard to computer-based safety systems. Since the 1998 revision to IEEE Std 603 does not change any IEEE Std 603-1991 requirements, Duke has evaluated the digital RPS/ESPS for compliance to IEEE Std 603-1998.

Section 3.5 provides details associated with pre-installation, installation, and post-installation testing performed or planned.

Section 3.6 addresses operations, maintenance, and support functions.

Section 3.7 provides a summary of the results of the Failure Modes and Effects Analysis.

Section 3.8 addresses cyber security considerations for the new system. Details associated with the cyber security measures taken for the digital upgrade were provided separately by letter dated January 30, 2008, due to the sensitive nature of the information.

3.2 Digital Instrumentation and Control Systems General Description

This section includes information on the qualification of the digital system, protection with respect to common-cause failure, and functional requirements of IEEE Std 603-1998 and the GDC. The subsections below address the first four topics (design criteria, I&C design, defense in depth and diversity, and functional requirements and commitments) of RG 1.206 Appendix C.I.7-A (page A-1). The last three topics (life-cycle process planning, life-cycle process requirements, and software life-cycle requirements) are addressed in Section 3.4.3 of this Enclosure, which provides information consistent with SRP BTP 7-14 guidelines.

3.2.1 Design Criteria

RG 1.206, Appendix C.I.7-A states the following topic shall be addressed:

"(1) The design criteria to be applied to the proposed system."

The design criteria for the generic TXS system, the digital RPS/ESPS, and ancillary equipment associated with the digital RPS/ESPS are provided below.

3.2.1.1 Generic TXS Design Criteria

The TXS is a digital I&C system designed to be used in safety-related I&C applications in nuclear power plants as replacements for or upgrades to analog I&C systems. Typical applications include the reactor protection functions and the engineered safety features (ESF) functions. The TXS Topical Report describes the TXS hardware and software design, qualification testing, and application capabilities.

The safety philosophy of IEEE Std 279 and IEEE Std 603 was the basis of the first nuclear power plants in Germany and the design criteria are very similar to those of current German Safety Standards (KTA). KTA 3501 covers the requirements of IEEE Std 279, IEEE Std 603, IEEE Std 338, IEEE Std 379, and IEEE Std 384, while KTA 3503 covers the requirements of IEEE Std 323 and IEEE Std 344. As in KTA 3501, the requirements in IEEE Std 279, IEEE Std 379, IEEE Std 384 and IEEE Std 603 address the application-specific design of a safety system. These standards influence the development and the type-tests of hardware and software components in that the standards set forth the required features of these components. Therefore these standards play an important role in the concept review and in the application-specific qualification.

The NRC identified the following 10 CFR, Appendix A, GDC as applicable to the review of the generic TXS (Reference 1):

- GDC 1 – quality standards and records
- GDC 4 – environmental and missile design bases
- GDC 13 – instrumentation and control
- GDC 20 – protection system functions
- GDC 21 - protection system reliability and testability
- GDC 22 - protection system independence
- GDC 23 - protection system failure modes
- GDC 24 – separation of protection and control systems

Additionally, in the TXS Safety Evaluation Report (SER)(Reference 1), the NRC identified 10 CFR 50.55a(h) as applicable, which requires IEEE Std 603-1991 to be met. IEEE Std 603-1991 addresses both system level design issues and quality criteria for qualifying devices. RG 1.152, Revision 2, indicates that IEEE Std 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std 603-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations." Duke considers the 1998 revision to IEEE Std 603 more appropriate for referencing since it clarifies the application of the standard to computer-based safety system. Since the 1998 revision to IEEE Std 603 does not change any IEEE Std 603-1991 requirements, Duke has evaluated the digital RPS/ESPS for compliance to IEEE Std 603-1998.

The NRC SER for the TXS (Reference 1) concluded that the design of the TXS safety systems meets the relevant requirements of GDC 1, 2, 4, 13, 19-25, and 29, and 10 CFR 50.34(f), 10 CFR 50.55a(a)(l), and 10 CFR 50.55a(h), and is, therefore, acceptable." It also indicates that the TXS system is acceptable for use in development, installation, and operation of safety-related systems in nuclear power plants, subject to 17 plant specific action items.

3.2.1.2 Duke Design Criteria

ONS protection systems were originally designed to meet the requirements of IEEE Std 279-1968, "Proposed IEEE Criteria for Nuclear Power Plant Protection Systems." In some cases, the UFSAR now references the approved standard IEEE Std-279-1971. IEEE Std 279-1971 was used as the required design criteria and IEEE Std 603 was used for guidance only unless otherwise specified for the existing plant equipment. The new digital RPS/ESPS equipment is required to conform with both IEEE Std 279-1971 and IEEE Std 603-1991. RG 1.152, Revision 2, indicates that IEEE Std 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std 603-1998, "Standard Criteria for Safety Systems for Nuclear Power Generating Stations." Duke considers the 1998 revision to IEEE Std 603 more appropriate for referencing since it clarifies the application of the standard to computer-based safety system. Since the 1998 revision to IEEE Std 603 does not change any IEEE Std 603-1991 requirements, Duke has evaluated the digital RPS/ESPS for compliance to IEEE Std 603-1998.

The plant design criteria (PDC) for ONS were developed in consideration of the seventy GDC for Nuclear Power Plant Construction Permits proposed by the Atomic Energy Commission in a proposed rulemaking published for 10 CFR Part 50 in the Federal Register of July 11, 1967. As such, the ONS design criteria do not directly correlate to the current GDC.

The following ONS plant design criteria (PDC) were specified in the RPS replacement project specification (refer to Item 38 in Table 1-2 of this Enclosure) for the new system:

- PDC 1 - Quality Standards,
- PDC 2 - Performance Standards,
- PDC 3 – Fire Protection,
- PDC 4 - Sharing of Systems,
- PDC 5 - Records Requirements,
- PDC 6 - Reactor Core Design,
- PDC 7 - Suppression of Power Oscillations,
- PDC 11 - Control Room,
- PDC 12 - Instrumentation and Control Systems,
- PDC 14 - Core Protection Systems,
- PDC 19 - Protection Systems Reliability,
- PDC 20 - Protection Systems Redundancy and Independence,
- PDC 21 - Single Failure Definition,
- PDC 22 - Separation of Protection and Control Instrumentation Systems,
- PDC 23 - Protection Against Multiple Disability for Protection Systems,
- PDC 24 - Emergency Power for Protection Systems,
- PDC 25 - Demonstration of Functional Operability of Protection Systems,
- PDC 26 - Protection Systems Fail-Safe Design,
- PDC 28 - Reactivity Hot Shutdown Capability,
- PDC 29 - Reactivity Shutdown Capability,
- PDC 31 - Reactivity Control Systems Malfunction, and
- PDC 40 – Missile Protection.

The following ONS PDC were specified in the ESPS replacement project specification (refer to Item 37 in Table 1-2 of this Enclosure) for the new system:

- PDC 1 - Quality Standards,
- PDC 2 - Performance Standards,
- PDC 3 – Fire Protections,
- PDC 4 - Sharing of Systems,
- PDC 5 - Records Requirements,
- PDC 11 - Control Room,
- PDC 12 - Instrumentation and Control Systems,
- PDC 14 - Core Protection Systems,
- PDC 15 - Engineered Safety Features Protection Systems,
- PDC 19 - Protection Systems Reliability,
- PDC 20 - Protection Systems Redundancy and Independence,
- PDC 21 - Single Failure Definition,

- PDC 22 - Separation of Protection and Control Instrument Systems,
- PDC 23 - Protection Against Multiple Disability for Protection Systems,
- PDC 24 - Emergency Power for Protection Systems,
- PDC 25 - Demonstration of Functional Operability of Protection Systems,
- PDC 26 - Protection Systems Fail-Safe Design,
- PDC 37 - Engineered Safety Features Basis for Design,
- PDC 38 - Reliability and Testability of Engineered Safety Features,
- PDC 39 – Emergency Power for Engineered Safety Features,
- PDC 40 – Missile Protection,
- PDC 41 - Engineered Safety Features Performance Capability,
- PDC 42 – Engineered Safety Features Components Capability,
- PDC 43 – Accident Aggravation Prevention,
- PDC 57 – Provisions for Testing of Isolation Valves, and
- PDC 61 – Testing of Operational Sequence of Containment Pressure Reducing Systems.

The existing RPS and ESPS field sensors and cabling are not being replaced as a part of this design change.

3.2.1.3 Design Criteria for Digital RPS/ESPS Ancillary Equipment

AREVA NP designed, manufactured, and qualified the NI Equipment and Reactor Coolant Pump Power Monitor (RCPPM) mounting plate assemblies. The Detector Power Supply, ESPS Status Panels (light emitting diode (LED) lamp boxes), and RCPPM components were procured commercial grade and dedicated by AREVA NP. The RCPPM components are all mounted on a mounting plate that will be installed in the existing RCPPM cabinets.

New and replacement control switches and indicating light assemblies have been purchased from qualified vendors for use in safety related applications.

The devices and assemblies above will be qualified for Class 1E protection system use in accordance with IEEE Std 323-1983 and IEEE Std 344-1987 to envelope the ONS seismic parameters and Control Room and Cable Spreading Room mild environment parameters described in Section 3.3.4 of this enclosure.

This is not an all inclusive list of ancillary equipment being installed as part of this design change.

3.2.1.4 Conclusion

The design criteria for the RPS/ESPS digital upgrade bound the design criteria applied to the TXS. The NRC SER for TXS (Reference 1) concluded that the design of the TXS safety systems meets the relevant requirements of GDC 1, 2, 4, 13, 19-25, and 29, and 10 CFR 50.55a(a)(l), and 10 CFR 50.55a(h), and is, therefore, acceptable. The NRC SER states that the TXS system is acceptable for use in development, installation, and operation of safety-related systems in nuclear power plants, subject to 17 plant specific action items (PSAIs). The applicable PSAIs are addressed in this LAR in various sections as indicated in Table 1-1.

3.2.2 Identification of the I & C Design

> *RG 1.206, Appendix C.I.7-A states the following topic shall be addressed:*
>
> *"(2)* The I&C design as applicable to the FSAR Sections 7.2 through 7.9.*"*

The I&C design for the digital RPS/ESPS is described in subsections 3.2.2.1 and 3.2.2.2 below.

3.2.2.1 Reactor Protective System

3.2.2.1.1 Design Bases

The RPS is designed to sense plant parameters and trip the reactor in the event of abnormal plant parameter values.

3.2.2.1.2 System Design

The RPS is a four channel system which monitors plant parameters related to safe operation and trips the reactor to protect the reactor core against fuel rod cladding damage. The RPS also protects against reactor coolant system damage caused by high reactor coolant system pressure by limiting the energy input into the system through reactor trip action. Two tripped-channels are required for tripping of the reactor.

A minimum of three functional channels are required to perform the RPS safety function. The RPS can be configured into a two-out-of-three channels required for reactor trip system by placing one of the four channels into a bypassed condition. If an additional channel must be placed in bypass, then the one channel already in "bypass" must be placed in the "tripped" condition resulting in a one-out-of-two channels (one tripped, one bypassed, two functional) needed to cause a reactor trip.

Refer to Section 2.2 of this Enclosure for a detailed description of the RPS.

3.2.2.1.3 System Evaluation

The RPS is a four channel system in which the four protective channels are brought together in four identical two-out-of-four relay logic networks.

Each of the relay logic networks controls the opening of a control rod drive breaker. Thus a trip in any two-out-of-four protective channels will initiate a trip of all the breakers.

In evaluating system performance, it is arbitrarily assumed that the "failure" can either prevent a trip from occurring or can initiate trip action. A trip of any two-out-of-four protective channels initiates a trip of all four relay logic networks. That is, any two channels tripping actuate the relay logic networks in all four channels. In the event of a single failure of one of the four relays in the relay logic network concurrent with a Design Basis Event (DBE), sufficient redundancy remains with the other three RPS channels to ensure a reactor trip occurs. In the event of a single failure of one of four RPS channel's actuation logic concurrent with a DBE, sufficient redundancy remains with the other three RPS channels to ensure a reactor trip occurs.

Each of the redundant four RPS channel sensor inputs operate in a two-out-of-four configuration internal to each channel. The internal arrangement of any channel permits a single failure of an input device, yet retains the ability to provide a channel trip on the remaining two-out-of-three input signals. Signals are electrically isolated and shared between channels via fiber-optic inter-connection (See Figure 2.1-2 and Section 3.4.6 of this Enclosure for detailed discussion of the 2.MIN/2.MAX feature). Use of fiber-optic inter-channel communication, dual port random access memory (RAM) hardware, and appropriate software data configuration assure independence and single failure design criteria are met.

With the RPS configured in this fashion, tolerance of single input failures, single channel failures and single output failures is assured.

3.2.2.2 Engineered Safeguards Protective System

3.2.2.2.1 Design Bases

The ESPS monitors plant parameters to detect the failure of the RCS and initiate operation of the HPI and LPI when required. The ESPS also initiates RB Isolation, RB Cooling and RB Spray when required. In addition, the ESPS signals are used to start the Emergency Power Systems and initiate transfer to the standby power sources when required. Additional discussion of the Emergency Power System arrangements and design can be found in UFSAR Section 8.3.1.1.3.

3.2.2.2.2 System Design

The ESPS is a dual - three channel logic system which monitors plant parameters related to safe operation and actuates the components and systems identified in Section 3.2.2.2.1. The ESPS safety function is to prevent or minimize the severity of an accident or to mitigate the consequences of an accident. During accident conditions, when reactor coolant is lost, or in the event of secondary system pipe breaks, the ESPS and the down stream systems act to initiate emergency cooling, assure structural integrity of the core, maintain the integrity of the RB and to collect and filter potential RB penetration leakage.

As described in Section 2.3 of this Enclosure, the ESPS actuation logic arrangement is a dual three channel system arranged in two redundant subsystems. Input sensors are shared between the two subsystems. Analog inputs are brought to the primary system and are then buffered and isolated and an analog signal is then provided to the backup system for its use. The channels are isolated between subsystems to allow work to be performed on one subsystem without impacting the other subsystem.

The input sensors (from the sensor through the field cable which terminates at the input to the ESPS cabinet) were not affected by the upgrade to the ESPS. The ESPS signal processing and logic hardware were replaced. The ESPS output logic arrangement consists of eight actuation channels. The eight output actuation channels are further divided into both Odd and Even channels. Channels 1, 3, 5 and 7 are Odd channels and Channels 2, 4, 6 and 8 are Even channels. Either ESPS actuation logic subsystem and corresponding Odd or Even actuation logic channel sets are fully capable of performing the ESPS design function.

Refer to Section 2.3 of this Enclosure for a detailed description of the ESPS.

3.2.2.2.3 System Evaluation

In evaluating ESPS performance, it is arbitrarily assumed that the "failure" can either prevent an ESPS actuation from occurring or can initiate unnecessary ESPS actuation. An actuation of any two-out-of-three input channels in either redundant subsystem will initiate both the Odd and Even Voters associated with the specific subsystem. That is, any two channel's input sensors will actuate all three channels of the subsystem. In the event of a single failure in one of the channels of a subsystem, concurrent with a DBE, sufficient redundancy remains with the other two ESPS actuation channels of the affected subsystem and with the unaffected three ESPS channels of the unaffected subsystem to ensure actuation of the Odd and Even Voters occurs. Actuation of these Voters will in turn actuate Emergency Core Cooling Systems (ECCS) and components as well as emergency power if required. In the event of a single failure of one of the three ESPS channel's Voter actuation logic (either Odd or Even) concurrent with a DBE, sufficient redundancy remains with the other unaffected Voter of the affected subsystem and both the Odd and Even Voter of the unaffected subsystem. Figure 2.1-2 provides a pictorial representation of the features described above.

The redundant three channels in each subsystem of ESPS (six channels total), the redundant Odd and Even Voter sets and the alignment of Odd and Even ECCS components ensure that the ESPS will perform to meet its required safety functions. The internal arrangement of any of the redundant three channels is designed to permit a single failure of an input device and retain the ability to provide a channel trip on the remaining two-out-of-two input signals. The sharing of sensor inputs between the two ESPS subsystems is via copper wire interface. The sharing of input signals between redundant channels of one subsystem is via fiber optic cables. The fiber optic cables provide the electrical isolation between channels (See Figure 2.1-2 and Section 3.4.6 for detailed discussion of the 2.MIN/2.MAX feature). Use of fiber optic inter-channel communication, dual port RAM hardware, and appropriate software data configuration assure independence and single failure design criteria are met.

With the ESPS configured in this fashion, tolerance of single input failures, single channel failures and single Voter failures is assured.

3.2.3 Defense-in-Depth and Diversity

> *RG 1.206, Appendix C.I.7-A states the following topic shall be addressed:*
>
> "*(3)* Defense in depth and diversity—For applications that involve a reactor trip system or an ESF actuation system, the applicant should address the combined ability of the I&C systems to cope with common cause failure. The application should confirm that defense-in-depth and diversity design features conform to the guidance of NUREG 0800, Chapter 7, BTP 7-19."

3.2.3.1 Background

Duke submitted a D3 assessment for the RPS/ESPS digital upgrade by letter dated March 20, 2003 (Reference 5). Duke provided additional information on the D3 assessment by letters dated September 23, 2004, October 6 and October 26, 2005, December 14, 2005, and April 26, 2006. Based on this information NRC made the preliminary conclusion that there is adequate D3 in the proposed design of the RPS/ESPS, including manual operator action and the DLPIAS, to meet the acceptance criteria of BTP HICB-19 and that the D3 analysis was acceptable.

Subsequently, by letter dated May 18, 2006, the NRC advised that the D3 analysis would be addressed in connection with the NRC's future SER on the license amendment request for the digital upgrade of the RPS/ESPS. During a May 18, 2006, telephone call between the NRC (M. Mayfield, C. Haney) and Duke (L. Nicholson), the NRC advised that this decision was for administrative reasons only and that they did not intend to re-review the D3 assessment. By letter dated July 20, 2006, Duke confirmed its understanding that no further D3 assessment would be required by Duke and no further review would be required by the NRC related to D3 assessment.

The documents listed above are applicable to this LAR and are incorporated by reference in accordance with 10 CFR 50.32.

3.2.3.2 Summary of ONS D3 Assessment

Duke used the methodology and acceptance criteria for D3 assessments established by the NRC for operating nuclear plants that implement digital based protection systems. This methodology and acceptance criteria are provided in SRP, Chapter 7, Appendix 7A, BTP HICB-19, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Rev. 4, June 1997.

With an integrated digital protection system, there is a concern that a software common mode failure (SWCMF) of redundant elements within the digital protection system could propagate in such a fashion that the acceptance criteria for the ONS UFSAR transient and accident analyses would not be met. This ONS D3 assessment provides the methodology used by Duke to address defense-in-depth and diversity and documents the results of an engineering study that examines the capability of the plant to withstand a hypothetical SWCMF that results in a total failure of the digital RPS/ESPS. The methodology assumes a complete loss of RPS/ESPS and re-analyzes the thermal-hydraulic response, the core and fuel response, and the offsite and control room dose consequences for a spectrum of transients and accidents from UFSAR Chapters 10 and 15. The ONS D3 assessment demonstrates that Duke's methodology to address D3 is consistent with NRC guidance and best estimate acceptance criteria for this issue. The acceptance criteria were met for all transients and accidents with the exception of the Large Break Loss of Coolant Accident (LBLOCA). For the LBLOCA, the failure of the automatic ESPS actuation of the LPI System causes an unacceptable delay in the delivery of the emergency core coolant. As a result, Duke proposed to add a diverse LPI actuation system to mitigate this beyond DBE. The design of this system is described in Section 2.4 of this Enclosure.

At the request of NRC staff, Duke performed sensitivity analyses to demonstrate that additional time is available for operators to manually initiate HPI, Reactor Building Cooling (RBC) and Reactor Building Spray (RBS) Systems during a Small Break Loss of Coolant Accident (SBLOCA) and a Control Rod Ejection (CRE) accident and still meet the acceptance criteria of the ONS D3 assessment. The sensitivity analyses demonstrated that at least 8 minutes are available for the operator to initiate HPI and at least 1 hour is available for the operator to initiate RBC and RBS Systems (compared to the 5 minutes for HPI and 8 minutes for RBC and RBS Systems assumed in the D3 assessment). These sensitivity analyses also bound the LBLOCA, which credits manual initiation of these systems.

To address continued NRC concerns regarding the time available for an operator to initiate HPI during a SBLOCA, Duke agreed to install a DHPIAS to provide additional defense in depth and address the issue of the RPS/ESPS common processor (i.e., RPS channels A, B, and C sharing a processor with ESPS channels A, B, and C). The design of this system is described in Section 2.4 of this Enclosure.

3.2.3.3 Benefits of DLPIAS and DHPIAS

Duke performed a qualitative assessment of the benefits of installing a DLPIAS and DHPIAS to mitigate either a large break or a small break LOCA occurring concurrent with a SWCMF of RPS/ESPS.

The D3 analyses evaluated the ability to mitigate a variety of transients following a SWCMF of both RPS and ESPS to function. These analyses determined that a diverse LPI actuation is required to mitigate a large break LOCA up to and including a double-ended guillotine break of the RCS piping. Although the D3 assessment concluded a diverse HPI actuation is not needed to mitigate a small break LOCA (based on crediting operator action to initiate HPI and trip the reactor), Duke committed to install a DHPIAS to address NRC Staff concerns regarding the time assumed for operator actions. The following evaluation examines the basis for the expected operator action, the consequences associated with failure of timely operator action, and the benefits obtained by the installation of a DLPIAS and DHPIAS.

3.2.3.3.1 Basis for Assumed Operator Action Response Times

The primary basis for the D3 analyses assumption that the operator can initiate HPI in 5 minutes is the expected response to a loss of subcooling margin (LOSCM). The subcooling indications are not affected by the RPS/ESPS design change. A postulated SWCMF of the RPS/ESPS logic will not affect the subcooling indications following installation of the digital RPS/ESPS. These control room indications will respond as they do currently.

The current licensing basis Chapter 15 LOCA analyses assume that the RCPs would be stopped within 2 minutes of a LOSCM for scenarios where offsite power is maintained. This assumption is based upon analyses required as a result of NUREG-0737 and licensing actions to evaluate an automatic RCP trip. The Oconee Emergency Operating Procedures (EOP) requires that the reactor and turbine be tripped prior to stopping the RCPs. One of the procedure steps for responding to a LOSCM is to initiate HPI flow. Therefore, given that this evolution is a time critical action that the operators currently train to meet, the operator would be expected to meet the action time assumed in the D3 analyses.

3.2.3.3.2 Consequences of Missed Operator Action

The small break LOCA transient sequence postulated by the NRC request to consider a minimum 30-minute operator action time is considered below. This section is entitled "Missed Operator Action" as the scenario is the same as what would be expected if the current licensing basis assumptions are not met. The initial conditions are assumed to be nominal hot full power conditions. Consistent with the D3 analyses a nominal system performance and best estimate boundary conditions are also assumed. No single failures are postulated. Given that the following discussion is qualitative, no specific break size or location is assumed, and some variability in actual results is expected for the possible range of breaks.

In the early stages of a small break LOCA concurrent with an RPS/ESPS SWCMF (or common mode failure ATWS) and no DLPIAS or DHPIAS installed, the RCS would remain near full power operation. The RCS inventory would be depleted by the small break LOCA, and normal charging systems would attempt to compensate for the decrease in pressurizer level. A second HPI pump would be expected to start due to low RCP seal flow, potentially alerting the operator to the upset. (Note: Each unit has three HPI pumps, each capable of supplying the normal charging flow from the letdown storage tank. One is normally in operation while another is in standby status to be used as needed. The third pump is used only for emergency injection. For emergency operation, the normal letdown coolant flow line and the normal pump seal return line are closed, and additional makeup flow is supplied through the HPI emergency lines from the borated water storage tank.) As the RCS inventory continues to decrease, voiding in the core due to RCS depressurization would occur, providing negative reactivity. The ICS controllers would withdraw control rods in an attempt to maintain core power. Reactor power would eventually decrease due to the voids in the core. The RCS would evolve to a well-mixed two-phase mixture due to continued RCP operation. The RCS liquid inventory would be decreasing since HPI flow would be limited to normal charging flow rates and letdown would remain unisolated until operator action was credited. RCS pressures would be higher than traditional LOCA analyses due to the continued power generation.

For larger breaks, the initial voiding in the core would be sufficient to shut down the core. RCS pressure and pressurizer level would decrease rapidly. The ICS response would not be sufficient to keep the core at power. A second HPI pump would start due to low RCP seal flow, but the additional injection would not significantly affect the RCS inventory depletion. The primary to secondary heat transfer would eventually be affected. The RCS would evolve to a well-mixed two-phase mixture due to continued RCP operation. For the largest breaks, core flood tank injection would occur.

At this point in the transient, containment conditions would be typical of a high energy line break, with the exception that ES equipment to mitigate the adverse containment conditions have not been actuated. If at some point in time, the RCP auxiliaries are lost, due to either equipment functioning correctly or operator action to isolate containment, then the RCPs may not be able to continue operating. The operators are trained to trip the RCPs on the loss of RCP auxiliaries, and would be expected to perform this action. The longer the delay before operator action is assumed, the more likely it is that the RCPs might stop. Current EOP guidance directs the operator to depressurize the steam generators to increase ECCS flow. However, a 30-minute operator action time would not allow this either. The consequence of having the RCPs trip while the RCS is highly voided is significant. The liquid dispersed around the loop would fall into the low points of the RCS, and depending on the amount of voiding could result in immediate core uncovery. The current 2-minute operator action time is designed to avoid this result. Relative to the current licensing basis calculations, the LOCA response in the D3 analyses is more severe due to the ATWS conditions and absence of ESPS actuation.

3.2.3.3.3 Benefits of Diverse HPI Actuation

The benefits of the proposed diverse HPI actuation are considered qualitatively below. The proposed diverse actuation setpoint is not specifically identified at this time, but will be defined below the current ESPS actuation setpoint. The diverse logic will actuate HPI for the majority of the LOCA spectrum.

The smallest portion of the small break LOCA spectrum does not result in an immediate HPI actuation using current licensing basis assumptions. These cases currently credit operator action to actuate HPI. For this break range, the initial RCS pressure decrease is not sufficient to ensure HPI actuates automatically before RCS pressure increases again due to the reactor trip.

For a small break LOCA with an RPS/ESPS SWCMF, the post-trip RCS pressure increase would not occur. RCS pressure would be expected to decrease monotonically. Thus, a diverse HPI actuation would be expected to occur for the entire LOCA break spectrum.

The diverse actuation of HPI would provide similar or better core cooling benefits than those demonstrated by the present UFSAR Chapter 15 LOCA analyses. The difference being the additional flow from a third HPI pump (traditional LOCA analyses only credit minimum safeguards flow). The negative reactivity addition due to the injected boron would ensure the reactor is shut down in the absence of operator action to mitigate the event concurrent with a SWCMF. Therefore, a SWCMF failure of the digital RPS and the ESPS to actuate is offset by additional HPI flow if no single failure is assumed.

3.2.3.3.4 Benefits of Diverse LPI Actuation

The benefits of the proposed diverse LPI actuation are considered qualitatively below. The proposed diverse actuation setpoint is not specifically identified at this time, but will be defined below the current ESPS actuation setpoint, and it is assumed this setpoint will be at an RCS pressure above the LPI shutoff pressure. This would indicate that LPI would perform as intended in the current design basis analyses, even with the presence of a RPS/ESPS SWCMF. Core cooling would be ensured for a double-ended guillotine break of the largest RCS piping. The negative reactivity addition due to the injected boron would ensure the reactor is shut down in the absence of operator action to mitigate the event concurrent with a SWCMF.

3.2.3.4 Conclusion

Duke has provided a D3 analysis that conforms to the guidance of SRP BTP HCIB-19. Duke has evaluated Revision 5 to the BTP (SRP BTP 7-19) dated March 2007 and concluded that the ONS D3 analysis also conforms to the guidance in the revision. D3 design features being installed as a result of the D3 analysis will conform to the BTP guidance as described in Section 2.4 of this Enclosure.

As indicated above, the ONS D3 analysis identified the need to install a diverse LPI actuation system. To address continued NRC concerns regarding the time available for an operator to initiate HPI during a SBLOCA and to address the issue of the RPS/ESPS common processor (i.e., RPS channels A, B, and C sharing processors with ESPS channels A, B, and C), Duke agreed to install a DHPIAS to provide additional defense in depth. The qualitative analysis provided in Section 3.2.3.3, performed to demonstrate the benefits of installing a DLPIAS and DHPIAS, justifies crediting a manual reactor trip to mitigate the effects of a small break LOCA concurrent with an SWCMF.

Duke commits to install a DLPIAS and DHPIAS concurrent with the RPS/ESPS digital upgrade for each ONS unit.

Based on the above, Duke concludes that the D3 analyses performed for the digital RPS/ESPS conforms with applicable NRC guidance.

3.2.4 Functional Requirements

> *RG 1.206, Appendix C.I.7-A states the following topic shall be addressed:*
>
> *"(4) Functional requirements and commitments—The application should address the functional requirements, commitments to comply with IEEE 603, and the GDC. In addition, the application should include information on conformance or commitments to NRC RG 1.152. RG 1.152 provides guidance on minimum functional and design requirements for computers used as components of a nuclear power generating plant safety system. RG 1.152 also provides digital safety system security guidance."*

The TXS Functional Requirements and commitments to comply with IEEE Std 603, and the Plant Design Criteria for the RPS and ESPS, also known as the Engineered Safety Features Actuation System (ESFAS) are contained in the following Duke documents:

- ESFAS Replacement Project Specification
- RPS Replacement Project Specification

- RPS and ESFAS System Functional Description
- RPS Design Basis Document
- ESPS Design Basis Document

The existing RPS/ESPS design functions and features are detailed in the Duke Design Basis Documents for these systems.

The RPS/ESPS Functional Description provides a functional description of the RPS Reactor trip functions and ESPS Actuation functions for the existing Bailey RPS and ESPS functions. The new digital RPS/ESPS design features are discussed in a New Design Features section for each Function. For the existing RPS and ESPS functions, the functional description document provides a high level description of the protective action, a description of the inputs required to perform the function, a description of the existing algorithm and a description of the outputs currently provided by the system. RPS Trip and ESPS actuation algorithms which utilize the 2.MAX and 2.MIN analog input parameter values are described for the RPS/ESPS functions. Contact input algorithms are also described.

The RPS/ESPS Functional Description describes the functional requirements for the modified RCPPM hardware. In addition, the functional requirements for the new ESPS Status Panel, replacement pushbuttons, indication lights and control switches are described. Other TXS system features such as the OAC gateway interface, the GSM and associated alarming, testing, and calibration requirements as well as graphical display screens are described.

In summary, the digital RPS/ESPS functional requirements are presented in the Duke documents stated above. Compliance with 10 CFR 50.55a(h), IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 (which is endorsed by RG 1.152, Revision 2) is addressed in Sections 3.3 and 3.4 of this Enclosure.

See also the Design Criteria requirements in Section 3.2.1 of this Enclosure.

3.3 Conformance with IEEE Std 603 [1]

The information included in this section explains how the design for the new digital RPS/ESPS complies with IEEE Std 603-1998 by addressing the safety system design basis listed in RG 1.206 Appendix C.I.7.B-1 and 2. The design basis items listed in the RG are consistent with the safety system criterion listed in Section 5 of the IEEE Std 603-1998.

The purpose of the revision from IEEE Std 603-1991 to 1998 is to clarify the application of this standard to computer-based safety systems and to advanced nuclear power generating station designs. The 1998 revision provides an information annex for the treatment of electromagnetic interference (EMI) and radio-frequency interference (RFI), clarifies definitions (e.g., Class 1E), and updates references. IEEE Std 7-4.3.2-1993 provides additional guidance on applying the safety system criterion specified by this standard for the use of computers as components in safety systems. Duke considers the 1998 revision to IEEE Std 603-1991 more appropriate for referencing since it clarifies the application of the standard to computer-based safety systems. Since the 1998 revision to IEEE Std 603 does not change any IEEE Std 603-1991 requirements, Duke has evaluated the digital RPS/ESPS for compliance to IEEE Std 603-1998.

3.3.1 Single-Failure Criterion

> *IEEE Std 603-1998, Clause 5.1 states:*
>
> *"The safety systems shall perform all safety functions required for a design basis event in the presence of:*
> *a) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures;*
> *b) all failures caused by the single failure; and*
> *c) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means."*

RG 1.53, "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Revision 2, November 2003, indicates that conformance with the requirements of IEEE Std 379-2000, "Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," provides methods acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application

[1] Section 3.3 contains excerpts from IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Copyright 1998 IEEE. All rights reserved. These excerpts are located in single-line boxes.

of the single-failure criterion to the electrical power, instrumentation, and control portions of nuclear power plant safety systems.

The protective features of the RPS/ESPS meet the single failure criterion as contained in IEEE Std 603-1991 (and IEEE Std 603-1998) and IEEE Std 279-1971. IEEE Std 603-1991 applies only to portions of the RPS/ESPS affected by the design change. Otherwise, IEEE Std 279-1971 continues to apply. In addition, application of the single failure criterion is further delineated in IEEE Std 379-2000. The protective options meet the single failure criterion of IEEE No. 379-2000 to the extent that:

- No single component failure will prevent a protective system, either ESPS or RPS, from fulfilling its protective function when action is required.
- No single component failure will initiate unnecessary protective system action where implementation does not conflict with the criterion above.

A FMEA performed for the digital RPS/ESPS concludes that the single failure criterion has been fully satisfied. Refer to Section 3.7 of this Enclosure for additional details and conclusions regarding the FMEA.

3.3.2 Completion of Protective Action

> *IEEE Std 603-1998, Clause 5.2 states:*
>
> *"The safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety systems to normal. This requirement shall not preclude the use of equipment protective devices identified in Clause 4, item k) of the design basis or the provision for deliberate operator interventions. Seal-in of individual channels is not required."*

3.3.2.1 Reactor Protective System

The RPS is designed such that protective actions, once initiated, will go to completion prior to being manually reset. The actuation of the RPS is a de-energize to actuate configuration. See Section 2.2, Reactor Protective System, for a detailed description of the design of the RPS. The fast actuation time (much less than 1 second) of RPS makes operator intervention (to reset the logic) improbable once RPS is initiated. In addition, the Control Rod Drive Breakers typically have actuation times much less than 100 milli-seconds making the combined RPS actuation to actual CRD breaker opening very short and virtually impossible to interrupt once initiated.

RPS Bypasses are discussed in Section 3.3.16.6 of this Enclosure. Maintenance bypasses are discussed in Section 3.3.16.7 of this Enclosure.

3.3.2.2 Engineered Safeguards Protective System

The ESPS is designed such that protective actions, once initiated, go to completion prior to being manually reset for continued accident recovery actions. The actuation of the ESPS is an energize to actuate configuration. See Section 2.3, Engineered Safeguards Protective System, for a detailed description of the design of the ESPS. Reset of the ESPS actuation logic once it is initiated is a procedurally controlled activity. The ESPS has a very fast actuation and initiation time, making operator intervention once sensor actuation has occurred highly improbable.

Operating bypasses of ESPS channels are discussed in Section 3.3.16.6 of this Enclosure. Maintenance bypasses are discussed in Section 3.3.16.7 of this Enclosure.

3.3.3 Quality

> *IEEE Std 603-1998, Clause 5.3 states:*
>
> *"Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (See ASME NQA-1-1994). Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993."*

Section 3.3.3 describes compliance with IEEE Std 603-1998, Section 5.3. The following subsections describe the Duke and AREVA NP Quality Assurance Programs, and how each program applies to the RPS/ESPS digital upgrade.

Compliance with IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3 "Quality," is described in Section 3.4.3.

3.3.3.1 Duke Energy Quality Assurance Program

Duke maintains full responsibility for assuring that its nuclear power plants are designed, constructed, tested and operated in conformance with accepted engineering practices, applicable regulatory requirements and specified design bases and in a manner to protect the public health and safety. To this end Duke has established and implemented a quality assurance program (QAP), which conforms to the criteria established in 10 CFR, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants." The Duke Energy Carolinas Topical Report – Quality Assurance Program (Reference 6) is written in the format of UFSAR Chapter 17, "Quality Assurance", in accordance with Revision 2 of RG 1.70, "Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants - LWR Edition" and subsequent NRC guidelines. The QAP described herein is applicable to ONS and referenced in ONS UFSAR Chapter 17.

The Topical Report describes the quality assurance (QA) requirements for those systems, components, items, and services which have been determined to be nuclear safety related (QA Condition 1). Duke's QAP also provides a method of applying a graded QAP to certain non-safety related systems, components, items, and services. These are classified as QA Conditions 2, 3, 4, or 5.

The quality of systems, components, items, and services within the scope of QA Conditions 1, 2, 3, 4, and 5 is assured commensurate with the system's, component's, item's, or service's importance to safety.

QA Condition 1 covers those systems and their attendant components, items, and services which have been determined to be nuclear safety related. These systems are detailed in the Safety Analysis Report applicable to each nuclear station. The Topical Report applies in its entirety to systems, components, items, and services identified as QA Condition 1.

The affected RPS/ESPS and associated components within the scope of this LAR are classified in accordance with the QAP. Those systems and components that perform an active safety function are classified as QA Condition 1.

Procedures and work instructions necessary to implement the requirements of the QAP are developed and approved by the organization responsible for the activity. These procedures and instructions may be contained in manuals, station procedures and directives, administrative instructions and/or other documents. These documents identify the criteria to determine acceptable quality for the activity being performed. On-site implementation of procedures and work instructions is the responsibility of the Site Vice President.

The following sections describe the primary manuals, procedures and directives, by project phase, used in the course of the RPS/ESPS digital upgrade project.

3.3.3.1.1 Design Phase

The design phase is performed within the context of the plant engineering change program, governed by department directives and design change program directives.

Duke contracted with AREVA NP to perform the managed task engineering change activities, with the exception of owner acceptance of the engineering deliverables (equipment specifications, calculations, drawings, implementing procedures, test procedures, engineering change package, etc.). The contract includes Outside Contractor Interface Agreements that describe how AREVA NP performs engineering change activities per the requirements of the Duke engineering change program while doing so under the AREVA NP QA Program (described in Section 3.3.3.2 below). AREVA NP maintains an engineering resource pool that is qualified to the Duke engineering change program. Duke is performing the Owner Acceptance function in accordance with the engineering change program.

Supplemental Oversight

In addition to using these standard QA procedures for a major change to a QA Condition 1 system, the RPS/ESPS project is using a supplemental, project-specific Quality Management Plan (QMP). The purpose of the QMP is to provide supplemental guidance and instructions to provide additional assurance that the RPS/ESPS digital upgrade project deliverables, including hardware and software engineering documents associated with licensing the new TXS system, meet the requisite quality requirements. A "deliverable" in the context of the QMP is defined as any configuration item, including hardware, software, or documents, that is produced by any organization responsible for that scope on the RPS/ESPS digital upgrade project.

The QMP applies to all activities related to the processes, policies and procedures used in the production, checking, review, approval and subsequent revisions to the deliverables described above. These activities include those assigned to Duke Energy personnel, including staff augmentation contractors, as well as activities assigned via contract to vendors and suppliers, such as AREVA NP.

The QMP employs a Licensing and Quality Steering Team (LQST) made up of Duke and AREVA NP Managers and Supervisors. The LQST deploys engineering resources from a Duke and AREVA NP "Core Team" charged with reviewing identified deliverables for technical completeness, accuracy, and quality. The LQST is also responsible for reviewing the results of the Core Team activities and providing feedback and direction as required.

The QMP is supplemental only. Where it may be in conflict with other Duke Energy policies, procedures, standards or guidelines, those documents govern.

3.3.3.1.2 Manufacturing

The manufacturing phase for the RPS/ESPS Upgrade Project is also contracted to AREVA NP. This phase includes basic hardware and software design, detailed hardware and software design, hardware manufacturing, software development, integration of the hardware and software, FAT, and SAT.

These equipment activities are outsourced to AREVA NP under the Duke Nuclear Procurement Program. AREVA NP is performing the contracted equipment scope under their QA program and their implementing procedures (described in Section 3.3.3.2 below). Specifications describing the equipment requirements as well as the required development and manufacturing activities are included in the contract. AREVA NP is an approved supplier, audited by Duke, under the Nuclear Procurement Program and associated directives.
The digital RPS/ESPS and supporting components are being procured from AREVA NP as basic components, furnished with Certificates of Conformance to purchase order requirements.

3.3.3.1.3 Inspection

Inspection of equipment purchased for implementation as part of design changes to Duke nuclear facilities is governed by the Duke Nuclear Procurement Program and associated directives.

As part of the procurement process, inspections occur at various stages of the project. Prior to submittal of specifications for bidding and eventual contract award to the vendor(s), verification is made that the potential vendor is qualified per industry QA processes to provide the equipment identified within the specification.

Once the contract is awarded for procurement of the specified equipment and/or services, project related inspections begin. The vendors manufacturing facilities and service organizations undergo a general engineering inspection and familiarization. More formalized inspections occur as the project progresses. Prior to shipment of the equipment, inspections occur at the vendor facilities with the purchaser to verify manufacture of the equipment to approved drawings, project documentation and perform pre-Factory Acceptance Testing (FAT) assembly, hardware configuration, and if applicable, software configuration.

The equipment is then shipped to the purchaser's site and upon arrival is inspected to verify the delivered materials are in general compliance with the equipment purchase specification(s) and the associated shipping documents. Additional detailed inspections occur by the engineering and implementation organizations to verify technical details of the received equipment as part of the staging for implementation. Various details such as material counts, wiring, mountings, arrangements, configurations, and physical packaging (cabinetry) is inspected by the purchaser.

As mentioned above, these activities are performed using both specific and general guidance provided in Duke Nuclear Procurement and Duke Nuclear Engineering directives and procedures.

3.3.3.1.4 Testing

The RPS/ESPS digital upgrade project includes several testing activities. A FAT will be performed on the equipment in accordance with the AREVA NP QA program, using FAT procedures accepted by Duke, as specified in the contract. Refer to Section 3.5, Testing, for more details on testing.

A 30-day Availability Run will be performed after the FAT to ensure no technical or quality issues emerge. After the Availability Run, a SAT will be performed. AREVA NP has the option to correct issues identified during the FAT before the FAT is completed, or during the SAT, using the SAT to perform validation testing of the changes.

A Modification Test Plan (MTP) will be developed for the project. The MTP specifies the necessary testing to be performed during and after installation of the upgraded systems and components. The actual test procedures used will be a combination of permanent operations procedures, permanent maintenance procedures, and temporary test procedures. These procedures are prepared, reviewed, approved, controlled and performed under existing Nuclear System Directives.

3.3.3.1.5 Installation

Installation of the upgraded systems and components will be performed in accordance with written installation procedures and work orders. The scope of the installation procedures and work orders includes safety tagging requirements, demolition and removal of existing cabinets and components, installation of new cabinets and components, modification of supporting structures, cabling, terminations, checkout, and system energization. The upgraded systems are not available or operable until all post modification testing is performed as required by the MTP and the implementation is accepted by the Owner Control Group (OCG) which for this project is the ONS Operations (OPS) staff.

Installation procedures are also prepared, reviewed, approved, controlled and performed under existing Nuclear System Directives (NSDs).

Work orders are planned, scheduled and controlled using the Duke Work Process Manual (WPM). Duke is experienced in the installation of major engineering changes, and is solely responsible for the quality of installation activities.

3.3.3.1.6 Operations

Operability of the digital RPS/ESPS and components will be determined in accordance with TSs 3.3.1, "RPS Instrumentation," 3.3.3, "Reactor Trip Modules," 3.3.5, "ESPS Analog Instrumentation," 3.3.7, "Engineered Safeguards Protective System Digital Automatic Actuation Logic Channels."

Operation of the digital RPS/ESPS and associated components is conducted under various department directives and procedures. Operations Procedures are used to perform operational tasks with plant systems and components. Periodic Test (PT) procedures are used to perform surveillance tests on plant systems and components. Abnormal Operating Procedures are used to perform abnormal event mitigation and recovery activities. Emergency Operating Procedures are used to perform design basis event mitigation and recovery activities. Duke is experienced in plant operation following major engineering changes, and is solely responsible for quality of operations.

3.3.3.1.7 Maintenance

Maintenance of the digital RPS/ESPS and components will be conducted under the Preventive Maintenance Program described in NSDs and the ONS Maintenance Manual, described in various Maintenance Directives (MDs). The MDs provide policies and procedures which direct and support the conduct of work as it relates to the philosophy of the ONS maintenance activities and other groups performing maintenance at ONS.

Maintenance procedures are used to perform maintenance activities on plant systems and components. Instrument Procedures (IPs) are used to perform module checkouts, instrument and instrument string calibrations and checks, system troubleshooting and corrective maintenance. PT procedures are used to perform surveillance tests on plant systems and components. Duke is solely responsible for the quality of maintenance on the RPS and ESPS.

The procedures described above will be revised as needed for the digital RPS/ESPS in accordance with existing NSDs.

3.3.3.2 AREVA NP Quality Assurance Program

The AREVA NP Quality Management Manual (QMM) (Reference 12) is the upper tier corporate document that defines the quality requirements for the design, manufacturing and testing of the TXS system and associated engineering services provided by AREVA NP for the ONS digital RPS/ES project.

Section 5.3 of Standard Review Plan Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," notes that for digital computer-based systems, the quality requirements described in Clause 5.3 of IEEE Std 7-4.3.2-2003 should be addressed. Compliance with Clause 5.3 of IEEE Std 7-4.3.2-2003 is addressed in section 3.4.3.

The QMM is written to comply with the following codes, regulations and standards:

International Code

- I.A.E.A. 50-C-Q (1996) Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations (I.A.E.A. - International Atomic Energy Agency)

National standards and regulations

- Order of August 10, 1984 relative to the quality of the design, construction and operation of Basic Nuclear Facilities (French Regulation)

- KTA 1401 (06/96) General Requirements Regarding Quality Assurance (KTA Kerntechnischer Ausschuss = German Nuclear Safety Standards Commission)

- 10 CFR 50 Appendix B Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants (U.S. Regulation)

- ANSI/ASME NQA-1-1983 and 1994 Addenda Quality Assurance Program Requirements for Nuclear Facilities (ASME – American Society of Mechanical Engineers)

For the United States (US) Region, the compliance with ANSI/ASME NQA-1-1994 is ensured through implementing procedures.

AREVA NP's implementation of the QMM is periodically audited by the Nuclear Procurement Issues Committee (NUPIC). The NUPIC program evaluates suppliers furnishing safety-related components and services and commercial grade items to nuclear utilities. The most recent NUPIC audit of AREVA NP was performed in November 2006.

Section 2.1 of the TXS Topical Report (Reference 2) describes the QA program for the design and qualification of the TXS platform (hardware, operating system software, Function Block library and application software development tools). NRC issued an SER for the TXS Topical Report by letter dated May 5, 2000 (Reference 1).

ANP-10272, "Software Program Manual for TELEPERM XS™ Safety Systems Topical Report," (referred to as the TXS Software Program Manual) (Reference 11) describes the program measures incorporated by AREVA NP to ensure that the TXS application software attains a level of quality commensurate with its importance to safety functions, performs the required safety functions correctly, and conforms to established technical and documentation requirements, conventions, rules, and industry standards. The TXS Software Program Manual applies to application software developed for all TXS projects in the United States. The TXS Software Program Manual was submitted to NRC for review and approval in a letter from Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Review and Approval of ANP-10272, 'Software Program Manual for TELEPERM XS™ Safety Systems Topical Report'," NRC: 06:061, December 21, 2006.

All design work, products and services provided for the RPS/ESPS digital upgrade project are performed to the requirements of the AREVA NP Quality Management Manual (Reference 12). These quality requirements are supplemented by the additional QA requirements for TXS projects described in the TXS Topical Report and the TXS Software Program Manual. Project documentation used as design input or delivered to the customer as design output is stored in the AREVA NP records management system. Similarly, project records arising from QA inspections and audits are stored in the AREVA NP records management system. The record storage requirements are described in the AREVA NP Records Management Program Manual.

3.3.3.3 Conclusion

The programs, policies, procedures, and activities described in Section 3.3.3 demonstrate that the components and modules of the digital RPS/ESPS have been designed, are being manufactured, and will be inspected, installed, tested, operated, and maintained in accordance with established QA programs by Duke and AREVA NP.

3.3.4 Equipment Qualification

> *IEEE Std 603-1998, Clause 5.4 states:*
>
> *"Safety system equipment shall be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980. Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993."*

The TXS system being installed at ONS is an identical functional design to the TXS system platform described in the AREVA NP Topical Report (Reference 2), which was approved by the NRC in their SER (Reference 1) of the TXS platform, dated May 5, 2000. There are some minor differences between the generically approved TXS and the TXS system being installed at ONS that do not affect the safety conclusions reached in the SER.

The digital and analog input and output modules are identical to the ones reviewed and approved by the NRC. A supplemental equipment qualification report (refer to Item 20 of Table 1-2) details the effort undertaken to qualify the SVE2 processor and concludes that the new replacement does not cause a variance in the NRC approval of the original TXS system. In summary, the ONS TXS system is enveloped by the TXS system detailed in the TXS Topical Report and approved by the associated SER. The TXS system, including the SVE2 microprocessor, meets the qualification guidance presented in EPRI TRs-107330 (Reference 7) and 102323 Revision 1.

The AREVA NP EQ Report (refer to Item 21 of Table 1-2) for the TXS provides a summary of the equipment testing and analysis performed to meet the requirements of IEEE Std 603-1998, IEEE Std 323-1983, EPRI TR-107330, EPRI TR-102323 Revision 1, and RG 1.180 Revision 1. This report addresses all of the equipment within the RPS/ESPS cabinets and summarizes the specific required environmental conditions and the testing/analysis performed to qualify this equipment. This testing/analysis confirmed that the TXS safety system is fully qualified and capable of performing its designated safety functions while exposed to normal, abnormal, test, accident, and post-accident environmental conditions, as required.

- Mild environment qualification conforms to the guidance of IEEE Std 323, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations."
- EMI/RFI qualification is consistent with the guidance of EPRI TR-102323, Revision 1,"Guidelines for Electromagnetic Interference Testing in Power Plants" and RG 1.180, Revision 1.
- Seismic Qualification is consistent with ONS Specification ECV-0601.00-00-0005.
- The isolation qualification test for selected components were designed to demonstrate isolation capability per the requirements of EPRI 107330. EPRI 107330 requires demonstration of isolation capability of at least 600VAC and/or 250 VDC, applied for 30 seconds, during which time the operation of the chassis backplane shall not be interrupted. The test specimen completed the isolation tests successfully, meeting the requirements of EPRI 107330 and the Duke Energy RPS and ESFAS Replacement Project Specifications.
- Surge Testing is compliant with EPRI TR-102323, Revision 1.

The effects of EMI Signal Susceptibility, EMI Signal Surges and Impulses, and Equipment Emissions for equipment in each plant area were addressed in accordance with the guidelines of EPRI TR-102323, Revision 1 and RG 1.180, Revision 1.

EQ testing for the RPS/ESPS cabinets consisted of environmental tests (temperature and humidity), seismic tests, EMI/RFI tests, electrical fast transient tests, surge withstand tests, electro-static discharge tests, power supply tests and isolation tests. Components that were not included in the qualification testing program but are utilized in the TXS safety system were either purchased as 1E or qualified by engineering analysis in accordance with an approved AREVA Quality program. Refer to the AREVA NP Equipment Qualification Report (Item 21 of Table 1-2 of this Enclosure). Environmental, seismic, and Electromagnetic Compatibility (EMC) testing was performed on ancillary equipment included in the RPS/ESPS design change. This equipment included the AREVA NP-manufactured NI equipment, AREVA NP-manufactured RCPPM equipment, a Qualitrol lamp box and Cutler-Hammer Type 10250T switches.

The ancillary equipment was type-tested and analyzed in accordance with the QA program, regulatory requirements and standards provided by IEEE Std 323-1983, EPRI TR-107330, RG 1.180, Revision 1, 10 CFR 50 Appendix B, RG 1.100 Revision 2, IEEE Std 344-1975, IEEE Std 381-1977, and EPRI TR-102348 and therefore meets the requirements as specified in Section 5.4 of IEEE Std 603-1991.

All components being installed as part of the RPS/ESPS digital upgrade are fully qualified to the applicable standards.

Refer to Section 3.4.4 of this Enclosure for additional details regarding compliance with the requirements of IEEE Std 7-4.3.2-2003.

3.3.5 System Integrity

> *IEEE Std 603-1998, Clause 5.5 states:*
>
> *"The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Guidance on the application of this criteria for safety system equipment employing digital computers and software or firmware is found in IEEE Std 7-4.3.2-1993."*

The TXS safety system has been designed and tested to confirm the equipment demonstrates system performance adequate to ensure completion of protective actions over the range of transient and steady-state plant conditions.

- The digital RPS/ESPS will be installed inside the control room envelope, which is maintained in an ambient environment (in order to assure its habitability for human operators, although intervention is not required for system function).
- The design basis specifies the Total Integrated Dose (TID), including both normal and accident conditions. The design basis conditions for the Control Complex (Control Room, Cable Spreading Room, and Equipment Room) are delineated both in the RPS/ESPS Replacement Project Equipment Specifications (refer to Items 37 and 38 of Table 1-2 of this Enclosure) and in the Oconee Environmental Qualification Criteria Manual for both Normal and Accident conditions including TID. The RPS and ESPS are qualified to both plant conditions.
- The digital RPS/ESPS will be installed inside the control room, which is to be maintained at a positive pressure with respect to adjacent areas during normal and accident conditions.
- The design basis specifies the range of ambient temperature conditions during normal and accident conditions as 60 – 100°Fahrenheit (F) for the Control Room, and 60 - 120°F for the Cable Spreading Room. For the new system, the heat load effects are less than the current system.
- The design basis specifies the range of humidity conditions during normal and accident conditions as 30 – 80% relative humidity (RH) (non-condensing)
- The design basis specifies the seismic response spectra for a design basis earthquake. This specification envelopes the range of seismic based vibration conditions that could occur during normal and accident conditions.

- The design basis specifies the range of electrical power supply conditions during normal and accident conditions in the 120 volts (V) 60 hertz (Hz) alternating current (AC) vital power systems as ±10% voltage and ±3% frequency.

The digital RPS contains no analog or digital control output function. A discrete/binary control output in the form of relay contacts opening does act to remove power from the CRD Trip Breaker(s) undervoltage (UV) coil. The digital ESPS is similarly configured to affect Reactor Building Isolation and Cooling, in addition to HPI or LPI injection of borated water into the RCS. RPS/ESPS applications are the same as those described in the TXS Topical Report. The NRC previously docketed their acceptance of these features in the TXS SER (Reference 1). Page 50 of the SER provides the following assessment:

> "The TXS meets the automatic and manual control requirements. Failure of the automatic controls does not interfere with the manual controls."

The FMEA is a qualitative analysis that uses a systematic approach to identify all potential failures, evaluates the consequence and effects of failures, and verifies that the design satisfies the safety criteria defined by the single-failure criterion and the other applicable safety criteria as they relate to the performance of the FMEA. The FMEA for the RPS/ESPS digital upgrade is described in Section 3.7 of this Enclosure.

Computer system integrity is addressed in Section 3.4.5 of this Enclosure.

3.3.6 Independence

IEEE Std 603-1998, Clause 5.6 indicates that:

The application document should demonstrate the independence between (a) redundant portions of a safety system, (b) safety systems and the effects of design basis events, and (c) safety systems and other systems. Three aspects of independence should be addressed in each case:
• Physical independence,
• Electrical independence, and
• Communications independence.

The modified portions of the RPS/ESPS design comply with IEEE Std 603-1998. The TXS Topical Report (Reference 2) and associated SER (Reference 1) provide generic information about the TXS system, showing compliance with the criteria, based on overall system design. Plant specific design documents describe how the design is implemented for the ONS RPS/ESPS digital upgrade project.

3.3.6.1 Redundant Portions of Safety Systems

All RPS protective functions are implemented through redundant sensors, measuring channels, logic, and actuation devices. These elements combine to form protective channels. Each protective channel is powered from a separate inverter-backed, safety-related power source. There are four protective channels (channels A through D, see Section 2.2.1 of this Enclosure for a detailed description). The RPS initiates a reactor trip when any two of the four protective channels detect that a safety limit has been exceeded. One non-safety channel (channel E, see Section 2.2.5 of this Enclosure for a detailed description) is implemented to provide a non-safety channel of redundant instrumentation and house the MSI and interface to the service units. Channel E is powered from a non-safety battery backed power source. Redundant protective channels are physically separated and electrically isolated from other redundant protective channels and from non-safety control instrumentation channels.

Each RPS channel has its own transmitters and contact inputs. For transmitter 4-20 mA inputs, TXS SAA1 Analog Signal Modules are used to convert the current signal to a voltage signal. The TXS S466 Analog Input Modules convert the voltage input signals to digital counts for processing by the TXS SVE2 Processing Modules. TXS software A-MRC Function Blocks convert the input signal digital counts to engineering units.

For RTD inputs, a Weed temperature transmitter receives the signal from the RTD and converts it to a 4-20 mA signal. That signal is then processed in a similar manner as described above.

The TXS RPS system supplies 120 VAC wetting voltage to the contact for process signal contact inputs. This binary voltage signal from the contacts (~0 VAC when contact is open or ~120 VAC when closed) is then converted to a 24 VDC binary signal (~0 VDC or ~24 VDC) by an Optocoupler for the input to the TXS S430 Digital Input Modules where inputs and status information are processed and sent to the SVE2 Processing Modules.

The four RPS Channel processors are interconnected via SINEC-L2 fiber-optic data links. Each RPS Channel uses these fiber-optic data links to exchange the process inputs. This enables each protective channel to perform validation checks, on-line signal monitoring, and signal selection when processing the RPS functions. This exchange of process inputs provides each channel the same set of information for safety function processing.

The RPS Channel processors use 2.MIN or 2.MAX Function Blocks for analog process input signal selection and signal validation. For signal selection, each protective channel uses the 2.MIN measurement to compare with the low set point value and then determines the partial trip status of that channel for a "low trip" parameter. Similarly, it uses the 2.MAX measurement to compare with the high set point value and then determines the partial trip status of that channel for a "high trip" parameter. This TXS function will reject the outlying signal in the process measurement and thereby minimize inadvertent trips.

The RPS Channel processors use two-out-of-four Function Blocks to provide coincidence logic for RPS trip functions that utilize process contact inputs (i.e., pressure switches, Reactor Coolant Pump Power Monitor relays, and anticipatory feedwater and turbine trips).

If two or more RPS channels indicate a valid software trip logic condition (two-out-of-four), the binary outputs will de-energize the trip relays associated with those channels in all RPS channel cabinets, tripping all four CRD breakers.

All ESPS protective functions are implemented through redundant sensors, measuring channels, logic, and actuation devices. These elements combine to form protective channels. There are three channels of input instrumentation and eight channels of digital output logic grouped in two divisions (Odd and Even channels). Each input channel is powered from a separate inverter backed safety power source. Odd and Even channels are also powered from separate inverter backed safety power sources. The ESPS shall initiate an output signal when any two of the three protective channels detect that a safety limit has been exceeded. Redundant protective channels are physically separated and electrically isolated from each other.

The ESPS consists of two subsystems. Each subsystem consists of three ESPS Input Channels (A1, B1, C1 and A2, B2, C2) and eight Automatic Actuation Output Logic Channels grouped into an Odd (Channels 1, 3, 5, 7) Voter and an Even (Channels 2, 4, 6, 8) Voter. Refer to Figures 2.1-2 and 2.3-1. Either subsystem can perform the required safety functions. The ESPS channels for ESPS Subsystem 1 (A1, B1, and C1) are located in the RPS cabinets and share TXS processors with RPS Channels A, B, and C. The input sensors (pressure transmitters and pressure switches) are shared between the two ESPS subsystems. The input sensors are connected to the ESPS subsystem 2 (located in the ESPS Cabinets) where the input signals are buffered and sent to ESPS subsystem 1 (located in the RPS Cabinets).

For transmitter 4-20 mA inputs, the signals enter the A2, B2 or C2 cabinets and are buffered through an SNV1 card. One signal continues in the A2, B2, or C2 cabinet to a TXS SAA1 module. The other signal is sent to the respective A1, B1, or C1 cabinet where it also goes to a TXS SAA1 module. TXS SAA1 modules are used to convert the current signal to a voltage signal. TXS S466 Analog Input Modules convert the voltage input signals to digital counts for processing by the TXS SVE2 Processing Modules. TXS software A-MRC Function Blocks convert the input signal digital counts to engineering units.

ESPS Subsystem 2 supplies 120 VAC wetting voltage to the contacts for process signal contact inputs. This binary voltage signal from the contacts (~0 VAC when contact is open or ~120 VAC when closed) is then converted to a 24 VDC binary signal (~0 VDC or ~24 VDC) by an Optocoupler for the input to a TXS S430 Digital Input Module where inputs and status information are processed and sent to the SVE2 Processing Modules.

Each ESPS channel within a subsystem exchanges the process variables obtained via fiber-optic data links with the other two channels. This enables each protective channel within a subsystem to perform validation checks, on-line signal monitoring, and signal selection when processing the ESPS functions. When the process variables monitored by a channel exceed the limit value defined by the function algorithm, then that channel generates a protective action which is sent via a fiber optic data link to the Odd and Even Voters associated with that subsystem. The TXS voters monitor for the required coincident logic (two-out-of-three) to initiate the system level protective actions (actuation channel initiation).

Physical Independence

The need for physical isolation is met by the physical arrangement of each channel within a separate cabinet(s) and wiring within the cabinets separating power and signal wiring to reduce the possibility of some physical event impairing system functions. The existing eight cabinets used by the four RPS channels will be replaced with four dual bay cabinets housing the TXS RPS equipment. Each of the four RPS channels (A, B, C, and D) will occupy a single TXS dual bay cabinet (no internal separation). Cabinet numbering follows the original layout convention. Two cabinet numbers are assigned to each dual bay cabinet. Physical separation is maintained between redundant RPS channels by the new dual bay cabinets. RPS Channel E occupies its own cabinet, separate from the other four channels.

The existing nine ESPS cabinets will be replaced with nine similar cabinets housing TXS ESPS equipment. Each of the three standalone ESPS input channels (A2, B2, C2) will occupy a single TXS cabinet. Output channels are grouped into Odd and Even channels. Each group (Odd or Even) will occupy two TXS cabinets arranged as dual bay cabinets (no internal separation). Two ESPS cabinets will be provided for ESPS Odd and Even Component Status.

All of the RPS/ESPS cabinets (either single or dual bay) are to be located within the Control Room. These are steel cabinets mounted on a cabinet mounting frame, which is mounted on the floor, and have no hardwired interconnections except for sharing of similar signals through fiber optic cables. (The exception being the hard wired signals between cabinets A1 and A2, B1 and B2, C1 and C2 of the ESPS subsystems.) Process signals for the same parameter are exchanged between channels through fiber optic cables. For cabinets mounted directly against one another, there are no openings between cabinets, except for the dual bay cabinets that are of the same channel. Each RPS/ESPS channel is likewise physically isolated from each other.

Outside the RPS and ESPS cabinets, vital signals and wiring are separated and physically protected to preserve channel independence and maintain system redundancy against physical hazards. System sensors are physically separated from each other. The arrangement of system sensors and field wiring is not changed by the proposed design change.

Electrical Independence

Electrical independence between redundant RPS/ESPS channels is provided for by using diversity of power supplies and separation/isolation of cabling. Each RPS channel is powered from a separate vital 120 VAC bus (KVIA, KVIB, KVIC, and KVID). Cables associated with the four RPS protection channels are color-coded Grey, Yellow, Blue, and Orange, corresponding to RPS protective channels A, B, C, and D, respectively, and are routed in separate cable trays.

ESPS channels are powered from separate vital 120 VAC buses KVIA, KVIB, and KVIC. ESPS channels are similarly color-coded Grey, Yellow, and Blue corresponding to ESPS channels A, B, and C and are routed in separate cable trays. The breakers that supply 120 VAC to the RPS/ESPS1 cabinets are separate from the ones that supply 120 VAC to the ESPS2 cabinets.

The ESPS Odd and Even voter channels are powered from separate vital 120 VAC buses KVIA and KVIB respectively. Voter channels are similarly color coded Grey and Yellow corresponding to Odd and Even and are routed in separate cable trays. The breakers that supply 120 VAC to the ESPS voter cabinets are separate from the ones that supply 120 VAC to the ESPS2 cabinets.

When a power source from another division enters a cabinet, the wiring isolation is maintained between the divisions using qualified 1E isolation devices and wiring practices that meet IEEE Std 384-1992 criteria. In some cases, coils and contacts on the same relays belong to different channels. In that case, electrical isolation of the coil from the contacts is credited for electrical isolation between the channels and the relays used are qualified for this use.

In order to maintain electrical independence when input signals are shared between channels, an SLLM module is used to convert the signal from copper wire to fiber optic. The fiber optic communication equipment is qualified as Class 1E isolation and provides the required electrical separation between each protective channel. Fiber optic communication equipment is also used between protective channels and the MSI and between the ESPS channels and the Voters. Fiber optic isolation prevents internal electrical faults from propagating from one protective channel to other redundant channels.

Communication Independence

Refer to Section 3.4.6.1 of this Enclosure.

3.3.6.2 Safety Systems and Effects of Design Basis Events

The portions of the RPS/ESPS being replaced are all located within the ONS Control Complex. This structure offers protection from the effects of tornado/wind, and pipe ruptures external to the control complex.

The majority of the equipment (including all TXS cabinets and equipment) will be located in the rear of the Control Room, with some auxiliary equipment located in cabinets in the Cable Spreading Room. The Oconee equipment specifications identify the required normal and post accident environmental, and seismic conditions to which the equipment will be qualified as well as providing reference to generic industry qualification standards such as those which apply to EMI/RFI qualification.

A qualification program for all equipment has been carried out to ensure that all equipment will remain functional during and after all applicable ONS Design Basis Events. This includes all equipment used to maintain the inter-channel communication independence described in Section 3.4.6.1 of this Enclosure. Refer to Section 3.3.4 of this Enclosure for more information on the equipment qualification program.

3.3.6.3 Safety Systems and Other Systems (i.e., non-safety equipment)

Physical Independence

RPS non-safety channel E will share a cabinet with the non-safety TXS MSI and the diverse actuation systems (DLPIAS and DHPIAS). This cabinet has been subjected to the same seismic testing as the other structurally identical 17 safety-related replacement TXS cabinets (The variation being in the equipment content of the various cabinets). These non-safety components are physically separated and electronically isolated from the safety systems, thereby assuring the safety systems will not be affected by failures in non-safety systems and vice versa.

The TXS Gateway computer provides the communication interface between the TXS RPS/ESPS and the OAC and is located in a separate OAC computer room adjacent to the Main Control Room. The Gateway does not utilize TXS hardware [components, but does operate on TXS proprietary software.]

The Service Unit is located in the general area of the OAC. Four coordinated programs are installed in the Service Unit – collectively the GSM, Alphanumeric Service Monitor (ASM), Service Monitor Server (SMS), and Specification and Coding Environment (SPACE) editor.

Electrical Independence

Power supplied to RPS non-safety Channel E and associated non-safety TXS equipment within that cabinet is from an inverter-backed 120 VAC power panel. Power to the TXS Gateway and TXS Service Unit computers are from separate non-1E inverter-backed 120 VAC power panels. All MSI communication links are via fiber optic cables, thereby assuring electrical isolation between the individual safety related RPS and ESPS channels and non-safety related components.

Communication Independence

Refer to Section 3.4.6.2 of this Enclosure.

3.3.7 Capability for Test and Calibration

> *IEEE Std 603-1998, Clause 5.7 states:*
>
> *"Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:*
>
> - *Appropriate justification shall be provided (e.g., demonstration that no practical design exists),*
> - *Acceptable reliability of equipment operation shall be otherwise demonstrated, and*
> - *The capability shall be provided while the generating station is shut down.:*

The TXS RPS/ESPS is designed to provide capability for test and calibration consistent with guidance provided in the following documents:

- RG 1.22, "Periodic Testing of Protection System Actuation Functions"
- RG 1.118, "Periodic Testing of Electric Power and Protection Systems," Revision 3
- RG 1.153, "Criteria for Power, Instrumentation, and Control Portions of Safety Systems," Revision 1
- RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems"
- IEEE Std 338-1987, "Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems"

3.3.7.1 Failure Detection

An FMEA was performed on the digital RPS/ESPS. Refer to Section 3.7 of this Enclosure. The FMEA evaluated the system to determine if it satisfies single failure criterion by determining if the safety system performs all safety functions required for a DBE in the presence of:

- 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 system actions that cause or are caused by the DBE requiring the safety functions.

The FMEA systematically evaluated the system to determine the effect on the system of credible single failures. The effects were evaluated to determine if remedial actions were required to assure conformance to safety system criteria including single-failure criterion, channel independence, automatic and manual control, completion of protective actions, operating and maintenance bypasses and testability.

For each postulated failure mode, the FMEA determined ways in which the failure could be detected. Failures that can be detected only by test were clearly identified. The conclusions section of the FMEA describes the interaction of components within the system and recommends criteria for testing. The FMEA recommended criteria have been factored into system testing activities and criteria.

3.3.7.2 Self Test Features

The RPS/ESPS provides automatic monitoring of each of the input signals in each channel to perform software limit checking (online signal validation) against required acceptance criteria and to provide hardware functional validation for performance of continuous channel checking. These automatic monitoring functions improve the availability of the system and reduce the maintenance burden.

The RPS/ESPS performs automatic online cross channel checks separately for each channel and performs continuous online signal fault detection and validation. The system also performs continual online hardware monitoring.

Online signal validation is implemented as follows:

- Analog signals coming into the TXS RPS/ESPS are validated based on out-of-range checks (where possible) and status of the analog-to-digital converter in the analog input cards.
- Binary signals coming into the TXS RPS/ESPS are validated based on functionality of the binary input card channels.
- Online signal comparison (analog and binary) between redundant measurements is utilized for deviation alarms.

[The NRC previously] docketed its acceptance of TXS test features in the TXS SER (Reference 1). Page 50 of the SER states:

> "The capability for testing and calibration has been demonstrated in compliance with RG 1.22, RG 1.118 and IEEE-338. "

In addition to the monitoring mechanisms inherent in the system there are also configured mechanisms that reduce the number of undetectable failures. The configured monitoring mechanisms make use of redundant information processing with down-circuit majority voting. By comparing redundant information, deviations can be detected that indicate the presence of a failure.

Equivalent analog signals of different measuring channels (i.e., redundant channels) will be continuously compared with each other to detect and monitor channel signal deviations. This includes the entire instrument string consisting of sensor, transducer, input signal module and the associated equipment for signal transfer. If the signals are not within a pre-defined tolerance range, this condition is alarmed on the Unit Statalarm and input to the plant OAC.

The self-testing features described above are implemented by the RPS/ESPS. The hardware and software associated with these systems are classified as Nuclear Safety Related, QA Condition 1. The MSI, located in RPS/ESPS cabinet 16, provides the interface between the safety related systems and the non-safety related TXS Gateway computer and TXS Service Unit. The MSI is the credited isolation point for communications between the safety related TXS protection channels and the non-safety related systems.

3.3.7.3 Periodic Testing

[The periodic testing which is] required is addressed by channel calibrations which encompass channel functional tests. The channel calibrations are performed during refueling outages. Specifics on [and the channel calibrations are addressed in Section] 3.3.16.5 of this enclosure.

If on-line testing is required for troubleshooting or in response to maintenance, the digital RPS/ESPS design allows for this testing. Simulated signal inputs into a channel can be applied using Measuring and Test Equipment. During performance of testing or maintenance of the digital RPS/ESPS, it may be necessary to place individual RPS channels and/or ESPS Voters into the bypass mode. When a channel or Voter is placed in bypass, a control room Statalarm and an OAC computer alarm will become active so the condition is clearly indicated to the CROs. The absence of a bypass alarm indicates that no RPS channel or ESPS Voter is in bypass.

Administrative procedures will provide appropriate guidance in the event a portion of the digital RPS/ESPS is in bypass or is tripped. These procedures are augmented by automatic indication at the system level that the system is in bypass or that a portion of the protection system and/or the systems actuated or controlled by the protection system is tripped.

On-line periodic testing of the control rod drive reactor trip breakers is required. The RPS is designed to allow the reactor trip relays to be de-energized so that this periodic breaker testing can be performed. The ESPS is designed to allow either a Go or No-Go Test to be performed. There are two output relays with the contacts wired in series from the ESPS voters for each ESPS actuated component (such as a valve). For the ESPS actuated component to receive the ESPS signal, both of these output relays must be energized. Energizing both relays to provide an ESPS signal to the ESPS actuated component is designated as a Go test. If needed, these output relays may be energized one at a time without affecting the ESPS actuated component. Energizing the output relays one at a time is designated as a No-Go test. GSM screens are provided to allow de-energizing the reactor trip relays and for Go/No-Go testing.

Diagnostic testing and monitoring of the system can be performed via the TXS Service Unit. The TXS Service Unit communicates with all TXS processors via the MSI. The TXS Service Unit allows authorized personnel to access all the functions required to conduct detailed tests and functional tests for system commissioning as well as modifications, periodic testing, and for monitoring the digital RPS/ESPS after installation in the plant. Essentially these comprise the following tasks:

- Monitoring the system state
- Reading and acknowledging of error and state messages of the online system
- Modifying online parameters
- Performing periodic tests
- Error detection and fault diagnosis
- Central reloading of software after modifications

3.3.7.4 Actions on Failure Detection

Upon detection of hardware, software or input failures, the digital RPS/ESPS is designed to notify the CROs by Statalarms and by OAC alarms so that appropriate action can be taken. Plant operating procedures provide specific guidance to the CROs for appropriate alarm response.

3.3.8 Information Displays

> *IEEE Std 603-1998, Clause 5.8 indicates that:*
>
> *The information displays for manually controlled actions should include confirmation that displays will be functional (e.g., power will be available and sensors are appropriately qualified) during plant conditions under which manual actions may be necessary. Safety system bypass and inoperable status indications should conform with the guidance of RG 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."*

IEEE Std 603-1998 prescribes the system requirements for displays for manual operator action, system status indication, indication of bypasses, and location of information displays.

The TXS safety system is designed to provide signals to display systems in accordance with plant specific functional logic diagrams. Outputs to non-safety displays or status indication devices are supplied through qualified isolation devices. If the TXS safety system is operated in a "Bypassed" mode, an output is provided to interface with a bypassed status indication. Page 51 of the TXS SER (Reference 1) states: "The bypassed and inoperable status indication conforms to the guidelines of RG 1.47."

The Software Requirements Specification for the digital RPS/ESPS, describes all of the digital RPS/ESPS annunciator alarms (statalarms), Event Recorder and plant OAC point outputs. The annunciator alarms are located on existing Statalarm Panels SA1, SA5 and SA7. The preliminary configuration of the annunciator alarms for Statalarm Panel 1SA1 shown in Figure 3.3-1 is typical of Statalarm Panels SA5 and SA7. The OAC displays and the Event Recorder are located in the control room and accessible to the CRO. Lamp test push buttons are provided on the control room unit boards to manually test the statalarm lamps.

Figure 3.3-1 Typical Statalarm Panel 1SA1

1A RPS TRIP 1	1A LO PRESS TRIP 2	1A FLUX/FLOW/IMB TRIP 3	1A HI TEMP TRIP 4	1A VAR LO PRESS TRIP 5	1A HI PRESS TRIP 6	1A RCP/FLUX TRIP 7	1 NI-5 HI FLUX TRIP 8	1A RB HI PRESS TRIP 9	ES 1 TRIP 10	ES 5 TRIP 11	ICS STATALARM 12
1B RPS TRIP 13	1B LO PRESS TRIP 14	1B FLUX/FLOW/IMB TRIP 15	1B HI TEMP TRIP 16	1B VAR LO PRESS TRIP 17	1A HI PRESS TRIP 18	1B RCP/FLUX TRIP 19	1 NI-6 HI FLUX TRIP 20	1B RB HI PRESS TRIP 21	ES 2 TRIP 22	ES 6 TRIP 23	ICS STATALARM 24
1C RPS TRIP 25	1C LO PRESS TRIP 26	1C FLUX/FLOW/IMB TRIP 27	1C HI TEMP TRIP 28	1C VAR LO PRESS TRIP 29	1A HI PRESS TRIP 30	1C RCP/FLUX TRIP 31	1 NI-7 HI FLUX TRIP 32	1C RB HI PRESS TRIP 33	ES 3 TRIP 34	ES 7 TRIP 35	LPI STATALARM 36
1D RPS TRIP 37	1D LO PRESS TRIP 38	1D FLUX/FLOW/IMB TRIP 39	1D HI TEMP TRIP 40	1D VAR LO PRESS TRIP 41	1A HI PRESS TRIP 42	1D RCP/FLUX TRIP 43	1 NI-8 HI FLUX TRIP 44	1D RB HI PRESS TRIP 45	ES 4 TRIP 46	ES 8 TRIP 47	LPI STATALARM 48
CRD SEQUENCE FAULT 49	CRD TRIP BKR A TRIP 50	CRD TRIP BKR B TRIP 51	CRD TRIP BKR C TRIP 52	CRD TRIP BKR D TRIP 53	CRD ELECTRONIC TRIP E 54	CRD ELECTRONIC TRIP F 55	SPARE 56	DIVERSE LPI EMER OVERRIDE 57	DIVERSE LPI BYP 58	DIVERSE LPI TRIP 59	LPI STATALARM 60

As described in the Hardware Requirements Specification for the digital RPS/ESPS, the existing Main Control Board ESPS Channel Trip/Reset pushbuttons and the ESPS HPI and LPI Bypass pushbuttons and indicating lamps will be replaced with new components, but the existing functions will not change.

The RZ Module status indicating equipment of the existing ESPS will be replaced with new ES Device Status Panels that will indicate the status of each device actuated by the ESPS arranged by channel. These Status Panels provide status indication only. The Status Panels will have lamp test push buttons provided to manually test the lamps.

The RZ module control functions for those ESPS actuated field devices that could be controlled from the Vertical Boards are being replaced with new control switches and status lamps. In addition, new controls for other ESPS actuated field devices that were not previously controlled by RZ modules will also be provided. A select group of pump and valve controls has been identified by the ONS Operations group for relocation to an area on unit board UB2, where the old EHC controls were located and removed. The remaining controls will be located on the vertical boards, near the new status panels. The new switches and their locations are summarized below:

The following ESPS components will have new control switches installed on UB2 below the selector switches for ESPS Output Channel 1-8 Auto/Manual Control (described below):

- RB Spray Pump A
- RB Spray Pump B
- Valve BS-1 – RB Spray Header A Containment Isolation Valve
- Valve BS-2 – RB Spray Header B Containment Isolation Valve

- Valve LPSW-6 – RCP Motor Coolers Isolation Valve
- Valve LPSW-15 – RCP Motor Coolers Isolation Valve
- Valve CC-7 – Component Cooling Return Penetration Inside Block Valve
- Valve CC-8– Component Cooling Return Penetration Outside Block Valve
- Valve HP-20 – RCP Seal Return Valve
- Valve HP-21 – RCP Seal Return Isolation Valve (Control switch for HP-20 is relocated from UB1 to UB2)

The following ESPS Odd Channel components will have new control switches installed on VB2 below the new ESPS Odd Channel Status Panel:

- Penetration Room Ventilation Fan A
- Valve FDW-105 – Steam Generator A Sample Penetration Isolation Valve
- Valve FDW-107 – Steam Generator B Sample Penetration Isolation Valve
- Valve PR-7 – RB Radiation Monitor Inlet Valve
- Valve PR-9 – RB Radiation Monitor Outlet Valve
- Valve RC-5 – Pressurizer Steam Sample Valve
- Valve RC-6 – Pressurizer Water Sample Valve

The following ESPS Even Channel components will have new control switches installed on VB2 below the new ESPS Even Channel Status Panel:

- Penetration Room Ventilation Fan B
- Valve FDW-106 – Steam Generator A Sample Penetration Isolation Valve
- Valve FDW-108 – Steam Generator B Sample Penetration Isolation Valve
- Valve PR-3 – RB Purge Control Valve
- Valve PR-8 – RB Radiation Monitor Inlet Valve
- Valve PR-10 – RB Radiation Monitor Outlet Valve
- Valve RC-7 – Pressurizer Sample Outside Isolation Valve

New Auto/Manual pushbutton switches will be provided on the Oconee Main Control Room Unit Boards to replace the existing individual Auto/Manual pushbuttons on the Bailey RZ modules. These pushbutton switches control all of the ESPS actuated devices on a channel basis (ESPS Automatic Actuation Output Logic Channel 1 through 8 and Keowee Load Shed 1 and 2), rather than control the devices on an individual basis as is currently designed. These new switches will be installed on the UB2 control board. Each pushbutton switch will include LEDs to indicate that either the Auto or Manual mode is selected. If an ESPS actuation signal (automatic or manual) is not present, the Auto/Manual pushbutton switches have no control function and the indicating LEDs will be off. Once an ESPS actuation signal is initiated, either from an automatic system demand actuation or by operator manual initiation actuation, the Auto light will be illuminated and the Auto/Manual pushbutton functions may then be selected from this control point. With the Auto/Manual pushbutton in Auto, the ESPS operates in the safeguards control mode. However, if it is desired to take manual control of the ESPS channel or the individual associated actuated components for that channel, the Manual mode can be selected. When the Manual mode is selected, the individual actuation components in that associated channel may then be operated from the normal component control switch. If Manual has been selected and the operator wishes to place the channel components back in the ES position, the operator can push the Auto pushbutton and the channel components will go to the ES position. Once an ESPS channel has been reset using the Reset pushbutton, the Auto/Manual LEDs for that channel will go out and the Auto/Manual pushbuttons will no longer respond.

The Load Shed logic Channels 1 and 2 will have separate Auto/Manual pushbutton selector switches from the switches used to select Manual for the balance of the ESPS Output Channel 1 and 2 components. The Load Shed 1 and 2 switches are installed on UB2 control board below the Auto/Manual switches for ESPS logic channels 1 and 2. These selector switches will allow the Load Shed permissive logic to remain enabled even if the operator places the ESPS Channels 1 or 2 Auto/Manual switches in the Manual mode. This gives the operator the ability to take manual control of the ESPS Channel 1 or 2 components while maintaining the Load Shed logic in an actuated state if normal power sources are not available. Allowing separate action to take manual control of ESPS Output Channel 1 or 2 components versus taking manual control to clear the Load Shed signal from ESPS is consistent with the actions that are required with the existing ESPS.

New Override/Reset control switches and indicating lamps (Odd and Even) will be provided on the Unit Boards. New annunciator and computer points will be provided.

The new DLPIAS will provide Bypass/Enable and Override/Reset control switches and indicating lamps, as well as new annunciator alarm windows. These new controls will be located near the existing LPI and HPI Bypass pushbuttons and indicating lamps on the Unit Boards.

Although the statalarm panels are being rearranged, no new information displays for NI, the NI recorders, or the RCPPMs are introduced.

All replacement indicating light assemblies, device indicating lights and Status Panel lamps will utilize LEDs. The RPS/ESPS cabinets will provide the 24 V direct current (DC) power for illuminating the ES Status Panels, pushbutton lamps and device position indication lamps. For ESPS actuated field devices where control board status indication is fed from the ESPS Normal Control Cabinets, the wetting voltage for field device position comes from the battery-backed vital 1E 120 VAC power source of the same division.

When a Shutdown or Manual Bypass keyswitch is operated, an annunciator alarm is displayed on the Statalarm Panel and provided to the OAC for continuous indication of the bypassed condition. Shutdown and Manual Bypasses are described in Sections 3.3.16.6 and 3.3.16.7 of this Enclosure.

The Statalarm Panels and Event Recorders are classified as Non-1E and are electrically isolated by Class 1E optical couplers.

The location of the information displays discussed above to support manual operator actions during a DBE have been previously reviewed as part of the RG 1.97 review and NUREG-0737 Control Room Design Reviews for ONS. In addition, Human Factors reviews are conducted throughout the detailed design process to ensure that no adverse impacts on the operators are introduced by this design change. Refer to 3.3.14 of this Enclosure for additional details.

3.3.9 Control of Access

> *IEEE Std 603-1998, Clause 5.9 states:*
>
> *"The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof."*

The ONS digital RPS/ESPS contains design features that provide means to control physical access to protection system equipment, including access to test points and the means for changing setpoints. The description of these design features is considered by Duke to be sensitive information and to be withheld from public disclosure pursuant to 10 CFR 2.390.

Duke submitted descriptions of the cyber security features of the digital RPS/ESPS that demonstrate that the applicable cyber security requirements have been met by letter dated January 30, 2008. This letter is incorporated by reference pursuant to 10 CFR 50.32.

3.3.10 Repair

> *IEEE Std 603-1998, Clause 5.10 states:*
>
> *"The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment."*

The digital RPS/ESPS is designed with features to detect both hardware and software faults and to assist in diagnostic and repair activities. The self-test features are designed consistent with the guidance presented in BTP HICB-17, "Guidance on Self-Test and Surveillance Test Provisions" (Revision 4 was in effect at the time the topical report was written).

The digital RPS/ESPS automatically detects most failures in the subracks, the function processors, the I/O modules, and the communication functions. Failures that affect the subrack internal power supplies or control of the backplane bus will result in an indication of a predefined fault condition (e.g., reset) on the function computers. The cause of failure and other status information are stored in the function processors.

These monitoring capabilities ensure the detection of function processor failures that could affect safety system operations. Detected failures always cause the signals concerned to be excluded from further processing.

The majority of failures concern signal input or output channels. If a multiplexer or a converter component fails, the entire module is affected. In unusual cases, a failure in the interface can also affect the backplane. Failures of LEDs and other signaling equipment do not affect the safety function of the system. The use of voting, which uses redundant signals to arrive at a safety state, provides assurance that a single failure in an I/O module will not disable the safety function because redundant channels are provided.

Additionally, the TXS system monitors cabinet temperatures and cabinet cooling fan speed and provides the plant operators with an alarm if setpoints are exceeded.

The hardware and software fault detection features for the ONS digital RPS/ESPS application are the same as those described in the TXS Topical Report. The NRC previously docketed their acceptance of these features in the TXS SER (Reference 1). These features are described on pages 28 and 29 of the SER.

Monitoring of non-TXS components, such as the Absopulse power supplies, bipolar power supplies, and detector power supplies, is accomplished through the monitoring of the signals dependent on those components. For example, if a signal fault is detected in one of the NI power supplies, the NI Power Supply Fail Statalarm is lit.

In general, TXS modules are replaced rather than repaired when equipment problems occur. Some non-TXS equipment, such as lamp boxes, may be repaired in the field. Repair and replacement guidelines for TXS modules and for non-TXS equipment are included in maintenance manuals and procedures.

3.3.11 Identification

IEEE Std 603-1998, Clause 5.11 states:

"In order to provide assurance that the requirements given in this standard can be applied during the design, construction, maintenance, and operation of the plant, the following requirements shall be met:

a) Safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1992 and IEEE Std 420-1982.
b) Components or modules mounted in equipment or assemblies that are clearly identified as being in a single redundant portion of a safety system do not themselves require identification.
c) Identification of safety system equipment shall be distinguishable from any identifying markings placed on equipment for other purposes (e.g., identification of fire protection equipment, phase identification of power cables).
d) Identification of safety system equipment and its divisional assignment shall not require frequent use of reference material.
e) The associated documentation shall be distinctly identified in accordance with the requirements of IEEE Std 494-1974 [B9].
f) The versions of computer hardware, programs, and software shall be distinctly identified in accordance with IEEE Std 7-4.3.2-1993."

The digital RPS/ESPS is configured in accordance with ONS plant specific identification requirements. A brief description of some of the methodologies is provided below.

The identification (ID) Coding Concept document (Refer to Item 12 of Table 1-2 of this Enclosure) provides a standardized method for identifying equipment, diagrams and signals for the purpose of continuity in identification during the project development process and beyond. This document defines the rules for the assignment of ID codes to:

- I&C equipment,
- I&C diagrams, and
- I&C signals.

The rules and methodology prescribed by the ID Coding Concept document are essential design input to the development of the ONS digital RPS/ESPS software. Further description of software coding is contained in Section 3.4.11 of this Enclosure. Some examples of ID conventions are described below in this section; a full description can be found in the ID Coding Concept Document.

All equipment is identified by ID codes. When naming new equipment, standard equipment abbreviations are used as a guideline. The ID coding of existing field equipment is based on the original Duke Energy ID assigned for the field devices. For example, for the Unit 1 HPI Pump 1, the ID would be coded as follows:

ONS Unit = 1
High Pressure Injection = HPI
Pump = PU (according to the standard equipment abbreviations used)
Pump number = 0001

And thus the ID becomes 1HPIPU0001.

The eighteen ONS RPS/ESPS cabinets are numbered sequentially as follows, where the first position is unit number, and PPSCA stands for Plant Protective System Cabinet:

Cabinet Number	Cabinet Function
1PPSCA0001	RPS Channel A, ESPS Channel A1
1PPSCA0002	RPS Channel A, ESPS Channel A1
1PPSCA0003	RPS Channel B, ESPS Channel B1
1PPSCA0004	RPS Channel B, ESPS Channel B1
1PPSCA0005	RPS Channel C, ESPS Channel C1
1PPSCA0006	RPS Channel C, ESPS Channel C1
1PPSCA0007	RPS Channel D
1PPSCA0008	RPS Channel D
1PPSCA0009	ESPS Channel A
1PPSCA0010	ESPS Channel B
1PPSCA0011	ESPS Channel C
1PPSCA0012	ESPS Odd Voter 1
1PPSCA0013	ESPS Odd Voter 2
1PPSCA0014	ESPS Even Voter 1
1PPSCA0015	ESPS Even Voter 2
1PPSCA0016	RPS-Channel E, MSI, DLPIAS, DHPIAS
1PPSCA0017	ESPS Odd Component Status
1PPSCA0018	ESPS Even Component Status

The ONS digital RPS/ESPS CPUs are given four (4) digit ID codes. The systematic naming scheme used for the CPU-ID is:

```
Pos. 1 2 3 4
     | | | |
     | | | |___Number
     | | |___Cabinet
     | |___Set
     |___Unit (1, 2, 3)
```

The numbers in Position 2 and Position 3 are assigned per the following table:

	POS. 2 = 0	**1**	**2**	**3**	**4**	**5**	**6**
POS. 3 = 1	MSI/RPS-E	RPS-A	RPS-B	RPS-C	RPS-D	VOTER Odd 1	VOTER Even 1
2	GW	ESF-A	ESF-B	ESF-C		VOTER Odd 2	VOTER Even 2
3	SU					STATUS Odd	STATUS Even

For example, the following sample CPU-IDs are shown for Unit 1:

- 1012 ONS-1, MSI, CPU 2
- 1121 ONS-1, ESF-A, CPU 1
- 1312 ONS-1, RPS-C, CPU 2
- 1511 ONS-1, Voter Odd 1, CPU 1
- 1631 ONS-1, Status Even, CPU 1

Power and control cables are color coded to identify their use and/or channel association. Standard color assignments for cables that are ESPS and RPS related are:

- Gray cables are used for Vital Power Panel Boards 1KVIA, ESPS Output Logic Channels 1, 3, 5 and 7 [Odd], ESPS Input Channel A, and RPS Channel A.
- Yellow cables are used for Vital Power Panel Boards 1KVIB, ESPS Output Logic Channels 2, 4, 6 and 8 [Even], ESPS Input Channel B, and RPS Channel B.
- Blue cables are used for Vital Panel Boards 1KVIC, components actuated from ESPS Odd/Even Channels, ESPS Input Channel C, and RPS Channel C.
- Orange cables are used for Vital Power Panel Boards 1KVID, RPS Channel D.

Color coding and physical installation of the digital RPS/ESPS power and control cables follows the existing ONS standards described above, thus meeting existing cable separation requirements. For example, the digital ESPS is also divided into two divisions or voter sets: Odd and Even. The Odd division uses gray cables and the Even division uses yellow cables. ES components that are actuated by either the Odd or the Even division use blue cables. The Even division is responsible for actuating the Even (yellow) components as well as the same six Odd/Even (blue) components (for Units 1 and 2 only) on an ESPS actuation. Similarly, the Odd division is responsible for actuating the Odd (gray) components as well as the same six Odd/Even (blue) components. The six components actuated from the Odd and Even Voters are HPI Pump B, LPSW Pump C for Unit 1 (LPSW Pump A for Unit 2), RBCU B, and LPSW valves 6, 15, and 21.

The TXS Software Engineering Tools also document the hardware and software in the form of diagrams, which are identified by ID codes. SPACE diagrams are distinguished by diagram type. For additional information on SPACE diagrams, see Section 3.4.11 of this Enclosure for additional information on ID coding of the digital RPS/ESPS software.

3.3.12 Auxiliary Features

> *IEEE Std 603-1998, Clause 5.12 states:*
>
> *"Auxiliary supporting features shall meet all requirements of this standard. Other auxiliary features that perform a function that is not required for the safety systems to accomplish their safety functions, and are part of the safety systems by association (i.e., not isolated from the safety system) shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level. Examples of these other auxiliary features are shown in Figure 3 and an illustration of the application of this criteria is contained in Annex A."*

Duke is not adding any new auxiliary features to the ONS. Those auxiliary features (e.g., cabinet power supplies) that are currently a part of the analog RPS/ESPS that are being replaced as a result of the RPS/ESPS digital upgrade comply with IEEE Standards and with standards applicable to the RPS/ESPS digital upgrade.

3.3.13 Multi-unit Stations

> *IEEE Std 603-1998, Clause 5.13 states:*
>
> *"The sharing of structures, systems, and components between units at multi-unit generating stations is permissible provided that the ability to simultaneously perform required safety functions in all units is not impaired. Guidance on the sharing of electrical power systems between units is contained in IEEE Std 308-1991. Guidance on the application of the single failure criterion to shared systems is contained in IEEE Std 379-1994."*

The RPS and ESPS are not shared between the ONS Units. The RPS/ESPS design change doesn't modify the initiation logic for any existing systems shared between units, such as, the Low Pressure Service Water System and the Keowee Hydro Units.

3.3.14 Human Factors Considerations

> *IEEE Std 603-1998, Clause 5.14 states:*
>
> *Human factors shall be considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Std 1023-1988.*

The Duke/ONS design change process requires that a Control Room Impact Evaluation be completed in conjunction with any station design change that affects a unit's control room. This evaluation includes Human Factors Engineering (HFE) reviews and Human-System Interface (HSI) reviews in accordance with the ONS Human Factors Engineering Procedure. The review guidelines of this procedure are consistent with NUREG 0700, "Human-System Interface Design Review Guidelines," Revision 2, 2002 (Reference 8), and NUREG 0711, "Human Factors Engineering Program Review Model," Revision 1, 2002 (Reference 9). The initial HFE review has been documented in a completed HFE Review Form for Plant Changes, which is an attachment to the HFE Procedure. Subsequent human factors reviews, which are done as part of the design process, are also performed and documented in accordance with the HF Engineering Procedure.

RPS and ESPS Replacement Project Specifications contain requirements to ensure compatibility with existing plant Operations, Maintenance, and Engineering configurations for HSI displays, indications and alarms. Project design change documents, HFE/HSI design reviews, and the HFE Task Analysis address those specification requirements. The results of the final reviews support compliance with RPS and ESPS Replacement Project Specifications and will be documented in the ONS design change Design Input Calculations per ONS Engineering Directives and department directive requirements.

Limited changes are being made to the control room as described in Section 2 of this Enclosure. From a human factors viewpoint the old and new designs are very similar.

A description of the initial reviews and the results is provided below.

3.3.14.1 Initial Operations Panel Review

An "Operations Panel" was created during the early stages of the ONS digital RPS/ESPS design development. The panel, made up of ONS engineering, operations and maintenance personnel, and equipment supplier personnel, was charged with an early integrated review of impacts to the control room.
The Operations Panel reviewed the initial plans to assess impact to the main control room control boards, the existing RZ Modules (ES actuated equipment controls) and the control room Statalarm annunciator panels. Although much of the scope information available for these early reviews was of a preliminary nature, it allowed the ONS Operations, Maintenance and System Engineering organizations to effectively review and comment early in the hardware design process.

This proactive approach to early design review effectively identified HFE design preferences associated with operator tasks that could potentially hinder human performance. Identifying HFE design preferences during the initial scoping phase provided a basis for changing the system design at a time that resulted in minimal design impact. The results of the corrective actions taken to resolve these HFE design preferences were reflected in subsequent HFE/Design Reviews. The documentation for this Operations Panel Review, which includes the RPS/ESPS Overview summaries and Unit control room Statalarm panel windows, identifies changes to the system operation and controls presented during the review. Additionally, interviews with Operations, Maintenance and System Engineering personnel who are familiar with these systems and have an understanding of the intended design change were conducted as part of the discussions. Continued involvement of these personnel throughout the design development process ensures that no new HFE concerns are introduced. These continuing reviews will be documented as part of the design and HFE review process, and will be captured in the Design Input Calculations in accordance with ONS requirements.

The HFE review applies to all of the individual elements of the proposed design.

The HFE/HSI review process, as implemented for the ONS RPS/ESPS digital upgrade, is divided into three phases:

1. Phase I consisted of the early design reviews of the digital RPS/ESPS as described above, and operating experience reviews. The results of the operating experience review are described in more detail below.
2. Phase II consisted of an IDR - HFE Review, which was completed on May 24, 2005, and an Operations Task Analysis Review, which was completed in October 2005. This review included detailed review of the new ES status panels, ES system/component controls, and RPS/ESPS annunciators. The results of this phase are also summarized below.
3. Phase III is an ongoing effort that will last throughout the design change process for the RPS/ESPS digital upgrade. This effort is an integral part of the final modification design and will incorporate the following items:
    - Review of the proposed HSI for incorporation of good HFE design practices.
    - Revisions to Operations, Maintenance, and other technical support procedures.
    - Coordination of simulator upgrades, Emergency Operating Procedures, training module development, and personnel familiarization and training sessions to support the implementation schedule.
    - Final review of proposed design, control/operation and outputs to Statalarms, OAC points and ICS input.
    - Completion of the project FMEA.
    - Final 100% review of the design change by the ONS Control Room Improvement Team.

    Final documentation of the reviews and results becomes an attachment to the design input calculation when the final design change package is assembled.

3.3.14.2 Operating Experience Review (OER)

An OER was performed to identify and analyze HFE-related issues. The objective was to identify any relevant plant specific or industry wide operating experience problems and issues encountered previously in designs and human tasks that were similar to the planned ONS design change.

There are 22 nuclear applications using the TXS design platform worldwide. The proposed design change for ONS is the first installation of a digital RPS/ESPS in the United States. Because of this, there is very little specific RPS/ESPS digital OE. There are, however, many safety-related and non-safety related digital control systems currently operating in US nuclear power plants in other applications. OE identified for those systems was included in the review. The following ONS plant specific, AREVA NP, and industry information sources were reviewed:

- >100 Problem Investigation Process (PIP) System PIPs
- AREVA NP Condition Report Database, described in AREVA NP procedure 1717-06, Corrective Action Program
- The ONS Digital Control Rod Drive Control System (DCRDCS) Project Lessons Learned Briefing
- INPO Significant Event Notifications/Reports and INPO Significant Operating Experience Reports (approximately 600 total events)
- 19 NRC Generic Letters
- 12 NRC Bulletins
- 172 NRC Information Notices
- 300 NRC License Event Reports
- 6 NRC Human Factors Information System events

Applicable items related to digital control systems have been provided to the RPS/ESPS Project Team for their review and have been considered as part of the plant specific design development.

3.3.14.3 Integrated Design Review - HFE Review

An Integrated Design Review (IDR) – HFE Review for the RPS/ESPS Replacement Project was held on May 24, 2005. The review team consisted of representatives from ONS Engineering, Operations, Maintenance, Licensing, Training and Project Management groups, and procedure writers. Representatives from the architect/engineer (A/E) organization participated as well.

The IDR team discussed topics relevant to HFE considerations and made design recommendations and suggestions for additional reviews. The discussions included

the location and functions of the new Manual/Auto Function buttons and emergency override switches, GSM screen indications, and indication light functionality.
The results of these discussions were considered and incorporated into the digital RPS/ESPS design as appropriate.

3.3.14.4 Operations Task Analysis Review

A Task Analysis evaluation of the digital RPS/ESPS was performed by Operations based upon drawings and technical information provided by AREVA NP. Rather than use existing Operating Procedures as a basis for performing the task analysis, Operations defined and analyzed the functions, or sets of tasks, associated with the system.

The task analysis focused on the RPS/ESPS inputs, loss of ESPS analog and digital power, loss of RPS power, ESPS and RPS bistable operation, RPS actuation, RPS function trip, RPS manual and shutdown bypasses, turbine and feedwater pump trips, ESPS actuation and ESPS component manipulation, and ESPS HPI and LPI bypasses. The task analysis described areas where the new digital RPS/ESPS closely matches the existing system, and pointed out differences from an Operations perspective. The task analysis illustrated the need for operators to be trained on the new system, with special notice of the new status panels and channel manual control buttons. The training described in Section 3.6.2 of this Enclosure addresses this concern.

Since operator staffing was not impacted, the evaluation did not address this aspect of NUREG-0711.

3.3.14.5 Conclusion

The results of the HFE reviews described above were considered and appropriate changes were made to the digital RPS/ESPS design and associated training, procedures and other documents.

3.3.15 Reliability

> *IEEE Std 603-1998, Clause 5.15 states:*
>
> *"For those systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis. Guidance on the application of this criteria for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993."*

One of the quality requirements for a safety I&C system is the reliability with which it performs its assigned safety functions. To assess this reliability, two complementary methods for analysis are used: the probabilistic analysis and the deterministic reliability analysis. Probabilistic analysis is used to quantify the reliability, with "non-availability on demand" used as the standard measure. "Non-availability on demand" is defined as the probability of a given system not being able to perform its safety function when it is called upon. This quality characteristic is used as a measure for assessing different equipment designs.

A detailed hardware reliability analysis was performed following the guidance of IEEE Std 352-1987 and IEEE Std 577–1976. The analysis uses failure rate data specific to the TXS components being used for the digital RPS/ESPS.

The hardware reliability analysis provides a study of the expected reliability of the RPS/ESPS TXS system hardware and documents the TXS system's susceptibility to various types of faults. Both qualitative analysis and quantitative analysis are utilized to identify the possible failure modes, for determining methods for eliminating or reducing the frequency or consequences of the postulated failures, and for calculating the probabilities of failures and estimates of reliability and availability. The results of the TXS hardware availability analysis show that the reliability/availability of the proposed digital RPS/ESPS is greater than those values assumed in the Probabilistic Risk Assessment and accident analysis of the existing systems. Based on the conservative calculations and analyses recorded in the TXS hardware reliability analysis, the digital RPS/ESPS are shown to have high reliability and availability compared to the currently installed system.

The results of the hardware reliability analysis also support extending the surveillance testing interval for channel functional tests to once per 18 months (refer to Enclosure 3 of this LAR), since the hardware availability analysis was based on assuming a 24 month surveillance testing interval.

The scope of the RPS/ESPS hardware is defined as the input sensor/signal termination points (terminal blocks), the protective channel sets (input signal function modules and isolation modules), the protective channel set computers, the ESPS actuation computers (Voters), the output function modules, the RPS reactor trip relay sets and associated contacts, and the ESPS interposing relays and associated contacts.

Software does not "fail" in the conventional way a hardware component might fail. Per RG 1.152, Revision 2, the NRC does not endorse the concept of quantitative reliability goals as a sole means of meeting its regulations for reliability of digital computers used in safety systems. A qualitative study of the reliability for the TXS software has been documented in the FMEA for the digital RPS/ESPS.

In summary, the reliability analyses of the digital RPS/ESPS were performed using qualitative and quantitative methods, incorporating probabilistic and deterministic reliability considerations. The NRC previously docketed their acceptance of these methods in the TXS SER (Reference 1). Page 50 of the SER provides the following assessment:

> "Reliability has been assessed with both probabilistic and deterministic reliability analyses. The probabilistic analysis has been used to quantify the non-availability on demand. The staff has reviewed these calculations; however, the staff does not use probabilistic and deterministic reliability analyses as the sole means of determining acceptability of a safety system. The calculations are related only to the hardware aspects of the TXS system; however, confirmatory testing performed by Siemens and GRS included the software. The deterministic analysis based on codes and standards delineates postulated failures that the system will be able to withstand."

3.3.16 Sense and Command Features – Functional and Design Requirements

3.3.16.1 Automatic Control

> *IEEE Std 603-1998, Clause 6.1 states:*
>
> *"Means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4, item e). The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in Clause 4, item e) following the onset of each design basis event. At the option of the safety system designer, means may be provided to automatically initiate and control those protective actions of Clause 4, item e)."*

The TXS platform is designed to work in cooperation with plant specific functional logic to automatically initiate and execute protective actions, with precision and reliability, for the range of conditions specified. In order to complete a plant specific design, an evaluation must be performed to identify the existing setpoints, margins, errors, and response times to ensure that existing plant safety analysis assumptions are enveloped.

For the RPS/ESPS digital upgrade, relevant setpoints, margins, errors and response times required for input to the digital RPS/ESPS design are provided in the ONS System Functional Description (Table 1-2 of this Enclosure, Item 36), the RPS Replacement Project Specification (Table 1-2 of this Enclosure, Item 38), the ESPS Replacement Project Specification (Table 1-2 of this Enclosure, Item 37), Unit 1 Parameter Calculation (Table 1-2 of the Enclosure, Item 45), and ONS Uncertainty

Calculations (Table 1-2 of this Enclosure, Items 28, 29, 31, 33, and 35). The digital RPS/ESPS is designed to operate within the bounds of the requirements provided in these documents so that the assumptions used in the existing safety analyses are not invalidated.

The digital RPS/ESPS automatically initiates all required protective actions needed to mitigate DBEs except for those that credit manual actuations for mitigation. Credited manual actuations do not rely on any information processed by the digital RPS/ESPS.

The automatic control features for the digital RPS/ESPS are based on the standard TXS platform described in the TXS Topical Report (Reference 2). The NRC previously docketed their acceptance of these features in the TXS SER (Reference 1). Page 50 of the SER provides the following assessment:

> "The TXS meets the automatic and manual control requirements. Failure of the automatic controls does not interfere with the manual controls."

3.3.16.2 Manual Control

> *IEEE Std 603-1998, Clause 6.2 states:*
>
> *"Means shall be provided in the control room to*
> *a) Implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1.*
> *b) Implement manual initiation and control of the protective actions identified in Clause 4, item e) that have not been selected for automatic control under 6.1. The displays provided for these actions shall meet the requirements of 5.8.1.*
> *c) Implement the manual actions necessary to maintain safe conditions after the protective actions are completed as specified in Clause 4, item j). The information provided to the operators, the actions required of these operators, and the quantity and location of associated displays and controls shall be appropriate for the time period within which the actions shall be accomplished and the number of available qualified operators. Such displays and controls shall be located in areas that are accessible, located in an environment suitable for the operator, and suitably arranged for operator surveillance and action."*

The generic TXS platform is designed to work in cooperation with plant specific functional logic requirements for manual controls. Manual controls enable the operator to initiate protective actions at the division or system level, as well as for individual components. Information displays are independent of the digital RPS/ESPS and provide the operator with information necessary to manually perform reactor trips, ES actuations, post-accident monitoring or safe shutdown functions. A failure in the digital RPS/ESPS does not prevent manual actuation of the plant protective functions.

The overall design for the digital RPS/ESPS incorporates manual controls for reactor trip at the system level, and emergency safeguards actuation at the channel and individual component levels. Requirements to perform manual operator actions remain minimal.

3.3.16.2.1 RPS Manual Control

Manual actuation of reactor trip is performed by a hard-wired pushbutton located on the Main Control Board. Manual Reactor Trip bypasses the digital RPS trip logic and sends a reactor trip signal directly to the control circuits of the trip breakers.

RPS shutdown and manual bypasses are discussed below in Sections 3.3.16.6 and 3.3.16.7 of this Enclosure.

3.3.16.2.2 ESPS Manual Control

The design allows the CROs to take manual control of ESPS actuated components on a channel basis as well as an individual basis. Depressing an ESPS channel manual Trip/Reset pushbutton will send a Trip signal to the associated ESPS channel in two ways: (1) via an input to the ESPS channel logic, and (2) directly to the associated channel output relays, bypassing the ESPS. The manual or automatic Trip signal can be reset by depressing the associated channel Reset button. The ESPS manual actuation paths do not pass through the TXS software, and therefore are not dependent on the correct functioning of the software.

Manual control of individual ESPS actuated components is provided using newly configured Auto/Manual switches that bypass the TXS platform. Each of the eight ESPS logic channels will have an individual Auto/Manual selector switch. Once an ESPS signal is actuated, the Auto light on this switch is illuminated while automatic ESPS operations proceed to completion.

ESPS Channels 1 and 2 also initiate Load Shed (Keowee); however, the design provides separate Auto/Manual Load Shed switches that will allow the Load Shed logic to remain enabled even if the CRO selects Manual on the Auto/Manual switch for ESPS Channels 1 and 2.

If it is necessary to take manual control of an individual component, the logic channel Manual mode may be selected, after which the individual components associated with that channel may be operated from their normal component control switches. Replacement control switches are provided for the following components:

- Odd ESPS Channel actuated components: PR-1A, FDW-105, FDW-107, PR-7, PR-9, RC-5, RC-6
- Even ESPS Channel actuated components: PR-1B, FDW-106, FDW-108, PR-3, PR-8, PR-10, RC-7
- Other ESPS actuated devices: RBSP-A, RBSP-B, BS-1, BS-2, CC-7, CC-8, HP-20, HP-21, LPSW-6, LPSW-15

A new ESPS Emergency Override feature is added so that the CROs can take control of all ESPS actuated devices in the event of an inadvertent ESPS actuation resulting from a failure of the digital ESPS (e.g., SWCMF). Two new Emergency Override pushbuttons (one Odd and one Even) will be installed on UB2 near the new ESPS Auto/Manual pushbuttons.

Existing HPI and LPI bypass capabilities are retained in the ONS digital ESPS.

Manual initiation of HPI is accomplished with the existing ESPS Channel 1 and 2 Trip/Reset buttons located on the main control board. Likewise, manual initiation of the LPI is accomplished with the existing ESPS Channel 3 and 4 Trip/Reset buttons located on the main control board. The logic for this manual initiation bypasses the ESPS logic and allows the CRO to initiate the required actuation on a per channel basis.

ESPS shutdown and Voter manual bypasses are discussed in Sections 3.3.16.6 and 3.3.16.7 of this Enclosure.

3.3.16.3 Interaction between the Sense and Command Features and Other Systems

IEEE Std 603-1998, Clause 6.3 states:

"6.3.1 Requirements

Where a single credible event, including all direct and consequential results of that event, can cause a non-safety system action that results in a condition requiring protective action and can concurrently prevent the protective action in those sense and command feature channels designated to provide principal protection against the condition, one of the following requirements shall be met:

1. *Alternate channels not subject to failure resulting from the same single event shall be provided to limit the consequences of this event to a value specified by the design basis. Alternate channels shall be selected from the following:*
   - a. *Channels that sense a set of variables different from the principal channels.*
   - b. *Channels that use equipment different from that of the principal channels to sense the same variable.*
   - c. *Channels that sense a set of variables different from those of the principal channels using equipment different from that of the principal channels.*
2. *Equipment not subject to failure caused by the same single credible event shall be provided to detect the event and limit the consequences to a value specified by the design bases. Such equipment is considered a part of the safety system.*

6.3.2 Provisions

Provisions shall be included so that the requirements in 6.3.1 can be met in conjunction with the requirements of Section 6.7 if a channel is in maintenance bypass. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel".

The TXS Topical Report (Reference 2) and associated SER (Reference 1) provide generic information about the TXS system, showing compliance with the criteria, based on overall system design.

The TXS, together with the plant specific functional logic requirements, use a number of strategies to ensure a single credible failure, will not result in a non-safety system action causing a condition requiring protective action and concurrently prevent the protective action in those channels designated to provide protection against the condition. These strategies include the following:

- Isolating the protection system from channel failure by providing additional redundancy.
- Isolating the control system from channel failure by using data validation techniques to select a valid signal for control system actuation.
- Electrical isolation techniques to prevent credible faults from propagating to redundant channels.

The NRC SER states:

> "In the TXS system design, signals interact between redundant Class-1E channels and transmit from Class-1E channels to non-Class-1E devices. The communication between Class-1E channels uses end-to-end fiber optic cables found acceptable in previous license applications in the United States. The communication from the safety I&C system to the non-safety plant information system is done via the MSI. The MSI serves as a means of isolation within the TXS architecture. For the upgrade of existing analog instrumentation and control systems in United States nuclear power plants, there is a need to provide an interface between Class-1E and non-class-1E systems by means of both analog signal and relay contacts. For these applications, Siemens will qualify an analog isolation device and a mechanical relay to provide adequate coil-to-contact isolation. This qualification will be performed in accordance with the Class-1E to non-Class-1E isolation requirements of EPRI TR-107330. This is a plant-specific action item."

The digital RPS/ESPS provides isolated signals to the ICS.

The digital RPS/ESPS FMEA analyzes interconnections and means of isolation between redundant safety channels and circuits and between non-safety and safety channels and circuits to assure that no single failure can cause the loss of a safety function or spurious actuations. Refer to Section 3.7, Failure Modes and Effects Analysis, of this Enclosure. Devices used for class 1E isolation have been qualified (by analysis and evaluation) to prevent electrical faults from propagating between redundant class 1E circuits and between class 1E circuits and non-1E circuits. The FMEA analyzes failures in non-safety systems, including non-safety test circuitry, to assure that no single failure can cause the loss of a safety function or lead to spurious ESPS actuations. The software communication structure and checking also prevent hardware failures which result in keeping software errors from affecting the TXS safety functions.

IEEE Std 603-1998, Section 6.3.2 states that a single failure must be considered in addition to a maintenance bypass. The FMEA specifically addresses the consequences of single failure, as required by Sections 6.3.1 and 6.3.2 of IEEE Std 603-1998. The FMEA is performed to assure that the single failure criterion is met assuming the Bypassed channels cannot provide the safety function.

Regarding failures outside the RPS/ESPS cabinets, the TXS system uses signal validation techniques where possible to identify faulted signals and remove them from further processing of that parameter by all protective channels. In addition, each protective channel compares its various analog input signals to corresponding signals provided by other protective channels via fiber optic communications and selects the 2.MAX or 2.MIN analog signal for continued processing against the setpoint trip function. These techniques minimize the impact of failures upon system operation.

There are no failures of the ICS which will cause the loss of a safety function of the RPS/ESPS, considering one channel to be in maintenance bypass..

3.3.16.4 Derivation of System Inputs

IEEE Std 603-1998, Clause 6.4 states:

"To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis."

The process variables and derived parameters used for the TXS RPS/ESPS actuation functions are the same as those currently being used at ONS for the Bailey RPS and Bailey ESPS and do not change from those used by the current safety analysis.

The inputs for the RPS are derived from the following parameters (refer to UFSAR Section 7.2.2.3):

- Reactor Power (Neutron Flux Level)
- Reactor Coolant System (RCS) Flow
- RCS Pump Monitor Logic
- RCS Pressure - Narrow Range
- RCS Outlet Temperature
- RB Pressure
- Main Turbine Trip
- Loss of Main Feedwater (Pump Turbine Hydraulic Oil Pressure)

The ESPS monitored variables include:

- RCS Pressure
- RB Pressure (Transmitters and Switches)

Although the process variables and derived parameters have not changed, other minor changes have been made to enhance the system capabilities. The changes are briefly described below.

Additional RPS inputs for the RCPPM circuits have been provided to make the system single failure proof. The parameters measured are the same as before, but redundancy has been added to increase reliability.

Also, enhancements have been made to the ESPS controls which are used after actuation. These consist of minor changes in selection of manual operation after an actuation has occurred. The changes are intended to reduce operator burden following an actuation where manual control of components is necessary. Some of these changes require additions of signal inputs, including control switch contacts. No process variables are added as inputs for this change.

Finally, enhancements have been made to provide additional self-check features for the RPS/ESPS. No process variables are added as inputs for this change.

The changes to RPS/ESPS listed above do not change the credited process variables and derived values in the current safety analysis.

3.3.16.5 Capability for Testing and Calibration of System Inputs

> *IEEE Std 603-1998, 6.5 states:*
>
> *The most common method used to verify the availability of the input sensors is by cross checking between redundant channels that have available instrumentation signal displays. When only two channels of signal displays are provided, the applicant/licensee should state the basis used to ensure that an operator will not take incorrect action when the two channel signals differ. The applicant/licensee should state the method to be used for checking the operational availability of non-indicating sensors. SRP Chapter 7, BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," discusses issues that should be considered in sensor checks and surveillance tests for digital computer I&C systems.*

The TXS RPS/ESPS is designed so that TS requirements for testing and calibration of system inputs are satisfied.

3.3.16.5.1 Capability for Channel Checks

The digital RPS/ESPS provides automatic analog and binary process signal monitoring for signal failure (Fault) and for Channel Deviation. If a channel fails the acceptance criteria, it is alarmed (OAC alarms & Statalarm windows) so that the Control Room Operator can take appropriate action.

[ ]

Each analog signal in all measuring channels (i.e., redundant channels) is cyclically compared to its respective 2.MIN/2.MAX value to detect and monitor channel signal deviations. Deviation beyond the established acceptance criteria is alarmed by the Unit Statalarm and by the plant OAC. The acceptance criteria (parameter settings) are developed using instrument channel uncertainty terms established in the RPS or ESPS instrument uncertainty and set point calculations. Terms include drift, measuring and test equipment (M&TE) uncertainty and calibration procedure setting tolerances.

Operating with only three Reactor Coolant pumps instead of four introduces real process parameter differences between the two reactor coolant system loops. Therefore for the Reactor Coolant Pressure and the Reactor Coolant Temperature parameter inputs into the RPS, a different set of 2.MAX blocks is provided within the software with slightly wider Channel Comparison tolerance value settings that can be used if only three RC pumps are running. The TXS software uses RC Pump status to automate swap-over of these channel comparison alarm settings. The system allows selection of one of the following options:

- Automatic selection of the comparison set of values (automatic selection based on either four pumps running or less than 4 pumps running),
- The four pump comparison set, or
- The < four pump comparison set. A GSM screen will be implemented for this function.

The automatic analog and binary process signal monitoring for signal failure and for Channel Deviation satisfy and exceed the frequency of the manual monitoring presently performed by Operations to meet the TS surveillance requirements for Channel Checks of the Bailey RPS/ESPS.

3.3.16.5.2 Functional Testing

There are no requirements for a Channel Functional Test of the digital RPS/ESPS to be performed separately from the Channel Calibration. The Channel Calibration encompasses the requirements of the Channel Functional Test.

3.3.16.5.3 Channel Calibration

The digital RPS/ESPS provides the capability to perform periodic Channel Calibrations. Calibrations for instrument loops are performed by using M&TE to calibrate the field devices locally. The RPS/ESPS loops may be calibrated from the field devices through to the TXS or by injecting test signals into TXS input modules. Some field devices are not included in the Channel Calibration (such as the nuclear instrumentation power range detectors). Digital engineering units are read at the TXS Service Unit for all calibrations. If the instrument loops provide outputs to other devices (such as indicators) or provide signals to the ICS, the Channel Calibration of these instrument loops shall include these devices and /or verification of the proper signal to the ICS. Verification of proper response of the ESPS includes actuation of the final devices (pumps, valves, etc.) to ensure they respond to an ESPS actuation signal and that they move to the proper ESPS state (on/off, open/closed, etc.). Verification of proper response of the RPS includes testing of the reactor trip relays.

Channel Calibrations also include tests of the Manual Trip Switches for both ESPS and RPS. The Channel Functional Test is encompassed by the Channel Calibration so that the system is tested to verify proper response and ensure system operability.

The GSM "Input Signal Monitoring" screens permit monitoring and recording of the analog and binary inputs to the system during the Channel Calibration tests. While performing these tests, the analog or binary signals under test may be placed in Bypass or Trip using the GSM "Trip/Bypass" screens.

3.3.16.6 Operating Bypasses

> *IEEE Std 603-1998, Clause 6.6 states:*
>
> *"Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions:*
> *a) Remove the appropriate active operating bypass(es).*
> *b) Restore plant conditions so that permissive conditions once again exist.*
> *c) Initiate the appropriate safety function(s)."*

RPS/ESPS operating bypasses are described below.

3.3.16.6.1 RPS Operating Bypasses

RPS Channels A, B, C and D can be placed in Shutdown (S/D) Bypass mode via a SD Bypass keyswitch to facilitate performance of CRD testing, zero power physics testing, and startup and shutdown procedures. Each RPS channel may be placed in S/D Bypass mode as required.

S/D Bypass is applicable when the unit is in Mode 3, 4, 5, 6 or no mode. The S/D Bypass mode affects the reactor trips as follows:

- High Flux Reactor Trip - once the RPS is in S/D Bypass, an alternate High Flux Trip setpoint of ≤ 4% Rated Thermal Power (the TS allowable value is 5%) is automatically enabled. The High Flux Variable setpoint can be adjusted via the GSM, if necessary.
- Flux/Flow/Imbalance Trip - this trip is bypassed.
- High RCS Pressure Trip - once the RPS is in S/D Bypass, an alternate High RCS Pressure Trip setpoint of 1710 psig is automatically enabled.
- Low RCS Pressure Trip – this trip is bypassed.
- Variable Low RCS Pressure Trip – this trip is bypassed.
- RCS High Outlet Temperature Trip - this trip is not affected.
- RB High Pressure Trip - this trip is not affected.
- Loss of Both Main Feedwater Pumps Trip - this trip is not affected.
- Main Turbine Anticipatory Trip - this trip is not affected.
- RCPPM Trip – this trip is bypassed.

3.3.16.6.2 ESPS Operating Bypasses

The existing HPI and LPI bypasses are maintained with the new digital ESPS. The bypasses are functionally the same as those of the existing system, and they are automatically removed when plant conditions change to an operating mode in which the protective actions are required to be operable, in order to mitigate the consequences for a design basis event.

3.3.16.7 Maintenance Bypass

> *IEEE Std 603-1998, Clause 6.7 states:*
>
> *"Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features should continue to meet the requirements of 5.1 and 6.3."*

The digital RPS/ESPS provides the same capabilities as those described in Reference 2 for the generic TXS, as described below.

3.3.16.7.1 RPS Manual Bypass

RPS Channels A, B, C and D can be placed in Manual Bypass mode to facilitate maintenance activities, including the complete power-down of the TXS computer for a channel. Each RPS channel can be placed in Manual Bypass mode via a Manual Bypass keyswitch.

[ ]

When an RPS channel is placed in the Manual Bypass mode (i.e., Manual Bypass keyswitch is placed in the Manual Bypass position), the following occurs:

- 24 VDC is provided from the keyswitch directly to the coils of the RPS trip relays, in parallel with the outputs from the RPS channel.

[ ]

- All trip functions of that channel are blocked.
- Statalarm and computer alarms are generated.

Power is supplied to the Manual Bypass Statalarm window from both the TXS output module and directly from the switch contact in order to ensure that the bypass condition is annunciated even when the TXS computer is powered down. If an RPS channel is powered down at the power supply, the manual bypass condition will not be maintained; the RPS channel will go into a Trip condition and the Manual Bypass Statalarm will clear.

TSs require that at least three out of four channels of RPS be operable at all times. Since the ONS RPS has four redundant channels, placing one channel into Manual Bypass causes the RPS to go into a two-out-of-three configuration. To comply with TS, only one RPS channel can be placed into Manual Bypass at a time.

3.3.16.7.2 RPS Channel Trip Function Bypass

An individual Channel Trip Function Bypass allows placing one trip function in bypass for maintenance activities through the RPS GSM screens. This allows the remaining trip functions in the channel to remain operable while the channel input device for the affected channel is inoperable. Operation to put functions in bypass is administratively controlled since there is no interlock to prevent placing functions in multiple channels in bypass.

3.3.16.7.3 ESPS Voter Manual Bypass

The ONS digital ESPS is comprised of two subsystems (A1, B1, C1 and A2, B2, C2), each with an Odd (F1, F2) and Even (G1, G2) Voter. Each Voter can be individually placed in the Manual Bypass mode for maintenance or testing of the system using separate keyswitches located in the Voter cabinets. The Odd Voter keyswitches are located in Cabinet 12 and the Even Voter keyswitches are located in Cabinet 14. Voter subsystem 1 (Fl and G1) are keyed the same and Voter subsystem 2 (F2 and G2) are keyed the same to reduce the potential for human error.

TSs require that three input channels (A1, B1, C1 or A2, B2, C2) and 8 output channels (four from the Odd Voter and four from the Even Voter) be operable. The system can allow the maintenance bypass of one entire ESPS Voter subsystem (F1, G1 or F2, G2) and still meet operability requirements.

Placing a keyswitch in the Manual Bypass position sends a signal to the TXS software indicating that the applicable Voter subsystem has been placed in Manual Bypass. This causes the TXS software to inhibit the outputs for that specific Voter subsystem. Additionally, Maintenance Bypasses are alarmed over the gateway so that local indication is provided in the control room in accordance with IEEE Std 603-1998 section 5.8.3 requirements. When a Voter is placed in Manual Bypass mode, the Voter status is indicated continuously in the control room via a Statalarm. The Voter status is also sent to the OAC via the TXS Gateway computer.

[ ]

[When the TSs require the ESPS] to be operable, plant procedures only allow placement of either ESPS Subsystem 1 Voters (F1 [Odd] and G1 [Even]) or ESPS Subsystem 2 Voters (F2 [Odd] and G2 [Even]) in Manual Bypass at one time.

3.3.16.7.4 ESPS Instrument Channel Manual Trip Mode

Each ESPS Instrument Input Channel A2, B2, and C2 can be manually tripped using a Channel Trip keyswitch. The Channel Trip switch also provides an input to the associated ESPS Instrument Input Channel located in the RPS cabinets (A1, B1, and C1). Tripping ESPS Channel A2 also trips ESPS Channel A1. The remaining channels are unaffected.

When an input channel is placed in Channel Trip, a trip signal is sent to the TXS software within both ESPS subsystem computers for that channel. All of the input parameters for that channel are placed in a tripped state. Trip of any additional ESPS Instrument Input Channel will complete the logic and initiate an ESPS actuation.

[Keyswitch status information is] sent to the Statalarm panel and to the OAC via the TXS Gateway.

Refer to Section 3.3.16.2 of this Enclosure for additional information.

3.3.16.7.5 Summary

In the ONS FMEA (refer to Section 3.7 of this Enclosure), one of the initial conditions assumed is that an RPS channel or ESPS voter subsystem is in Bypass status. This initial condition imposed on the analysis is used in determining the overall effect of an evaluated failure on the safety system's ability to perform the required safety functions. Failures are assumed to occur in the operable channels or voters. The FMEA successfully demonstrates that the digital RPS/ESPS design incorporates sufficient redundancy, independence and other design fundamentals to ensure that no credible single failure can compromise the RPS/ESPS safety function, even assuming that one RPS channel or ESPS voter subsystem has been placed in maintenance bypass.

3.3.16.8 Setpoints

> *IEEE Std 603-1998, Clause 6.8 states:*
>
> *"The allowance for uncertainties between the process analytical limit documented in Clause 4, item d) and the device setpoint shall be determined using a documented methodology. Refer to ANSI/ISA S67.04-1994.*
>
> *Where it is necessary to provide multiple setpoints for adequate protection for a particular mode of operation or set of operating conditions, the design shall provide positive means of ensuring that the more restrictive setpoint is used when required. The devices used to prevent improper use of less restrictive setpoints shall be part of the sense and command features."*

Duke has revised uncertainty calculations (refer to Table 1-2 items 28, 29, 31, 33, and 35 of this Enclosure) affected by the RPS/ESPS digital upgrade to account for the effect of replacing an analog system with a digital system. The revised calculations confirm that there is adequate margin between operating limits (or alarm limits) and trip setpoints such that there is a low probability for inadvertent actuation of the system. They also confirm that adequate margin exists between the trip setpoints and the safety limits such that the system initiates protective actions before safety limits are exceeded.

As such, there are no safety limits, TS allowable values, or RPS/ESPS trip/actuation setpoints that require changing as a result of the digital RPS/ESPS installation.

The total loop uncertainties are utilized in the safety analyses to ensure that the analyzed values are bounding and conservative. Table 3-1 provides the total loop uncertainties of measured parameters important to ONS safety analyses. In general, the values reported for the digital RPS are one-sided uncertainties while those reported for the analog RPS are two-sided uncertainties. Since the ONS safety analyses are only concerned with approaching the trip setpoint from one direction, the one-sided uncertainties are appropriate.

The margin between the maximum allowed alarm limits and the RPS/ES trip setpoints contains, in part, the total loop uncertainty. If the total loop uncertainty decreases relative to the existing analog assumptions, as is the case for all trip strings except high temperature, then the maximum allowed alarm limits could be increased. Duke does not plan to increase the maximum allowed alarm limits. Maintaining the current maximum allowed alarm limits results in a slight increase in margin between the maximum allowed alarm limits and the trip setpoints. The only trip strings with a higher uncertainty are the high temperature trip and the wide range RCS pressure trip. For the high temperature trip, this increase is on the order of 0.2 °F. ONS normally operates with a T_{hot} of ~602-603 °F.. The high temperature trip setpoint is

617 °F. The difference between normal operation and a reactor trip is much greater than the uncertainty and there is no increased probability of an inadvertent trip. For the wide range pressure signal in a degraded reactor building, the increase is 0.5 psi for the positive uncertainty and 53.4 psi for the negative uncertainty. Since these uncertainties only apply to accident conditions, they do not increase the probability of an inadvertent ES actuation during normal operation.

Adequate margin must also exist between the trip setpoints and the safety limits such that the system initiates protective actions before safety limits are exceeded. The safety limits, TS allowable values, and RPS/ESPS trip/actuation setpoints are not changing as a result of the digital system installation. The total loop uncertainties identified in Table 3-1 below are similar to the uncertainties corresponding to the existing analog system and in all cases, even for the two trip functions with the increased uncertainty, are bounded by the allowance assumed in the safety analyses. The safety analyses verify that the safety limits are satisfied. To determine acceptable results, the safety analyses assume a RPS or ESPS trip actuates when the measured value of a particular parameter meets or exceeds the TS allowable value, then ensures that the actual value of that parameter, which is the measured value adjusted for the Allowance, is bounded by the safety limit. Therefore, by demonstrating that the uncertainty is less than the Allowance, the existing safety analyses remain bounding. However, in the future, Duke may decide to reanalyze the safety analyses to take credit for the reduced RPS/ESPS uncertainties thereby recapturing some of the inherent margin.

Table 3-1 Total Loop Uncertainty

Trip Function	Total Loop Uncertainty		Current Safety Analysis Allowance
	Digital RPS/ESPS	Analog RPS/ESPS	
High RCS Pressure	±14.17 psi	±16.2 psi	-30 psi
Low RCS Pressure	±14.17 psi	±16.2 psi	+30 psi
High RCS Temperature	±1.31 °F	±1.14 °F	-2 °F
Variable low P-T (See Note 2)	±17.7 psi	±21.4 psi	N/A (See Note 2)
High Flux (See Note 1)	±2.32 %FP	±5.0 %FP	-(5.0 %FP + transient effects)
Pump power/flux (See Note 3)	±2.321 %FP	±5.15 %FP	N/A (See Note 3)
Flux/flow/imbalance (See Note 2)	±3.184 %FP	N/A	N/A (See Note 2)
WR RCS Pressure – Normal (See Note 4)	+31.16 psi -28.16 psi	+ 49.1 psi - 46.1	+50 psi
WR RCS Pressure – Accident (See Note 4)	+188.4 psi -173.8 psi	+ 187.9 psi - 120.4 psi	+190 psi
RB Pressure – Accident (See Note 5)	±0.6 psi	±0.6 psi	-5 psi

Table Notes:

General

- Sign convention is "Indicated – Actual value". Thus, a positive value means the actual value is less than what the instrumentation indicates by that amount, and vice-a-versa.

- The second column is subdivided into two columns. The first column is for the digital RPS/ESPS total loop uncertainty. The second column is for the analog RPS/ESPS total loop uncertainty. The last column is the allowance utilized in the current safety analyses. This allowance is the calculated analog RPS/ESPS total loop uncertainty (TLU) plus margin and represents the difference between the actual value of a parameter at the TS allowable value. The allowance is applied, in the analyses, as an adjustment to the signal that is being compared to the trip setpoint. For example, if the high RCS pressure TS allowable value is 2355 psig, the actual pressure at the time a high pressure trip is actuated in the safety analyses is 30 psi higher (assuming higher is conservative).

Specific

(1)The TLU for the high flux trip in the analog system is calculated as an algebraic sum of the excore NI calibration allowance, the heat balance, and the trip setpoint uncertainty allowance. The TLU for the digital RPS is the square root sum of the squares for the same values as specified in the Duke procedure used for instrument uncertainty and setpoint calculations. The Allowance with the analog system additionally includes transient NI effects, such as control rod shadowing and reactor vessel downcomer attenuation, that differ for each transient and hence the allowance is different depending on the transient. Treatment of the transient NI effects will not change with the installation of the digital system.

(2) Given the way the Allowance is applied in the analyses, a single value for the variable low pressure-temperature trip and the flux/flow/imbalance trip functions is not applicable. For analyses that might actuate the variable low pressure-temperature trip, the input temperature signal is adjusted by the temperature TLU allowance (2°F) and the pressure signal is adjusted by the pressure TLU allowance (30 psi). Likewise, for analyses that might actuate the flux/flow trip (imbalance contribution conservatively neglected in the safety analyses), the flux signal is adjusted by the flux TLU (4%FP for non-Statistical Core Design analyses) and the flow signal is adjusted by the uncertainty allowance for RCS flow (2% design flow for four reactor coolant pump (RCP) analyses, 2.75 % design flow for three RCP analyses).

(3) The pump-power/flux trip is modeled as a binary trip. Upon the loss of 2 or more RCPs, a pump-power/flux trip signal is generated. The TLU for this trip function applies to the power level at the time the second RCP trips off. The pump-power/flux trip is active above 2 % FP and the uncertainty is applied to determine if the reactor is above 2% FP. All of the at-power transient analyses are at 15 % FP or higher. Thus, the TLU for this trip function is inconsequential to the transient analyses. It is provided here for completeness.

(4) Even though a positive and negative uncertainty is calculated for wide range pressure, HPI and LPI actuation only occurs when pressure decreases to the setpoint. Therefore, the safety analyses only consider the positive uncertainty.

(5) The current TS allowable value for ES actuation is 4 psig. The safety analyses assume 9 psig for this setpoint. Hence, there is -5 psi allowance.

3.3.17 Execute Features – Functional and Design Requirements

> *IEEE Std 603-1998, Clause 7 states (in part):*
>
> *In addition to the functional and design requirements in Clause 5, the requirements listed in 7.1 through 7.5 shall apply to the execute features. Execute features are the electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling.*

The sense and command features for the ESPS end at the output of the Voters. As part of the design change, the one existing relay output (RO) relay was replaced with two RO relays. No other changes were made. For RPS the sense and command feature ends at the digital output module. The reactor trip modules were replaced by reactor trip relays which perform the RPS execute feature.

3.3.18 Power Source Requirements

> *IEEE Std 603-1998, Clause 8 states:*
>
> ***"Electrical power sources***
> *Those portions of the Class 1E power system that are required to provide the 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 308-1991.*
> ***Non-electrical power sources***
> *Non-electrical power sources, such as control-air systems, bottled-gas systems, and hydraulic systems, required to provide the power to the safety systems are a portion of the safety systems and shall provide power consistent with the requirements of this standard. Specific criteria unique to non-electrical power sources are outside the scope of this standard and can be found in other standards.[11] [B4, B5]*
> ***Maintenance bypass***
> *The capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (i.e., reducing temporarily its degree of redundancy to zero[12]), the remaining portions provide acceptable reliability."*

3.3.18.1 Electrical Power Sources

The digital RPS/ESPS equipment is powered by redundant 120 VAC / 24 VDC Absopulse power supplies, model PFC419-Q9418. Each power supply provides a 24 VDC, 500 W output with an input voltage range of 90-150 VAC, 47-63 Hz. The

RPS/ESPS uses the 120 VAC to power redundant auctioneered ±24VDC power supplies that power RPS/ESPS circuitry and power existing field devices . The Absopulse power supplies, located in cabinets 2, 4, 6, 8, 9, 10, 11, 12, and 14 receive 120 VAC from the inverter-backed vital power panels and breakers shown below. Odd/Even Checkback Cabinets 17 and 18 receive 24 VDC from the Absopulse power supplies located in cabinets 12 and 14, respectively, and 120 VAC from breakers also as shown below. Duke analyses demonstrate that these breakers are adequate to supply the RPS/ESPS cabinets and that the load on the inverters is not negatively impacted.

Cabinet 16 (RPS Channel E) is powered via a battery-backed non-1E 120 VAC I&C panel board.

Table 3.3.18-1 TXS Cabinet Power Sources

Cabinet	Breaker	Inverter
PPSCA0001/PPSCA0002	KVIA-1	DIA
PPSCA0003/PPSCA0004	KVIB-1	DIB
PPSCA0005/PPSCA0006	KVIC-1	DIC
PPSCA0007/PPSCA0008	KVID-1	DID
PPSCA0009/PPSCA0012	KVIA-2	DIA
PPSCA0010/PPSCA0014	KVIB-2	DIB
PPSCA0011	KVIC-2	DIC
PPSCA0017	208 VAC MCC XS1-R3B	N/A
PPSCA0018	208 VAC MCC XS2-R3CB	N/A

Since the Absopulse power supplies apply a non-linear load to the 120 VAC Vital I&C Power System, the effects of harmonic distortion must be considered. The Absopulse power supplies have a total harmonic distortion (THD) of 4.45%. IEEE 519-1992 requires that THD be no more than 10%. Duke has analyzed the existing harmonic distortion levels and the requirements for additions of non-linear loads to the 120 VAC Vital I&C Power System. The calculation states that loads on the 120 VAC Vital I&C Power System are not impacted by THD of less than 5% on the source voltage (5% is based on the THD rating of the output voltage of the Inverters). Since the Absopulse THD of 4.45% is less than the IEEE 519-1992 limit and also less than the THD rating of the inverters, it is acceptable.

EPRI TR-107330 requires that control system power supplies have a hold-up time sufficient to handle a power interruption of at least 40 milliseconds. The Absopulse power supplies for this design change have been tested and exceed the requirements of EPRI TR-107330.

The Gamma-Metrics NI racks are designed to operate with 120 VAC +/- 10%, 60 Hertz +/- 3%, single phase. Each of the four redundant NI racks is powered by an battery-backed vital 1E 120 VAC power source. There is no change to the Gamma-Metrics NI drawers or circuitry design.

3.3.18.1.1 Load analysis

Duke analyzed loads placed on the inverters by the digital RPS/ESPS and confirmed the loads are acceptable. The load analyses review and calculate the changes in loads associated with the replacement of the existing RPS/ESPS with the new digital RPS/ESPS system.

The analyses document the electrical load changes to the 120 VAC breakers and 125 VDC battery backed power source that occur due to replacement of the RPS/ESPS and modification to the RCPPM components.

For each affected panel and breaker, the load changes were tabulated and added to determine the net load change. The panel / breaker net load change was then compared to the acceptance criteria prescribed for the analyses. The analyses determined that the digital RPS/ESPS reduces loads on the affected breakers listed above.

The components in existing cabinets ES-8 and ES-9 are being replaced by TXS equipment and the cabinets are being renamed to PPSCA0017 and PPSCA0018, respectively. These cabinets currently contain Bailey Auxiliary B relay modules for acquiring device status from the field and providing this status to the OAC and RZ module indication lights. This design change will remove the Auxiliary B relays and two 120 VAC / 24 VAC transformer. New Phoenix relays and optocouplers will be installed for acquiring device status. Status will be processed by the digital RPS/ESPS with indication provided by two ESPS status panels on the MCB via 24 VDC signals. The current status signals and the 120 VAC transformer are both powered from 208 VAC MCC XS1-R3B for ES-8 (new PPSCA0017) and 208 VAC MCC XS2-R3CB for ES-9 (new PPSCA0018).

The only loads remaining on XS1-R3B and XS2-R3CB from the RPS/ESPS are the Phoenix relays and optocouplers. 24VDC indication on the ESF Status Panel is provided by the Absopulse Power Supplies powered by KVIA-2 and KVIB-2. Analyses show that the digital RPS/ESPS decreases the loading on XS1-R3B and XS2-R3CB.

This design change will replace all twelve (12) status relays in ESTC3 with new Phoenix relays that will interface directly with ESPS cabinets PPSCA0017 and PPSCA0018. Also, four (4) relays providing control for LPSW-6 and LPSW-15 will be replaced with new Phoenix relays, and new control switches and indicating LEDs on UB2 for LPSW-6 and LPSW-15 will be installed. Additional Phoenix relays will be installed in ESTC3 to provide indication above the new control switches. A total of 28 Phoenix relays will be installed to replace the status and control relays in ESTC3. Analysis shows that the overall load change to XS3-5B decreases and therefore this change is acceptable.

Currently the on/off status for KHUs 1 and 2 is provided directly to the RZ indication on control board VB2 from relays in cabinets KOIC-A and KOIC-B, respectively. In order to provide device status to the ESPS Odd/Even Checkback Cabinets 17 and 18, four Phoenix relays will be added, two for Odd and two for Even. Instead of the relays in KOIC-A and KOIC-B lighting lights, they will pick up the new Phoenix relays. Contacts from the Phoenix relays will be sent to cabinets 17 and 18 for input to digital RPS/ESPS. Analyses determined that this change has a negligible impact on the transformers in KOIC-A and KOIC-B.

3.3.18.1.2 Voltage Analysis

Duke analyzed the voltages seen by the equipment being installed by the digital RPS/ESPS design change , taking into account the voltage drops seen within the associated circuits. These analyses demonstrate that the voltage seen by each device is adequate to allow each device to perform its intended function.

The circuit analyses include all loads that are powered by the digital RPS/ESPS, along with any voltage drops associated with each loop. The RPS circuit analysis addresses NI and RCPPM components. No adverse effects are seen from voltage drops associated with the digital RPS circuitry, NI or RCPPM equipment were found.

The calculated voltage drops and dips are calculated using the worst case scenario for the digital RPS circuitry, NI, and RCPPM. The worst case voltage is based on a normal voltage source and an alternate voltage source. The worst case voltages are analyzed with respect to the system equipment and components and are determined not to be adversely impacted by the worst case voltage levels seen in the analysis.

In addition to the power panels, the ESPS circuit analysis also addresses MCC Panels XS1, XS2 and XS3, the 120VAC/24VAC transformers in KOIC-A and KOIC-B, and the control power relays. This analysis shows that the voltage seen by each device is adequate to allow each device to perform its intended function.

3.3.18.1.3 Breaker Coordination Analysis

The main feeder breakers supplying the digital RPS/ESPS are Gould QP, 1-Pole, 20A breakers. The digital RPS/ESPS is supplied with ETA 2210-S2, 16A. Duke analyses shows the 16A breaker supplied with the digital RPS/ESPS will trip and clear faults in the thermal region prior to the main 20A breaker upstream. The analyses determined that the digital RPS/ESPS supplied breakers are acceptable.

3.3.18.2 Non-electrical Power Sources

There are no non-electrical sources of power for the digital RPS/ESPS.

3.3.18.3 Maintenance Bypasses

As described above, the digital RPS/ESPS uses the same power sources as does the existing system that it will replace. The digital RPS/ESPS will behave the same as does the existing system when power supplies are in maintenance bypass.

3.4 Conformance with IEEE Std 7-4.3.2 [2]

The information included in this section explains how the ONS design for the digital RPS/ESPS complies with IEEE Std 7-4.3.2-2003 by addressing the safety system design basis listed in RG 1.206, Appendix C.I.7-C. The design basis items listed in the RG are consistent with the safety system criterion listed in Section 5 of the IEEE Std 7-4.3.2-2003. Per RG 1.152, Revision 2, conformance with the requirements of IEEE Std 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants

Additional computer specific requirements to supplement the criteria and requirements of IEEE Std 603-1998 are specified. Within the context of this standard, the term computer is a system that includes computer hardware, software, firmware, and interfaces. The criteria contained herein, in conjunction with criteria in IEEE Std 603-1998, establish minimum functional and design requirements for computers used as components of a safety system.

This standard serves to amplify criteria in IEEE Std 603-1998 to address the use of computers as part of safety systems in nuclear power generating stations. The criteria contained herein, in conjunction with criteria in IEEE Std 603-1998, establish minimum functional and design requirements for computers used as components of a safety system.

[2] Section 3.4 contains excerpts from IEEE Std 7-4.3.2-2003, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Copyright 2003 IEEE. All rights reserved. These excerpts are located in single-line boxes.

3.4.1 Single-Failure Criterion

> *IEEE Std 7-4.3.2-2003, Clause 5.1 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary (see also Annex B)."*

IEEE Std 603-1998 'Single-Failure' requirements are addressed in Section 3.3.1 of this Enclosure.

3.4.2 Completion of Protective Action

> *IEEE Std 7-4.3.2-2003, Clause 5.2 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 'Completion of Protective Action' requirements are addressed in Section 3.3.2 of this Enclosure.

3.4.3 Quality

> *IEEE Std 7-4.3.2-2003, Clause 5.3 states:*
>
> *"...Software quality is addressed in IEEE/EIA Std 12207.0-1996 and supporting standards. Computer development activities shall include the development of computer hardware and software..."*
>
> *And it further states:*
>
> *"In addition to the requirements of IEEE Std 603-1998, the following activities necessitate additional requirements that are necessary to meet the quality criterion:*
> *— Software development*
> *— Qualification of existing commercial computers (see 5.4.2)*
> *— Use of software tools*
> *— Verification and validation*
> *— Configuration management*
> *— Risk Management"*

RG 1.152, Revision 2, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," endorses IEEE Std 7-4.3.2-2003, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as a method acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants.

This LAR addresses these additional requirements for the Duke and AREVA NP Software QA programs, as applicable, in Sections 3.4.3.1 and 3.4.3.2 below. These programs do not differentiate between the initial system development or any changes to the new system after it is installed. The new system installation as well as any changes to the system (hardware or software) will be performed within the context of the engineering change program, governed by department directives.

The three stages of development identified in BTP 7-14: Software Life Cycle Process planning, Software Life Cycle Process Implementation, and Software Life Cycle Process design outputs are also addressed, as applicable to the Duke and AREVA NP Software QA programs.

3.4.3.1 Duke Energy Software and Data Quality Assurance (SDQA) Program

The Duke SDQA program is described in a department directive (refer to Table 1-2, Item 27 of this Enclosure) which provides the QA requirements for nuclear safety related (QA Condition 1) software and data. In addition, it provides a method of applying a graded QA approach to all other software and data used in the Nuclear Generation Department (NGD). The graded program assures quality commensurate with the item's importance to safety.

The department directive applies to all software and data used in support of the RPS/ESPS, including software and data currently in operation (after installation), under development, or in procurement. The department directive fulfills the requirements of the Duke Energy Carolinas Quality Assurance Topical Report (Ref. 7) related to the development, procurement, operation, and maintenance of software and data in support of the NGD. Its requirements are applied to the RPS/ESPS for the:

- Development of software and data.
- Development of supporting QA documentation for software and data.
- Maintenance and management of software after release, including requirements for management of changes to source code, hardware, and operating systems.
- Maintenance and management of data including possible requirements for calibration and certification of data sources and data links.
- Development of disaster recovery plans.
- Monitoring of system health.

The following direction is provided:

- Preparation and management of SDQA Documents which identify the applicable QA requirements, contain all supporting documentation, and document approvals and revision history necessary to assure the quality of the software and data.
- Identify when software and data may be in the same document and when separate documents for software and data are recommended.
- Use of a graded approach to develop and manage software and data commensurate with the items importance to nuclear safety and which considers controls provided by other programs allowed by the QA Program Topical Report (i.e. Measuring & Test Equipment).
- Software Configuration Management and Document Management for software, data, firmware, and associated hardware.
- Guidance for detailed procedures, which support this department directive, to be used by Information Technology group(s) or outside organizations responsible for the development and maintenance of software or data and the management of associated hardware.
- Requirements for the management of computer networks and mainframes which support the operation of software and data.
- Requirements for the implementation of this Directive relative to existing software, data, and associated hardware.

Duke contracted AREVA NP to perform software engineering for the RPS/ESPS digital upgrade project. AREVA NP has a Software Quality Assurance Program (SQAP) that meets the requirements of the Duke SQAP described above. The AREVA NP SQAP is described in Section 3.4.3.2 below.

AREVA NP is responsible for software QA and configuration management during the development, integration, and test phases of the upgraded systems. There are three tests that require full and satisfactory completion, including resolution of identified discrepancies, before Duke accepts responsibility for software configuration management. These tests are a FAT, a 30-Day Reliability Test, and a SAT.

Duke will be responsible for configuration management of the integrated hardware/software system upon acceptance. From that point forward, configuration management will be performed in accordance with the SDQA Plan. The SDQA Plan will identify specific elements of the Duke software QA program, and how these elements apply to the digital RPS/ESPS.

After Duke SAT, any changes needed to the software will require issuance of a Software Data Change Request (SDCR). If a software change is needed after the Design Change Package (DCP) is Tech Approved, per the Engineering Change Program (described in Section 3.3.3 of this Enclosure), then the change will require an SDCR and a Variation Notice against the DCP to revise the SDQA plan.

Once the digital RPS/ESPS is installed, tested, turned over to Operations, and declared operable, the Design Change Package will be closed, and all affected documents will be as-built per the Engineering Change Program. After as-building the RPS/ESPS Upgrade Project, any proposed software changes will require a new Engineering Change.

The SDQA plan prepared for the upgrade will remain open and active during the Operations and Maintenance phases of the software lifecycle. Duke will remain responsible for initiating any changes to the software using Engineering Changes and associated SDCRs under the SDQA Plan. The detailed engineering for the software change, including functional changes and changes to supporting engineering documents will be performed under the AREVA NP software QA program (described below). Duke will remain responsible for acceptance, installation, and post-installation testing of the changes, as well as continued operations and maintenance of the modified system in accordance with TS 3.3.1, "RPS Instrumentation," TS 3.3.3, "Reactor Trip Modules," TS 3.3.5, "ESPS Analog Instrumentation," and TS 3.3.7, "Engineered Safeguards Protective System Digital Automatic Actuation Logic Channels."

3.4.3.2 AREVA NP Software Quality Assurance Program

Section 3 of the TXS Topical Report (Reference 2) describes the Software Life Cycle Process Planning for the design and qualification of the TXS platform (hardware, operating system software, Function Block library, and application software development tools).

The TXS Software Program Manual (Reference 11) addresses the development process for application software in Section 1.2. The software life cycle activities for TXS projects fit into the following phases:

- Basic Design
- Detailed Design
- Testing - FAT
- Installation and Commissioning
- Final Documentation

The TXS Software Program Manual (Reference 10) also addresses software modifications and maintenance by AREVA NP after the system has been turned over to the customer.

The TXS Software Program Manual was submitted to the NRC for review and approval in December 2006 after the basic design and much of the detailed design on the ONS RPS/ESPS project was completed by AREVA. The Software Program Manual reflects how the design and documentation was developed prior to its existence and in some cases caused improvements to design documentation to bring it up to the standards of the manual.

3.4.3.2.1 Software Development

> *IEEE Std 7-4.3.2-2003 Clause 5.3.1 states:*
>
> *"Computer software shall be developed, modified, or accepted in accordance with an approved software quality assurance (QA) plan consistent with the requirements of IEEE/EIA 12207.0-1996. The software QA plan shall address all software that is resident on the computer at run time (i.e., application software, network software, interfaces, operating systems, and diagnostics). Guidance for developing software QA plans can befound in IEC 60880 (1986-09) [B4] and IEEE Std 730™-1998 [B8]."*

Section 2.1 of the TXS Topical Report describes the QA program for the design and qualification of the TXS platform (hardware, operating system software, Function Block library, and application software development tools). Section 3 of the TXS Topical Report describes the software life cycle process planning of the design and qualification of the TXS platform (hardware, operating system software, Function Block library, and application software development tools).

The TXS Software Program Manual describes the program measures incorporated by AREVA NP to ensure that the TXS application software attains a level of quality commensurate with its importance to safety functions, performs the required safety functions correctly, and conforms to established technical and documentation requirements, conventions, rules, and industry standards. The TXS Software Program Manual applies to application software developed for all TXS projects in the U.S., including the ONS RPS/ESPS digital upgrade.

The TXS Software Program Manual requires that a SQAP be developed. The TXS SQAP, which is implemented by an AREVA Operating Instruction (OI), identifies measures to ensure the developed TXS application software conforms to established technical requirements, rules, and standards. The OI also describes the tools to be used and methodology to be followed in developing and maintaining software to be used for the design of TXS application software.

The TXS Software Program Manual defines the overall software development process for TXS application software for United States projects. It uses IEEE Std 730-2002, "IEEE Standard for Software Quality Assurance Plans," as guidance for the software QA plans. IEEE Std 730-2002 is considered equivalent to IEEE/EIA Std 12207.0-1996.

Section 1.1 of IEEE Std 730-2002 states:

> "Although this document does not require the use of IEEE/EIA Std 12207.0-1996 and IEEE/EIA Std 12207.1-1997, it is consistent with those two standards. An SQAP meeting the requirements of this standard will be in document compliance with the SQAP information item of IEEE/EIA 12207.1-1997."

The TXS Software Program Manual describes a software development program that conforms to the guidance of BTP HICB-14, "Guidance on Software Review for Digital Computer-Based Instrumentation and Control Systems," dated June 1997 (the version in effect when the TXS Topical Report was approved and the Software Program Manual was submitted to NRC for review and approval). This guidance was revised in March 2007 (and renumbered as BTP 7-14) to provide additional reviewer guidance but is generally consistent with the earlier version except for the numbering conventions of the BTP.

The TXS Software Program Manual describes the application software development life cycle, which is based on the set of life cycle activities provided in IEEE Std 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes." RG 1.173, September 1997, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std. 1074-1995.

3.4.3.2.2 Software Quality Metrics

IEEE Std 7-4.3.2-2003 Clause 5.3.1.1 states:

"The use of software quality metrics shall be considered throughout the software life cycle to assess whether software quality requirements are being met. When software quality metrics are used, the following life cycle phase characteristics should be considered:
— Correctness/Completeness (Requirements phase)
— Compliance with requirements (Design phase)
— Compliance with design (Implementation phase)
— Functional compliance with requirements (Test and Integration phase)
— On-site functional compliance with requirements (Installation and Checkout phase)

> *— Performance history (Operation and Maintenance phase)*
> *The basis for the metrics selected to evaluate software quality characteristics should be included in the software development documentation. IEEE Std 1061™-1998 [B11] provides a methodology for the application of software quality metrics."*

Software quality metrics are used throughout the Software Life Cycle to assess the effectiveness of the Software Quality Assurance Program. Software and design errors are recorded as "Open Items" during each phase of development. These items are tracked and trended to determine the progress in eliminating the errors present in the software and design. Details on these quality metrics are described in Sections 3.8, 6.3, and 10.2 of the TXS Software Program Manual.

3.4.3.2.3 Software Tools

> *IEEE Std 7-4.3.2-2003 Clause 5.3.2 states:*
>
> *"Software tools used to support software development processes and verification and validation (V&V) processes shall be controlled under configuration management. One or both of the following methods shall be used to confirm the software tools are suitable for use:*
> *a) A test tool validation program shall be developed to provide confidence that the necessary features of the software tool function as required.*
> *b) The software tool shall be used in a manner such that defects not detected by the software tool will be detected by V&V activities. Tool operating experience may be used to provide additional confidence in the suitability of a tool, particularly when evaluating the potential for undetected defects".*

Section 3.8 of the TXS Software Program Manual describes the software tools used for the TXS projects. The tools are all part of the TXS platform. Section 5 of the TXS Topical Report describes the development process for the TXS software tools.

The SPACE engineering system contains the tools for converting function diagrams into software code and includes the source code-generators, such as function diagram group module and run time environment, and the software for compiling, linking and locating, such as make command. These tools are part of the qualified TXS software package. The logic diagrams in the Software Design Description (SDD) are entered into the SPACE tool, which generates the code.

The software design group uses the TXS tool, FunBase, to create the SDD. FunBase is a database that is designed to facilitate the organization of the application software functions and the respective internal and external input/output signals. FunBase controls the assignment of module and signal naming so that each entity in the software is uniquely and unambiguously named. The Verification and Validation (V&V) team traces customer requirements from the Software Requirements Specification (SRS) into the SDD.

The tool for software simulation testing is the TXS Simulation and Validation Tool (SIVAT). SIVAT was developed based on a requirements specification and technical specification document. The development process follows the AREVA NP GmbH procedure for Software Lifecycle Processes. The validation of the product was performed with tests of a real TXS application (data from a test) and the results of a SIVAT simulation of the same application. Changes to the SIVAT tool are controlled by the AREVA NP GmbH procedure for Configuration Management, which establishes requirements to ensure that changes are controlled, documented, and tested. AREVA NP has operating experience with the use of SIVAT for more than 20 project-specific applications. RETRANS was used as part of of the independent qualification of the automatic code generation tool used for TXS application software.

3.4.3.2.4 Verification and Validation

IEEE Std 7-4.3.2-2003 Clause 5.3.3 states:

"NOTE—See IEEE Std 1012-1998 and IEEE Std 1012a™-1998 [B10] for more information about software V&V.

V&V is an extension of the program management and systems engineering team activities. V&V is used to identify objective data and conclusions (i.e., proactive feedback) about digital system quality, performance, and development process compliance throughout the system life cycle. Feedback consists of anomaly reports, performance improvements, and quality improvements regarding the expected operating conditions across the full spectrum of the system and its interfaces.

V&V processes are used to determine whether the development products of an activity conform to the requirements of that activity, and whether the system performs according to its intended use and user needs. This determination of suitability includes assessment, analysis, e valuation, review, inspection, and testing of products and processes.

This standard adopts the IEEE Std 1012-1998 terminology of process, activity and task, in which software V&V processes are subdivided into activities, which are further subdivided into tasks. The term V&V effort is used to reference this framework of V&V processes, activities, and tasks.

V&V processes shall address the computer hardware and software, integration of the digital system components, and the interaction of the resulting computer system with the nuclear power plant.

The V&V activities and tasks shall include system testing of the final integrated hardware, software, firmware, and interfaces.

> *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 (i.e., IEEE Std 7-4.3.2™). See IEEE Std 1012-1998 Annex B for a definition of integrity level 4 software."*

Sections 2.1 and 3.2 of the TXS Topical Report describe the software V&V activities for the design and qualification of the TXS platform (hardware, operating system software, Function Block library, and application software development tools).

Section 6 of the TXS Software Program Manual describes the software V&V plan for development of TXS application software for U.S. projects. The TXS application software V&V plan follows the guidance of IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," with the following exceptions. The alternate approach to component V&V test execution of Function Diagrams and Groups of Function Diagram Group Modules is described in Section 6.2.7.4.1 and the alternate approach to acceptance test V&V is described in Section 6.2.7.4.3. RG 1.168, Revision 1, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," endorses IEEE Std 1012-1998.

Layers of simulation testing V&V are used to ensure application software testing quality to demonstrate proper application software functionality.

Second, SIVAT testing is performed by the development group. This testing process is an integral part of the TXS engineering process. The SIVAT test plans, procedures and results are prepared using the standard engineering process. Verification of the function diagrams by the engineers is facilitated by the use of a commonly understood notation used to prepare the Function Diagrams. The NRC evaluation of the automatic code generation process was documented in the safety evaluation report issued for the TXS Topical Report. The SIVAT tool is used to validate the application software functionality using a wide variety of manipulation functions (i.e., built-in malfunctions). This approach enables the I&C engineer to compare the validation results to the functional requirements.

And third, the SIVAT test plan and results are verified by the V&V group to ensure software functionality. The independent software V&V group can also trace the requirements through the SIVAT testing specifications and procedures. The V&V group is completely independent of the software development organization. The I&C functionality can be fully assessed by verification of SPACE diagrams. This check is equivalent to code verification in other code development systems. The code generation verification checks performed by the SPACE tool can be readily verified. The SIVAT testing methods and results can be readily verified.

Layers of verification and validation are used to ensure FAT quality to demonstrate proper integrated system performance.

First, the generic TXS platform software and hardware integration is subject to the generic qualification process described in the TXS Topical Report. This approach provides a very high degree of V&V independence commensurate with the importance of generic system qualification.

Second, the FAT is performed by a test group (comprised of hardware and software development personnel). This testing method ensures that the proper hardware and software personnel are used in an integrated fashion to develop and conduct the FAT. The FAT plans, procedures, and results are prepared using the standard engineering process. This approach enables the hardware and software engineers to compare the test results to the design and customer specifications.

And third, the V&V group performs the independent verification and can also perform the independent Appendix B design review of the FAT procedures and results to ensure software functionality. The independent V&V group has the authority to perform independent acceptance testing as deemed necessary.

During the FAT, the V&V engineer will periodically observe the testing and verify that the testing follows the approved FAT procedures. The V&V team uses the software requirements traceability matrix to ensure that the original requirements have been tested. The V&V engineer independently verifies that the software versions being tested match those listed in the Software Configuration Management Plan.

The ONS RPS/ESPS project contract was awarded in November 2001. The applicable software V&V guidance was IEEE Std 1012-1986, which was endorsed by NRC RG 1.168, dated September 1997. The guidance in effect at that time did not include any V&V requirements for an Acquisition Process and Supply Process.

Consequently, no V&V work was performed of the contract activities between AREVA NP and AREVA NP GmbH. Duke and AREVA NP evaluated and concluded that the absence of V&V work for this activity had no impact on the application software for the ONS RPS/ESPS project. The TXS system was purchased from AREVA NP GmbH. The TXS system is a fully integrated and qualified digital system suitable for use in the ONS RPS/ESPS. The TXS system is fully described in the TXS Topical Report (Reference 2) that was reviewed and approved by NRC (Reference 1) for use in nuclear power plant safety systems. The generic TXS platform qualification process included qualification work performed by an independent third party TÜV (Technischer Überwachungs Verein, German Technical Inspection Agency). No additional V&V work was required for the operating system software, the Function Block library, or the SPACE tool.

The AREVA NP procedure guidance in effect at the time of the Concept Activity for Unit 1 only defined the initial software V&V plan as an output for this Activity. IEEE Std 1012-1986 and IEEE Std 1012-1998 both identify a Concept Documentation Evaluation task. No Concept Documentation Evaluation was performed for Unit 1 of the ONS RPS/ESPS project. Duke and AREVA NP evaluated and concluded that the absence of this V&V task had no impact on the Unit 1 application software for the ONS project. The TXS system is a fully integrated and qualified digital system suitable for use in the ONS digital RPS/ESPS. The TXS system is fully described in an NRC approved Topical Report for use in nuclear power plant safety systems. The TXS software architecture and various TXS hardware arrangements are described in the TXS Topical Report to demonstrate the conceptual application of TXS technology in nuclear power plant protection systems.

IEEE Std 1012-1998 also added tasks to the Concept Activity: Criticality Analysis, Hardware/Software/User Requirements Allocation Analysis, Traceability Analysis, Hazard Analysis, and Risk Analysis. These Concept Activity tasks were not performed for Unit 1 of the ONS RPS/ESPS project, since these tasks were not included in the V&V plan in effect at that time. Duke and AREVA NP evaluated and concluded that the absence of these V&V tasks will not adversely impact the Unit 1 application software for the ONS RPS/ESPS project. The applicable Concept Activity tasks will be addressed in the corresponding tasks or the Interface Analysis tasks performed in the later Activities of the Unit 1 application software V&V work. As noted in the TXS Software Program Manual, AREVA NP does not perform a specific hazard analysis as part of the Software Safety Plan and there is no corresponding V&V task.

TXS application software is generated by the SPACE tool. AREVA NP uses SIVAT testing of the application software generated by the SPACE tool to detect errors that would prevent the software from fulfilling its safety function. SIVAT testing, coupled with the FMEA, response time analysis, and FAT are sufficient to ensure that there are no software hazards. Features of the TXS system that limit or mitigate the effects of software hazards are addressed in Section 2.4 of the TXS Topical Report (Reference 2).

3.4.3.2.5 Independent V&V Requirements

> *IEEE Std 7-4.3.2-2003 Clause 5.3.4 states:*
>
> *"The previous section addresses the V&V activities to be performed. This section defines the levels of independence required for the V&V effort. IV&V activities are defined by three parameters: technical independence, managerial independence, and financial independence. These parameters are described in Annex C of IEEE Std 1012-1998.*
>
> *The development activities and tests shall be verified and validated by individuals or groups with appropriate technical competence, other than those who developed the original design.*
>
> *Oversight of the IV&V effort shall be vested in an organization separate from the development and program management organizations. The V&V effort shall independently select*
>
> *a) The segments of the software and system to be analyzed and tested,*
> *b) The V&V techniques, and*
> *c) The technical issues and problems upon which to act.*
>
> *The V&V effort shall be allocated resources that are independent of the development resources.*
>
> *See Annex C of IEEE Std 1012-1998 for additional guidance."*

Section 3 of the TXS Topical Report describes the independence of software V&V activities for the design and qualification of the TXS platform (hardware, operating system software, Function Block library, and application software development tools).

Section 6.2.1 of the TXS Software Program Manual requires that the V&V team report to different reporting chain of command from that of the design functions to provide technical, managerial, and financial independence. The V&V team is made up of personnel who are not involved in the development of the software and are sufficiently proficient in software engineering to ensure that software V&V is adequately implemented. The independent verifiers are also knowledgeable regarding nuclear safety applications. The V&V team indirectly reports to Quality Management, which has oversight authority over the V&V activities.

3.4.3.2.6 Software Configuration Management

IEEE Std 7-4.3.2 Clause 5.3.5 states:

"Software configuration management shall be performed in accordance with IEEE Std 1042-1987. IEEE Std 828™-1998 [B9] provides guidance for the development of software configuration management plans.

The minimum set of activities shall address the following:

a) Identification and control of all software designs and code
b) Identification and control of all software design functional data (e.g., data templates and data bases)
c) Identification and control of all software design interfaces
d) Control of all software design changes
e) Control of software documentation (user, operating, and maintenance documentation)
f) Control of software vendor development activities for the supplied safety system software
g) Control and retrieval of qualification information associated with software designs and code
h) Software configuration audits
i) Status accounting

Some of these functions or documents may be performed or controlled by other QA activities. In this case, the software configuration management plan shall describe the division of responsibility.

A software baseline shall be established at appropriate points in the software life cycle process to synchronize engineering and documentation activities. Approved changes that are created subsequent to a baseline shall be added to the baseline.

The labeling of the software for configuration control shall include unique identification of each configuration item, and revision and/or date time stamps for each configuration item.

Changes to the software/firmware shall be formally documented and approved consistent with the software configuration management plan. The documentation shall include the reason for the change, identification of the affected software/firmware, and the impact of the change on the system. Additionally, the documentation should include the plan for implementing the change in the system (e.g., immediately implementing the change, or scheduling the change for a future version)."

Section 5.2 of the TXS Topical Report describes the software configuration management plan for the design and qualification of the TXS platform (hardware, operating system software, Function Block library, and application software development tools).

Section 5 of the TXS Software Program Manual describes the Software Configuration Management Plan for the TXS projects in the U.S. The Software Configuration Management Plan describes the process for identifying software configuration items, controlling the implementation of and changes to software, recording and reporting the status of changes, and verifying the completeness and correctness of the released software. The Software Configuration Management Plan follows the guidance of IEEE Std 828-1990, "IEEE Standard for Software Configuration Management Plans," and IEEE Std 1042-1987, "IEEE Guide to Software Configuration Management," with the exception of the use of a configuration control board. The exception regarding the use of a configuration control board is acceptable, since the members of such a configuration control board would include the project team members that deal with each other on a daily basis. Software changes are tracked via the open item disposition process, which requires an evaluation of document and software changes. A configuration control board would duplicate other existing processes by using the same personnel. IEEE Std 828-1990 and IEEE Std 1042-1987 are endorsed by RG 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."

Software vendor controls are described in TXS Software Program Manual Section 3.10. AREVA NP GmbH developed the TXS system software and implemented an approved software QA program for the life cycle of the TXS software. AREVA NP GmbH is an approved supplier for AREVA NP Inc. Software in the TXS system software package is uniquely identified and is subjected to an incoming inspection and is base-lined for configuration control. No other safety-related software (Safety Integrity Level-4) is required to be procured during the software life cycle of TXS projects at AREVA NP.

Additional software, such as the software running on the Gateway or GSM, do not perform design basis accident mitigation functions and may be classified with a lower SIL classification that is appropriate to the relative importance to safety. These software elements do not run on the safety processors computers and do not perform any safety functions. They can be classified at lower SIL levels than the safety-related application software running on the safety processors because they are not directly a part of the safety function. This approach is in accordance with IEEE Std 1012-1998, which bases SIL classifications on probability of occurrence and severity of the consequences. A criticality analysis assigns the appropriate SIL classification to the non-safety related software elements.

3.4.3.2.7 Software Project Risk Management

IEEE Std 7-4.3.2 Clause 5.3.6 states:

"Software project risk management is a tool for problem prevention: identifying potential problems, assessing their impact, and determining which potential problems must be addressed to assure that software quality goals are achieved. Risk management shall be performed at all levels of the digital system project to provide adequate coverage for each potential problem area. Software project risks may include technical, schedule, or resource-related risks that could compromise software quality goals, and thereby affect the ability of the safety computer system to perform safety related functions. Software project risk management differs from hazard analysis, as defined in 3.1.31, in that hazard analysis is focused solely on the technical aspects of system failure mechanisms.

Risk management shall include the following steps:
a) Determine the scope of risk management to be performed for the digital system.
b) Define and implement appropriate risk management strategies.
c) Identify risks to the software project in the project risk management strategy and as they develop during the conduct of the project.
d) Analyze risks to determine the priority for their mitigation.
e) Develop risk mitigation plans for risks that have the potential to significantly impact software quality goals, with appropriate metrics for tracking resolution progress. (These risks may include technical, schedule, or resource-related project risks that could compromise the ability of the safety computer system to perform safety related functions.)
f) Take corrective actions when expected quality is not achieved.
g) Establish a project environment that supports effective communications between individuals and groups for the resolution of software project risks.

Additional guidance on the topic of risk management is provided in IEEE/EIA 12207.0-1996, and IEEE Std 1540™-2001 [B13]."

AREVA NP uses a standardized project management process to assess project risks, as described in Section 3.13 of the TXS Software Program Manual. This methodology is used to identify, assess, monitor, and control areas of risk that arise during the software development project. The methodology utilizes a process to rate the complexity and risks of projects to optimize project planning and execution. In the course of project execution, the project risks are monitored, and the original rating is reviewed to determine if the rating needs to be modified.

[ ]

3.4.3.2.8 Software Lifecycle Output Documents

All AREVA NP design work, products, and services provided for the ONS RPS/ESPS digital upgrade project are performed to the requirements of the AREVA NP QMM (Reference 11.) These quality requirements are supplemented by the additional QA requirements for TXS projects described in the TXS Topical Report and the TXS Software Program Manual. Project documentation used as design input or delivered to the customer as design output is stored in the AREVA NP records management system. Similarly, project records arising from QA inspections and audits are stored in the AREVA NP records management system.

Documents associated with Software Life Cycle Process Planning, Software Life Cycle Process Implementation, and Software Life Cycle Development Process Outputs are listed in Table 1-2 and are available for NRC review as indicated in that table.

3.4.3.3 Conclusion

The programs, policies, procedures, and activities described in Section 3.4.3 provide reasonable assurance that the computer hardware and software components of the ONS digital RPS/ESPS have been developed with high quality consistent with industry standards and in accordance with Duke and AREVA NP software QA programs.

3.4.4 Equipment Qualification

> *IEEE Std 7-4.3.2-2003, Clause 5.4 states:*
>
> *"In addition to the equipment qualification criteria provided by IEEE Std 603-1998, the requirements listed in 5.4.1 and 5.4.2 are necessary to qualify digital computers for use in safety systems."*

IEEE Std 7-4.3.2 Clauses 5.4.1 and 5.4.2 address computer system testing and qualification of existing commercial computers, respectively. Computer system qualification testing is discussed in Section 3.3.4 of this Enclosure.

The ONS digital RPS/ESPS does not contain any commercial digital computers therefore Clause 5.4.2 does not apply.

Section 3.3.4 addresses compliance with IEEE Std 603 requirements for equipment qualification. The TXS system is considered acceptable for safety-related service by the NRC as documented in NRC SER dated May 5, 2000. Therefore, the provisions within Section 5.4.2 of IEEE Std 7-4.3.2 regarding qualification of existing commercial-grade computers do not apply.

A multi-level test program is used to ensure quality in the hardware and software products. The testing addresses the hardware and software used, from input to output terminals. The testing also includes the TXS Service Unit and TXS Gateway. The overall qualification testing includes the following:

- Component Testing
- Qualification Testing
- Development Testing

RPS/ESPS equipment qualification testing was performed with the computers functioning, with software and diagnostics as representative of operational service. Future testing, including Factory Acceptance, Site Acceptance, Installation, and Post Installation, will be performed with the computers fully functional as well. All portions of the computer used for safety functions, or whose operation or failure could impair safety functions, will be tested. The testing will demonstrate compliance with performance requirements related to safety functions.

3.4.5 System Integrity

> *IEEE Std 7-4.3.2-2003, Clause 5.5 states:*
>
> *"In addition to the system integrity criteria provided by IEEE Std 603-1998, the following are necessary to achieve system integrity in digital equipment for use in safety systems:*
> *— Design for computer integrity*
> *— Design for test and calibration*
> *— Fault detection and self-diagnostics"*

In addition to the system integrity discussed in IEEE Std 603 and the guidance in NUREG 0800 Appendix 7.1-C, IEEE Std 7-4.3.2-2003 includes criteria in sub-clauses 5.5.1 through 5.5.3 on designs for computer integrity, test and calibration, fault detection and self diagnostics activities.

The TXS safety system has been designed and tested to confirm that the equipment demonstrates system performance adequate to ensure completion of protective actions over the range of transient and steady state plant conditions. TXS safety system response times were calculated during the design phase. These response times will be demonstrated to be consistent with plant specific accident analysis acceptance criteria during the testing phase. Failure modes are discussed in Paragraph 2.7, "Fault Tolerance Features" of the TXS Topical Report (Reference 2).

3.4.5.1 Design for computer integrity

The integrity of the TXS processing (computer) functions are assured by power supply quality monitoring and software module qualification to assure avoidance of inadmissible numerical operations. The direct current power supply quality supplied to the TXS processing modules is continuously monitored for high or low voltage. If either a high or low condition is sensed by the system monitor, the TXS processor is shutdown and its outputs are placed in a defined safe state (zero output). When power quality is restored, the monitor will signal that it is permissible to restart the system during which time the full complement of startup tests is run. If any of the startup tests are negative the system will halt for diagnosis.

3.4.5.2 Design For Test And Calibration

Refer to Section 3.3.7, Capability for Test and Calibration, of this Enclosure.

3.4.5.3 Fault Detection And Self-Diagnostics

The RPS/ESPS provides automatic monitoring of each of the input signals in each channel to perform online signal validation against required acceptance criteria and to provide hardware functional validation for performance of continuous channel checking. These cyclic system monitoring functions improve the availability of the system and reduce the maintenance burden. The TXS safety system software performs a continuous online automated cross channel check, separately for each channel, and continuous online signal fault detection and validation.

Section 3.3.5, System Integrity, of this enclosure addresses system integrity criteria provided by IEEE Std 603-1998.

3.4.6 Independence

> *IEEE Std 7-4.3.2-2003, Clause 5.6 states:*
>
> *"In addition to the requirements of IEEE Std 603-1998, data communication between safety channels or between safety and non-safety systems should not inhibit the performance of the safety function..."*

The Oconee digital RPS/ESPS system design complies with IEEE Std 7-4.3.2-2003. The TXS Topical Report and associated SER provide generic information about the TXS system, showing compliance with the criteria, based on overall system design. Plant specific design documents describe how the design is implemented for Oconee.

IEEE Std 7-4.3.2-2003 specifies computer-specific requirements to supplement the criteria and requirements of IEEE Std 603-1998. Regulatory Guide 1.152, Revision 2, endorses IEEE Std 7-4.3.2-2003 as an acceptable method for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants.

3.4.6.1 Data communication between safety channels

3.4.6.2 Data Communication between safety and non-safety systems

The fiber-optic communication equipment (SLLM and fiber optic cable) is qualified as Class 1E isolation and provides the required electrical separation between each protective channel, between the MSI and the media converter and then the TXS Service Unit. Fiber-optic isolation prevents internal electrical faults from propagating from one protective channel to the other redundant channels.

The communication path between the safety processor and the MSI uses SL21 communication interface modules, SLLM L2 link modules for converting electrical signals to optical signals, and fiber-optic cables to interface between processors.

The MSI computer also collects and processes analog and binary plant status information received from the protection channels, and prepares MSI annunciation and indication information suitable for output to indicator panels in the control room and the plant information system/process computer.

3.4.7 Capability for Test and Calibration

> *IEEE Std 7-4.3.2-2003, Clause 5.7 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 'Capability for Test and Calibration' requirements are addressed in Section 3.3.7 of this Enclosure.

3.4.8 Information Displays

> *IEEE Std 7-4.3.2-2003, Clause 5.8 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 'Information Display' requirements are addressed in Section 3.3.8 of this Enclosure.

3.4.9 Control of Access

> *IEEE Std 7-4.3.2-2003, Clause 5.9 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 "Control of Access" requirements are addressed in Section 3.3.9 of this Enclosure.

3.4.10 Repair

> *IEEE Std 7-4.3.2-2003, Clause 5.10 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 'Repair' requirements are addressed in Section 3.3.10 of this Enclosure.

3.4.11 Identification

> *IEEE Std 7-4.3.2-2003, Clause 5.11 states:*
>
> *"To provide assurance that the required computer system hardware and software are installed in the appropriate system configuration, the following identification criteria specific to software systems should be met:*
> *(a) Firmware and software identification should be used to assure the correct software is installed in the correct hardware component.*
> *(b) Means should be included in the software such that the identification may be retrieved from the firm-ware using software maintenance tools.*
> *(c) Physical identification requirements of the digital computer system hardware should be in accordance with the identification requirements in IEEE Std 603-1998."*

The ONS application software design is documented on function diagrams generated by using the SPACE engineering tool. Two software authentication tools, "**scanmic**" and "**reflist,**" are used for authentication of the application software. These tools support the use of Cyclic Redundancy Check (CRC) checksums for the unambiguous identification of files and directories. The TXS authentication tool "**scanmic**" is used to analyze and document the software configuration of the loadable code (MIC file). "**Scanmic**" reads the version strings for all software components included in a MIC file and calculates the CRC checksum for each software segment included in the MIC file as well as a CRC checksum across the complete MIC file.

The TXS authentication tool "**reflist**" safeguards directory trees and files using CRC checksums. The "**reflist**" tool is used to document the software configuration of the Application Software Code that is installed on the service unit. The "**reflist**" tool creates CRC checksums recursively for all the subdirectories and files within a directory and outputs them in a list. An overall listing of the files (CRC checksums and file sizes) of the Application Software Code as contained in the SPACE database is documented in a Code Configuration document.

Identification may be retrieved from the firm-ware using software maintenance tools. The software version of each System Software component running on RPS/ESPS processors can be read back by the Service Unit at any time. The Service Unit accesses the RPS/ESPS processors through Service Messages which originate from the Service Unit. The messages are routed to the addressed RPS/ESPS processor via the MSI. Since the Service Messages have lower priority in the processing sequence than protection signals, there is no adverse effect on system functionality.

An additional feature of the Service Unit is that several cyber security measures are in place to ensure that the Service Unit cannot adversely affect the software configuration control of the RPS/ESPS processors. Cyber security measures are discussed in more detail in Section 3.8 of this enclosure.

Physical Identification requirements of the digital computer system hardware are addressed in Section 3.3.11 of this Enclosure.

3.4.12 Auxiliary Features

> *IEEE Std 7-4.3.2-2003, Clause 5.12 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 'Auxiliary Features' requirements are addressed in Section 3.3.12 of this Enclosure.

3.4.13 Multi-unit Stations

> *IEEE Std 7-4.3.2-2003, Clause 5.13 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 'Multi-Unit Station' requirements are addressed in Section 3.3.13 of this Enclosure.

3.4.14 Human Factors Considerations

> *IEEE Std 7-4.3.2-2003, Clause 5.14 states:*
>
> *"No requirements beyond IEEE Std 603-1998 are necessary."*

IEEE Std 603-1998 'Human Factors Considerations' requirements are addressed in Section 3.3.14 of this Enclosure.

3.4.15 Reliability

> *IEEE Std 7-4.3.2-2003, Clause 5.15 states:*
>
> *"In addition to the requirements of IEEE Std 603-1998, when reliability goals are identified, the proof of meeting the goals shall include the software. The method for determining reliability may include combinations of analysis, field experience, or testing. Software error recording and trending may be used in combination with analysis, field experience, or testing."*

RG 1.152, Revision 2, states that the NRC does not endorse these quantitative methods alone for meeting its regulations for reliability of digital computer systems in safety-related applications.

Software does not "fail" in the conventional sense the way a hardware component can fail. No analysis can provide a quantitative analysis (in a numerical sense) of the probability of software failure. However, a quality study of the reliability for the TXS software has been documented in the FMEA for the digital RPS/ESPS as discussed in Section 3.7 of this Enclosure.

Hardware reliability is addressed in Section 3.3.15 of this Enclosure.

3.4.16 Sense and Command Features – Functional and Design Requirements

> *IEEE Std 7-4.3.2-2003, Clause 6 states:*
>
> *No requirements beyond IEEE Std 603-1998 are necessary.*

IEEE Std 603-1998 'Sense and Command Features – Functional and Design Requirements' are addressed in Section 3.3.16 of this Enclosure.

3.4.17 Execute Features – Functional and Design Requirements

> *IEEE Std 7-4.3.2-2003, Clause 7 states:*
>
> *No requirements beyond IEEE Std 603-1998 are necessary.*

IEEE Std 603-1998 'Execute Features – Functional and Design Requirements' are addressed in Section 3.3.17 of this Enclosure.

3.4.18 Power Source Requirements

> *IEEE Std 7-4.3.2-2003, Clause 8 states:*
>
> *No requirements beyond IEEE Std 603-1998 are necessary.*

IEEE Std 603-1998 'Power Source Requirements' are addressed in Section 3.3.18 of this Enclosure.

3.5 Pre-Installation Testing, Installation, Post-Installation Testing

The governing testing standards applicable to the digital RPS/ESPS are described in Section 3.5.1 below. Pre-FAT testing conducted for the digital RPS/ESPS is described in Section 3.5.2 below. Factory acceptance testing, site acceptance testing, installation testing, and post-installation testing planned for the RPS/ESPS design change is described in Sections 3.5.3 through 3.5.6 below. A brief description and explanation of the purpose of the testing is also provided.

3.5.1 Governing Test Standards

The process used to develop the tests starts with the requirements identified in the Project Equipment Specifications and Functional Requirements Specifications (both Hardware and Software). Testing ends with the completion of the installation and commissioning tests prior to system turnover to the plant operations staff for use. Once the system is operational, periodic testing and surveillances are required by TSs.

The Requirements Traceability Matrix (Reference Table 1-2, Item 2 of this Enclosure) is used as a tool to ensure all functional requirements are tested.

Software testing is conducted using the guidance of RGs 1.170 and 1.171. Hardware testing is conducted using standards and guidance listed below.

Testing standards and guidance that are specified in the Equipment Specifications include:

IEEE Std 323-1983	IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
IEEE Std 344-1975	IEEE Standard for Seismic Qualification of Class 1E Electric Equipment for Nuclear Power Generating Stations

IEEE Std 383-1974	IEEE Standard for Type Test of Class 1E Electric Cables, Field Splices, and Connectors for Nuclear Power Generating Stations
IEEE Std 1008–1987	IEEE Standard for Software Unit Testing
ANSI Std N45.2.4-1972	Installation, Inspection and Testing Requirements for Instrumentation and Electronics during the Construction of Nuclear Power Generating Stations.
ISA S67-06-1984	Response Time Testing on Nuclear Safety Related Instrumentation Channels
RG 1.180 Rev 1	Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems
SRP BTP HICB-17	Guidance on Self-Test and Surveillance Test Provisions

A common approach to testing is taken. It uses multi-level test programs to ensure quality in both the hardware and software products. Examples of testing utilized for the digital RPS/ESPS include the following:

- Component Testing (Modules, Isolators, Signal Converters, Power Supplies, etc.)
- Qualification Testing (Assembled Hardware in racks or cabinets. This is usually done at an equipment qualification testing facility or by analysis. This may be a complete system or groups of system components)
- Development Testing (Hardware and Software prior to initial assembly as a system. This is usually done by the vendor in a fabrication shop for hardware and a development facility for software.)
- Pre-FAT Testing (Post hardware assembly testing performed at vendor location. See detailed discussion in Section 3.5.2)
- SIVAT testing (Testing of software elements during development)
- Software integration-level testing (Testing of formalized software elements prior to integration with hardware)
- FAT (Testing of integrated Hardware and Software elements in conformance with functional requirements)
- SAT (Testing by ONS to confirm satisfactory receipt of the system and to familiarize operational, engineering and maintenance staff)

- Installation Testing (Testing to verify correct installation and assembly of the system)
- Post Installation Testing (Final testing to formalize procedures that confirms functional and operational requirements at the conclusion of installation)

3.5.2 Pre-FAT Testing

Pre-FAT testing was conducted at the GmbH manufacturing facility in Erlangen, Germany to ensure the hardware components were assembled properly and were ready for FAT. In addition, the AREVA NP SIVAT Testing tested software elements at the lowest level of development. Planning for SIVAT tests occurred concurrently with the software design process. Test case and procedures are generated using SIVAT to check software components individually for typographical, syntactic, and logic errors to ensure that each correctly implements the software design and satisfies the software requirements. Software Testing is conducted in accordance with the SIVAT Test Plan.

3.5.3 Factory Acceptance Testing

The purpose of a FAT is to comprehensively and completely test the components and functions of the digital RPS/ESPS under all credible combinations of operating conditions to ensure that the system meets functional requirements.

A FAT plan has been developed for the digital RPS/ESPS that establishes the framework for conducting the FAT on the system. The FAT Plan provides guidance for the development of the individual test specifications, the procedures, the test reports, the test log, testing incidents reports and the final FAT Summary report. The FAT Plan also provides the guidance for preparing, performing, documenting, resolving and finalizing tests associated with the FAT. Cyber security features of the RPS/ESPS will be tested during FAT.

Software integration testing is performed to examine how software interfaces and interacts with the assumption that objects (e.g., data) it/they manipulate(s) have all passed their respective tests. Software integration tests check how the software functions interact with other software (e.g., libraries) and hardware. Software Integration Testing checks the inter-component communication links and tests aggregate functions formed by groups of components. Software integration testing tests all signal paths using a test machine and special scripts. Software Integration Testing is included in the FAT Plan.

The FAT, in the context of V&V, involves the conduct of tests to execute the completely integrated system. Software system testing is the validation that the software meets its requirements. Validation of the complete system may involve many tests involving all system components. The software system tests exercise only those system functions that invoke software. The perspective is on the software aspects of the system, and whether the software behaves as intended relative to complete system performance. These tests must be conducted in such a manner as to stress and break the system based on software responses to system inputs (e.g., from sensors, operators, and databases).

3.5.4 Site Acceptance Testing

Once the FAT is completed, the system can be exercised, validated, and otherwise tested by ONS staff. This may be performed with both operational and maintenance procedures, by Duke.

A SAT Plan will be developed to guide the plant staff in the performance of the SAT. The SAT Plan will provide guidance for the development of any individual test specifications, any specific procedures, the test reports, the test log, testing incidents reports and the final SAT Summary report. The SAT Plan also provides the guidance for preparing, performing, documenting, resolving and finalizing tests associated with the SAT.

The SAT is normally performed by rerunning selected portions of the Factory Acceptance Test. The SAT can also be used to:

- Ensure the equipment is thoroughly tested and free of transit faults (loosing of wires, dislodged relays, loosing of component mountings, etc.) that may have occurred during shipment from the vendor to the licensee location,
- Provide a platform for the development, verification and validation of periodic tests, calibration procedures, and operations procedures, and
- Ensure familiarization of the plant staff (engineering, operations, maintenance, training, etc.) with the new replacement equipment.

3.5.5 Installation Testing

Installation Testing is testing to verify installation per drawings or installation specifications. Examples of Installation Tests include:

- Electrical insulation testing (Megger)
- Visual Inspections
- Continuity Checks
- Voltage Checks

Included in installation testing are various inspections. Inspections may be performed by engineering, Quality Control (QC), or by equivalent peers. Examples of inspections include:

- Equipment Conditions (mountings, final installation condition)

- Bolt & Screw Torques
- Equipment assemblies (gaskets, sealants, orientations, etc.)
- Cable and Wiring Separation (distances)
- Contact block inspection (normally open versus normally closed)

Installation testing also includes instrument string calibrations. This testing is performed per approved station maintenance procedures. These calibrations are performed in preparation for post installation testing to verify functionality.

3.5.6 Post-Installation Testing

After installation is complete, the system is fully exercised, verified and validated in its normal operating environment using approved post modification testing procedures. Post Installation Testing is performed prior to and during unit startup extending through to full unit operation if required.

RPS/ESPS Post-Installation Testing will verify proper operation of the system and will validate the operability of system performance which includes:

- Validation of proper system process inputs (pressure, temperatures, flows, flux, etc.)
- Validation of proper system outputs (to recorders, indicators, etc)
- Validation of proper operation of the trip functions for the RPS
- Validation of receipt of the required alarms, indications and operation of the plant computer interfaces
- Validation of proper initiation of plant system mitigation functions for the ESPS
- Validation of isolated system outputs to the plant control system for the required parameters.
- Validation of the proper Reactor Trip logic arrangements (two-out-of-four with all various channel permutations) including CRD breaker trip
- Validation of the proper ESPS actuation logic arrangements (two-out-of-three in either the primary or backup sub-systems)

The above post-installation testing will be performed while the unit transitions from a de-fueled mode during the outage to a full operational mode including power generation utilizing approved test procedures. These test procedures will be evaluated under Duke Energy directives relative to risk management processes. These directives describe administrative controls, responsibilities and duties for identification, direction, control and oversight of risk significant activities at Duke Energy Nuclear sites. The directives describe a hierarchy of risk management controls with respect to infrequently performed test and evolutions. This requires the strictest controls, followed by critical activities and then complex activities. The RPS/ESPS design change encompasses all three of these kinds of activities.

3.6 Operation, Maintenance, and Support

The safety functions of the RPS/ESPS will not change as a result of upgrading the RPS/ESPS from an analog to digital system. The impact of the RPS/ESPS digital design change on TSs (including periodic surveillance tests), procedures, training and the simulator is being evaluated as part of the design change process at ONS. This evaluation is performed to ensure that sufficient and appropriate procedures will be in place to monitor and evaluate error reports generated by the digital RPS/ESPS, maintain configuration control as the new system is repaired, upgraded or modified and ensure documentation is kept up to date. The impact evaluation also ensures that the simulator is updated to allow operator training on the new digital RPS/ESPS.

In terms of system operation, the need for procedures and training was identified early in the design change process. New procedures (and revisions) and training are described further in Sections 3.6.1 and 3.6.2, respectively. Comprehensive formal training will be provided to ONS personnel that addresses all operational features and aspects of the system. Associated with the training aspects of the digital RPS/ESPS, the need for upgrading the simulator was identified. Plans for upgrading the simulator to allow operator training on the new system are provided in Section 3.6.3.

On-going maintenance of the RPS/ESPS includes periodic testing performed at scheduled intervals to detect failures and verify operability. Surveillance testing taken together with automatic self-testing should provide a mechanism for detecting all detectable failures. Periodic tests include surveillance tests required by TSs. Further discussion is provided in Section 3.6.5.

Maintaining configuration control is critical to assure that the licensing basis is preserved. Configuration control at ONS, particularly how it applies to the new digital RPS/ESPS, is described in Section 3.6.4.

3.6.1 Procedures

In 2005 Duke established a team of maintenance procedure writers to determine the scope of procedure revisions and to begin development of the revisions to the existing Maintenance procedures. The procedure team's preliminary evaluation identified approximately 40 new IPs would be required and approximately12 complex revisions to existing IPs, 70 simple revisions to existing IPs, and 15 deletions of existing IPs would be necessary.

AREVA NP was contracted to develop and conduct a Training course specific to the procedure writers needs. The course was held in March 2005. In addition to the existing, dedicated procedure writers, Duke provided two experienced I&C technicians to serve as subject matter experts and assist the procedure team as necessary.

The procedure writers ensure that all procedures are written, verified and validated to comply with the requirements of department directives.

Maintenance procedure development work was suspended in 2006 to allow AREVA NP sufficient time to complete necessary documentation. Maintenance procedure development is scheduled to resume in 2008.

The impact to operation procedures is nominal in comparison to maintenance procedures. Operations personnel will begin their procedure revisions as soon as practical. SAT provides an opportunity to use the equipment to validate aspects of procedural interfaces. Ample time is provided for procedure V&V.

3.6.2 Training

ONS contracted AREVA NP to provide a comprehensive formal training program to train ONS personnel in the operation, maintenance and servicing of the system as installed at ONS. The training program will provide ONS personnel in-depth training of all operational features and aspects of the system, including a review of both the required and recommended maintenance procedures related to software and hardware. These training courses shall utilize the installed revision of the system hardware and software, including all design changes made prior to or during the system implementation. Courses shall be developed to be consistent in format, content, etc. with existing ONS training materials.

ONS contracted AREVA NP to provide the initial system and software training on the TXS. This includes the following courses:

- TXS Introduction
- TXS Hardware
- TXS Software

Course outlines are provided below. Upon completion of each course, training manuals and lesson plans shall be provided to ONS for internal use. Initial training on each course will be completed prior to implementation of the RPS/ESPS design change in accordance with the RPS/ESPS project schedule.

3.6.2.1 Maintenance Procedure Writer Training

Two training sessions were designed to satisfy the identified need of the procedure writers.

Session 1, an Introduction/Overview, introduced the TXS product to the end user. Specific ONS plant applications were identified to the extent appropriate,.

Session 2 built upon the knowledge obtained in Session 1. The course offering was based upon Maintenance and Engineering course materials and specifically designed to fulfill the needs of the Maintenance Procedure Writers.

The Maintenance Procedure Writers training was completed in March 2005.

3.6.2.2 User's Overview Training for System Engineers, I&C Technicians and Operators

The user's overview training course will be an introduction to all operational features and aspects of the system.

The TXS Introduction Course provides an overview of the scope and application for TXS safety-related systems. It is a prerequisite for the hardware, software and system administration courses.

The course is targeted at individuals that need a basic understanding of the TXS system capabilities, structure, and operation. Typical attendees include:

- Management
- Engineering
- Operations
- Maintenance
- Software Engineering
- Quality Assurance
- Procedure Writers

3.6.2.3 Hardware Maintenance Training for System Engineers and I&C Technicians

The hardware maintenance training will be on routine maintenance and troubleshooting techniques. Instruction on the operation of all hardware diagnostic programs will be provided. The course will include operation and troubleshooting on the actual system hardware.

The TXS Hardware Course provides insight into the hardware integration, configuration and maintenance. Each module's operation and indications are covered in depth.

This course provides the detailed system knowledge required by personnel involved in maintenance, surveillance, trouble-shooting and those attending the Software Course. Groups expected to attend this training include:

- Plant Engineering
- Maintenance Technicians
- System Administrators

3.6.2.4 Software Engineering Training

Software engineering training will focus on system software design changes that include configuration control and testing. Software courses will foster a familiarity with off-line procedures of the generation of new programs, operation of peripherals, use of the documentation, use of the console, start-up and shutdown procedures, and the use of off-line debugging aids. The software engineering training will also include reviews of code listings for all the major software subsystems.

The TXS Software Course provides an in-depth look at the TXS software. It provides hands-on instruction in use of the SPACE tool for engineers and maintenance technicians. The knowledge gained in this course supports the understanding of:

- Software control functions
- How software parameters replace set-points
- Generation and checking of TXS software
- Testing using digital control technology
- How to change system parameters
- Input/Output channel testing
- Diagnostics

Groups expected to attend this training include:

- Plant Engineering
- I&C Technicians
- Computer Engineering

3.6.3 Simulator

The simulator will be modified to accurately reflect both the new digital RPS/ESPS and the old analog RPS/ESPS. This will enable Duke to train operators on both configurations. When the RPS/ESPS digital upgrade is completed on all three ONS units, the analog model will be removed.

Duke did not use the simulator as input into the design of the RPS/ESPS digital design change. Rather, the need to modify the simulator is driven by the Duke design change process. The simulator is used primarily for operator training. As such, the simulator must be maintained to support this function.

3.6.4 Configuration Management

Configuration Management (CM) is used to provide assurance to the owner, operator and regulator that a nuclear power plant is designed, operated and maintained in accordance with commitments, which provide for the safety of the public and protect the environment.

The objective of CM is to assure the consistency between design requirements, physical configuration and the facility configuration information (drawings, calculations, etc.) for the nuclear power plant owner, operator and regulator.

Well established, documented and conformed work processes and programs provide assurance that CM is maintained at all times. These same processes and programs are utilized when a CM deficiency is identified through a corrective action or condition reporting program. A quality CM program ensures that all changes are authorized and that conformance (as-built condition) can be proven through documentation and comparison to the physical installation. Changes to the as-built condition of the plant are made only with approved documentation ensuring design requirements are maintained. The physical configuration is bounded by the design and the design is bounded by the design basis. This process assures that the physical configuration is also bounded by the design basis.

With the application of digital equipment utilizing configurable software for nuclear power plant safety systems, an additional element of CM was introduced. Software CM is part of the overall project and plant CM which provides additional methods and tools to identify and control the software throughout its development, use and eventual change or retirement. Software Configuration Management activities include but are not limited to the initial identification of software requirements, the preparation and reviews and approvals of the software developed, the tracking of changes, any testing of software, the independent verifications and validations of the software, the integration of the software with the hardware, any audits or assessments, and the interfacing documentation between vendor/supplier, engineering organization, purchaser and operator.

3.6.4.1 Project Related Configuration Management

Duke defines the requirements for configuration management of Structures, Systems and Components (SSC), including software, at its nuclear facilities in a department directive. Further guidance specifically on software configuration management is provided in another department directive, which requires the preparation of a SDQA document for safety related software. The SDQA document contains key aspects and important elements of software and data QA and also the requirements for vendors and suppliers for a specific project.

Requirements for a configuration management program for both hardware and software are contained in the RPS/ESPS Replacement Project Specifications (refer to Table 1-2, Items 37 and 38, of this Enclosure).

AREVA NP defines the requirements for CM for products and projects in general in an AREVA NP document that addresses their software QA plan. Project and application specific guidance is included in the TXS Software Program Manual (Reference 11) and several OIs addressing software QA plans, software verification and validation plans, software documentation and software and hardware CM. The topical report and OIs provide the programmatic guidance and basis for CM from an AREVA NP perspective.

3.6.4.2 Hardware Related Configuration Management

At ONS, hardware documentation under CM is stored in the Document Control Records Management (DCRM) vault in the Oconee Office Building or in satellite locations in specified work group areas. The individual responsible to the safe-keeping and organization of hardware related documentation is the DCRM supervisor. Individual documents such as specifications, cabinet outlines/layouts, schematics, wiring diagrams, calculations, operating and maintenance manuals, panel outlines/layouts, cable routes, panelboard one-lines, instrument details, location drawings and test reports are located in these locations. Documents are controlled and released by both manual and automated check-out systems and procedures.

The document control process is described in a department directive that addresses both safety related and non-safety related documentation. Design changes are controlled per the programmatic guidance in a department directive. An engineering directive provides guidance for the work place performance of design changes.

AREVA NP hardware related configuration guidance is provided in an AREVA NP OI. Additional project related guidance is contained in an AREVA NP OI for TXS Project Phases.

3.6.4.3 Software Related Configuration Management

At ONS, software under CM is stored in the DCRM vault. The software librarian is the DCRM supervisor. The SDQA document, required to be prepared by the department directive for safety related software, identifies the software elements to be controlled and the documents they will be controlled by. These documents along with the software are transmitted to DCRM to retain and control.

Duke defines the requirements for configuration management of SSC, including software, at its nuclear facilities in a department directive that addresses CM requirements. Further guidance on CM of software is given in another department directive for Duke's SDQA Program. This department directive requires the preparation of a SDQA document for safety related software. The SDQA document contains both the elements of the software and data quality assurance plan and also the elements of the CM plan.

Duke's department directive for document control designates the DCRM Supervisors and their staffs, as custodial owners, having overall responsibility for the physical control of software at ONS. Duke's department directive for records management requires permanent records to be stored in a facility (vault) which is designed to criteria specified in RG 1.88, Revision 2, except as noted in Table 17-1 of the Duke Energy Carolinas QA Topical Report (Reference 7), to protect records from loss.

Primary AREVA NP software CM programmatic guidance is contained in an AREVA NP OI for CM. Additional AREVA NP software related configuration guidance is contained in the TXS Software Program Manual (Reference 11) and OIs for software QA plans and software V&V plans. Additional project related guidance is contained in AREVA NP OI for TXS Project Phases.

3.6.5 Periodic Surveillance

On-going maintenance for the existing analog RPS/ESPS includes periodic testing performed at scheduled intervals to detect failures and verify operability. Periodic tests required by ONS TSs include channel checks, channel functional test, and channel calibrations. This testing provides a mechanism for detecting failures. The digital RPS/ESPS includes design features that will perform channel checks and diagnostic tests automatically and cyclically.

Each RPS/ESPS channel includes design features that will perform independent channel checks automatically and cyclically.

Automatic self-testing features are described in detail in Enclosure 3. These features reduce the time to detect and identify failures and are credited for fulfilling TS channel check requirements and extending the TS surveillance interval for channel functional tests. Further discussion is provided in Enclosure 3.

3.7 Failure Modes and Effects Analysis

The methodology and scope of the Failure Modes and Effects Analysis (FMEA) (refer to Table 1-2, Item 6 of this Enclosure) is provided below. A summary of the results and conclusions is provided below.

3.7.1 Methodology

The ONS RPS/ESPS FMEA was performed using guidance contained in RG 1.53 to verify that the design satisfies the single-failure criterion of IEEE Std 603-1998. IEEE Std 603-1998 references IEEE Std 379-1994 as providing a method acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application of the single failure criterion. The ONS FMEA conforms with the specification requirements of IEEE 379-2000. IEEE Std 379 requires that a systematic analysis of the design be performed to determine whether any violations of the single failure criterion exist. IEEE Std 379 presents a procedure and methods that illustrate the principles that may be used for the performance of a single-failure analysis. It also references IEEE Std 352 as providing other procedures that may be used for the performance of the single-failure analysis. IEEE Std 379 also references IEEE Std 577 as providing further guidance in performing reliability analysis.

The general guidance and principles provided in IEEE Std 379, IEEE Std 352, and IEEE Std 577, as described below, were used to perform the FMEA. In addition, this methodology is consistent with inspection criterion provided in the NRC's SRP, Section 7, regarding guidance provided for the NRC's review of the FMEA in verifying compliance with the single failure criterion and related requirements.

As required by IEEE Std 379, the FMEA is a qualitative analysis that uses a systematic approach to identify all credible failures, evaluate the consequence and effects of failures, and verify that the design satisfies the safety criteria defined by the single-failure criterion.

The ONS Design Basis Document for the ESFAS, also known as the ESPS, states that the ESPS shall meet the single failure criterion of IEEE Std 279-1971 to the extent that:

- No single component failure will prevent a protective system from fulfilling its protective function when action is required.
- No single component failure will initiate unnecessary protective system action where implementation does not conflict with the criterion above.

Therefore, the FMEA success criteria includes the consideration that spurious actuations will not occur due to single failures when in any permissible mode, to include normal operation, parameterization (change enable for test and diagnosis), and when the system is Bypassed.

The FMEA has been performed in compliance with the general principles described above. The analysis has been conducted by following the steps described below:

- The system under analysis is described, including the boundaries of the system and external interfaces.
- The initial condition for the analysis is defined.
- The boundaries of analysis are defined.
- The system is represented in a functional block diagram.
- The level of analysis is established.
- The possible failure modes and associated failure mechanisms are identified.
- The basis for exclusion of certain non-credible failure modes from analysis that may be remotely possible but extremely implausible is provided.
- The credible failure modes are analyzed and the effect on the system is determined.
- The method of failure detection is identified.
- An extended analysis is performed to examine the effects of credible common-cause failures.
- The analysis is documented by tabulating the analysis and recording the results in a table format.

3.7.2 Scope

The ONS RPS/ESPS FMEA scope includes a detailed analysis for all the hardware and software provided for the digital RPS/ESPS. All credible failure modes for the replacement equipment are within the scope including both software-related failures and hardware-related failures. The specific boundary of the FMEA is described and provided in Section 4.3 of the FMEA. The scope of the ONS RPS/ESPS design change is described in Section 2.1 of this Enclosure.

The digital RPS/ESPS is designed in accordance with codes and standards, as well as specified design requirements. Personnel training, Design Qualification, Software V&V, Software Testing, Factory Acceptance Testing, Site Acceptance Testing, and Quality Assurance programs afford protection from software design deficiencies. Software common-cause failures are not subject to single-failure analyses. For additional SWCMF discussion see Section 3.2.3 of this Enclosure.

3.7.3 Results

The FMEA for the Oconee RPS/ESPS digital upgrade demonstrates that credible failure modes of TXS hardware are detectable and that the design complies with the single failure criterion. Potential failures have been systematically investigated to determine bounding failure modes for each component, module or portion of the system. The effects of each failure mode on the system have been determined.

The scope of the detailed FMEA analysis focuses on RPS Channel C and ESPS Channels C1/C2 of the redundant protection channels. There are no significant functional differences between the redundant RPS A, B, C, and D or the ESPS A, B, and C Channels but there are some differences that can be summarized as follows:

- RPS Channel D does not process an associated ESPS Channel. The RPS functions in Channel D are identical to Channel C and are addressed in Attachment 2.
- Channels A and B vital power supplies the RPS/ESPS Channels A and B cabinets, ESPS Voter Odd and Even subsystems and Odd and Even status computers. The Channels C and D vital power is supplied to just the RPS/ESPS Channels C and D cabinets. This most significant difference is addressed by evaluating the effects of failure modes of Channel B vital power in Attachment 1.
- RPS Channel E is non-safety and substantially different from RPS Channels A, B, C, and D and is analyzed in Attachment 5.
- Signals to the ICS are provided from RPS Channels. The inputs for the ICS signals are provided in parallel to the hardware input signals to the TXS input cards, and are configured to maintain separation through the isolating SNV1 cards. The ICS system is non-safety and is outside the boundary of the TXS

FMEA. Thus the effects of failure modes on signals to the ICS are not addressed and the differences in Channel outputs to the ICS are not significant to the safety functions of RPS/ESPS.

The detailed FMEA is organized into Attachments that contain tables for each group of cabinets or hardware that performs similar functions. Within the attachments the discussions follow the order of input signal failures, multiple input signal failures, output signal failures, multiple output signal failures, function processing, and lastly communications failure modes. Where an attachment addresses hardware that is not TXS, such as the RCPPM, the flow of information presented is still generally input to output.

The analyses of the RCPPM, Nuclear Instrumentation (NI) Interface equipment, TXS power distribution, DLPIAS, and the Non-TXS Equipment (TXS Service Unit, TXS Gateway, and interfacing hardware) are structured on a hardware component basis.

The detailed analysis is documented in the following attachments to the TXS FMEA report:

Attachment 1
System Power

This analysis covers failures that would affect power distribution to RPS Channel C (Cabinets 5 and 6), ESPS Channels C1 (Cabinets 5 and 6) and C2 (Cabinet 11), the Even Voters (Cabinets 14 and 15), RPS Channel E and the MSI (Cabinet 16), and the Even Status Cabinet (Cabinet 18)

Attachment 2
RPS C / ESPS C1

This analysis covers failures within RPS Channel C and ESPS Channel C1 (Cabinets 5 and 6)

Attachment 3
ESPS C2

This analysis covers failures within ESPS Channel C2 (Cabinet 11)

Attachment 4
ESPS Even Voter
Subsystem G1

This analysis covers failures in the ESPS Even Voter Subsystem (Cabinets 14 and 15)

Attachment 5 RPS E
and the MSI

This analysis covers failures in the non-safety RPS Channel E and failures within the MSI. RPS Channel E and the MSI do not perform any protection functions (Cabinet 16)

Attachment 6
ESPS Even Status

This analysis covers failures in the ESPS Even Status Cabinet. Actual positions of the ES components at the time of failure is indicated as part of the analysis (Cabinet 18)

Attachment 7
NI Power Range Interface

This analysis covers the Power Range Interface to NI-7, including the control power, power range test monitor, linear amplifiers, voltage control modules and feedback resistors, and detector and bipolar power supplies (Cabinet 5)

Attachment 8
Reactor Coolant Pump Power Monitor-

This analysis considers failures in the RCPPM for RCP 1A1, which is typical for RCP 1A1, 1A2, 1B1 and 1B2

Attachment 9
Diverse LPI Actuation System

This analysis covers the DLPIAS, including the relays and Unit Board pushbuttons (Cabinet 16)

Attachment 10
Future Diverse HPI Actuation System

When completed, this attachment will analyze failure modes and effects for the DHPIAS (Cabinet 16)

Attachment 11
Non-TXS Connections (SU/Gateway)

This attachment discusses failure modes and effects for the Service Unit and Gateway PCs, and for the networking devices (port aggregator, Ethernet switch, and media converter)

Attachment 12
Common Cabinet Monitoring

This analysis covers failures of the monitoring functions for Cabinets 5 and 6 which contain RPS Channel C and ESPS Channel C1. Monitoring functions covered include the Cabinet Alarms, the Door Open alarm, the temperature alarm, the fan alarm, the power supply fault alarms, the Watchdog alarm, and Insertion Monitor alarm.

3.7.4 FMEA Conclusion

3.7.4.1 RPS/ESPS Protective Functions

The architecture of the digital RPS/ESPS was confirmed to contain multiple redundant channels to accomplish all safety functions required to mitigate the effects of design basis events. The credible functional or power failures that could result from the ONS RPS/ESPS hardware and software were examined in the FMEA. It was found that failures in one channel were confined to the affected channel and not propagated to other redundant channels. Failures were considered down to the part, module, subsystem and system levels and included evaluation of impacts to the system functional trips and indications. In accordance with the IEEE 379-2000 methodology, once redundancy and separation are confirmed single failures do not have to be further investigated except at points where the separate RPS/ESPS channels come together. The FMEA was extended in detail to ensure that credible failures are automatically detected or indicated. Periodic testing is recommended where required to ensure that failures affecting the automatic safety functions are detected. The RPS/ESPS channels are commonly addressed by the TXS Service Unit via the MSI. All credible failures of the TXS Service Unit and MSI were evaluated. The FMEA concludes that critical functions required for performing protective actions, during normal and abnormal conditions, will continue to be performed for all credible single failure modes. Further, the FMEA concludes that the failure modes for the digital RPS/ESPS have been adequately considered and that there are no credible failures that could defeat the ability of RPS/ESPS to perform its safety functions. As such, the RPS/ESPS meets the single failure criterion. In the examination of all of these failures and consequences, no spurious RPS Trips, either single or multiple channels, or ESPS actuations were found to occur.

3.7.4.2 RPS Channel E, MSI, TXS Service Unit and Gateway

The FMEA examined the identified failures of RPS Channel E, MSI, non-TXS Connections, TXS Gateway and TXS Service Unit functions and concluded that they have no impact on the completion of RPS/ESPS protective functions.

3.8 Cyber Security Considerations

The Duke and AREVA NP processes and the design features that secure the ONS RPS/ESPS from electronic vulnerabilities are considered sensitive information per 10 CFR 2.390. As agreed during Duke's May 1, 2007 meeting with the NRC on RPS/ESPS cyber security, this information has been provided by a separate Duke submittal. In addressing RPS/ESPS cyber security, Duke considered NEI-04-04, Cyber Security Program for Power Reactors, pending 10 CFR 73.55(m), Digital Computer and Communication Networks, rulemaking on and RG 1.152, Criteria For Use Of Computers In Safety Systems Of Nuclear Power Plants, Revision 2.

This information was submitted by letter dated January 30, 2008. The information submitted demonstrates that the applicable cyber security requirements have been met. This letter is incorporated by references pursuant to 10 CFR 50.32.

3.9 Conclusion

Duke has demonstrated, based on information provided in Chapters 1 through 3 of this Enclosure that the proposed ONS RPS/ESPS design complies with IEEE Std 603-1998 and IEEE Std 7-4.3.2-2003. Further Duke has provided information per the guidelines of RG 1.206, C.I.7 necessary for the NRC Staff to make this finding.

4. Regulatory Evaluation

4.1 Significant Hazards Considerations

Pursuant to 10 CFR 50.91, Duke has made the determination that this amendment request involves a No Significant Hazards Consideration by applying the standards established by the NRC regulations in 10 CFR 50.92. This ensures that operation of the facility in accordance with the proposed amendment would not:

(1) Involve a significant increase in the probability or consequences of an accident previously evaluated:

No. The analog Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) currently described in the UFSAR is being replaced with a digital RPS/ESPS. The proposed TS change extends Required Action (RA) Completion Times (CT) for placing a channel in trip, automates channel checks, and extends the surveillance interval (SI) for channel functional tests. The digital RPS/ESPS performs the same functions that are currently performed by the existing systems and has additional capabilities that justify automation of the channel checks and extension of RA CTs and the SI's for channel functional tests.

The digital RPS/ESPS provides continuous online automatic monitoring of each of the input signals in each channel, performs software limit checking (Signal Online Validation) against required acceptance criteria, and hardware functional validation so that the channel check requirement is cyclically being performed. The TXS functional operational design capabilities demonstrate that the channel functional tests of the complete RPS/ESPS is being performed continuously online by the TXS system. Those portions of the system not within the bounds of this online continuous monitoring have a reliability and availability factor that support channel functional test SI extensions.

Safety features have been designed into RPS/ESPS to prevent spurious actuation. Reactor protection is by four channels with two-out-of-four coincidence logic, and ES features are by three channels with two-out-of-three coincidence logic. This design provides redundancy against the affects of single failures that could cause spurious response. The RPS is used to trip the reactor and ESPS is used to mitigate an accident. Since neither of these functions can initiate an accident, there is no significant increase in the probability of an accident. Since the digital RPS/ESPS provides the same functionality as the existing systems, the proposed design change does not result in a significant increase in the consequences of an accident previously evaluated. Therefore, the installation of the digital

RPS/ESPS does not involve a significant increase in the probability or consequences of an accident previously evaluated.

(2) Create the possibility of a new or different kind of accident from any kind of accident previously evaluated:

No. The analog RPS/ESPS is being replaced by a digital RPS/ESPS with additional capabilities that justify automation of channel checks and extension of channel functional test SIs and RA CTs for placing a channel in trip. As part of the digital upgrade a diverse low pressure injection actuation system (DLPIAS) and a diverse high pressure injection actuation system (DHPIAS) is being installed as additional defense in depth against software common mode failures. These diverse systems are designed to initiate low pressure injection or high pressure injection at a point after the ESPS. The digital RPS/ESPS performs the same functions that are currently performed by the existing systems. Safety features have been designed into RPS/ESPS to prevent spurious actuation. Reactor protection is by four channels with two-out-of-four coincidence logic, and ES features are by three channels with two-out-of-three coincidence logic. The diverse LPI and HPI actuations are by three channels with a two-out-of-three coincidence logic. This design provides redundancy against the effects of single failures that could cause spurious actuation. All Protection System functions and the new diverse actuation system functions are implemented by redundant sensors, instrument strings, logic, and actuation devices that combine to form the protection channels or diverse actuation system channels. There are no postulated failures such as loss of power that differ from those assumed for an analog control system that would prevent proper system response. Therefore, the digital RPS does not introduce new hardware failures that inhibit a Control Rod Drive trip when required and the digital ESPS, DLPIAS or DHPIAS do not introduce hardware failures that inhibit proper operation of Engineered Safeguards equipment or cause spurious actuation. As such, the proposed design change does not create the possibility of a new or different kind of accident from any kind previously evaluated.

(3) Involve a significant reduction in a margin of safety.

No. The proposed change does not adversely affect any plant safety limits, set points, or design parameters. The change also does not adversely affect the fuel, fuel cladding, Reactor Coolant System, or containment integrity. The analog RPS/ESPS currently described in the UFSAR is being replaced with a digital RPS/ESPS. The digital RPS/ESPS performs the same functions that are currently performed by the existing systems. Duke analyzed the response times of the digital RPS/ESPS functions and confirmed that the response times of the new digital systems does not impact the ability of the system to perform its safety function. The additional capabilities of the TXS system justify automation of channel checks and extension of channel functional tests and RA CTs. Therefore, the proposed change does not involve a significant reduction in a margin of safety.

Duke has concluded, based on the above, that there are no significant hazards considerations involved in this amendment request.

4.2 Applicable Regulatory Requirements/Criteria

The following addresses the regulatory requirements and plant-specific design bases related to the proposed change.

4.2.1 Regulatory Requirements

Technical Specification 3.3.1 - "Reactor Protective Systems"

The regulatory basis for TS 3.3.1 is to automatically initiate a reactor trip to protect against violating the core fuel design limits and the RCS pressure boundary during anticipated transients. By tripping the reactor, the RPS also assists the ES Systems in mitigating accidents.

Technical Specifications 3.3.5 - "Engineered Safeguards Protective Systems Analog Instrumentation," and 3.3.7 - "Engineered Safeguards Protective System (ESPS) Digital Automatic Actuation Logic Channels,"

The regulatory basis for TS 3.3.5, and TS 3.3.7, is to automatically initiate necessary safety systems, based on the values of selected unit Parameters, to protect against violating core design limits and to mitigate accidents.

10 CFR 50.36 – "Technical Specifications"

10 CFR 50.36 requires licensees have a TS limiting condition for operation for a structure, system, or component that is part of the primary success path and which functions or actuates to mitigate a design basis accident or transient that either assumes the failure of or presents a challenge to the integrity of a fission product barrier. When a limiting condition for operation (LCO) is not met, a licensee shall shut down the reactor or follow any remedial action permitted by the TSs until the condition can be met. Accompanying LCO and remedial actions are surveillance requirements relating to test, calibration, or inspection to ensure the necessary quality of systems and components is maintained, that facility operation will be within safety limits, and that the limiting conditions for operation will be met.

TSs affected by the RPS/ESPS digital upgrade were evaluated to identify changes needed as a result of this design change. Proposed changes and a justification for these changes are included in Enclosure 3 of this license amendment request (LAR).

10 CFR 50.55a (h) – "Codes and Standards"

10 CFR 50.55a (h) requires the ONS protections systems to meet the requirements of either IEEE Std 279, "Criteria for Protection Systems for Nuclear Power Generating Stations," or IEEE Std 603-1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. The criteria contained in IEEE Std 603–1991 establish minimum functional and design requirements for the power, instrumentation, and control portions of safety systems for nuclear power generating stations.

10 CFR 50.62 – "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants"

10 CFR 50.62 (c) requires that ONS have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

10 CFR 50.62 (c)(2) requires that ONS have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods).

10 CFR 50, Appendix A – "General Design Criteria for Nuclear Power Plants"

The original licensing of ONS precedes the development and issuance of the General Design Criteria (GDC) as they exist in the current regulations. For ONS, the design criteria are termed "Principle Design Criteria (PDC). The PDC for ONS Units 1, 2 and 3 were developed in consideration of the seventy General Design Criteria for Nuclear Power Plant Construction Permits that were proposed by the AEC in a rule-making published for 10CFR Part 50 in the Federal Register of July 11, 1967. ONS UFSAR Section 3.1 lists the seventy criteria proposed by the AEC, together with Duke's response indicating our interpretation of an agreement with the intent of each criterion.

10 CFR 50, Appendix B – "Quality Assurance Criteria"

This appendix establishes QA requirements for the design, construction, and operation of those structures, systems, and components. The pertinent requirements of this appendix apply to all activities affecting the safety-related functions of those structures, systems, and components; these activities include designing, purchasing, fabricating, handling, shipping, storing, cleaning, erecting, installing, inspecting, testing, operating, maintaining, repairing, refueling, and modifying.

Appendix B requires a licensee to have a QA program that complies with the requirements of the appendix. This program shall be documented by written policies, procedures, or instructions and shall be carried out throughout plant life in accordance with those policies, procedures, or instructions. The appendix requires the licensee to identify the structures, systems, and components to be covered by the QA program. The QA program shall provide control over activities affecting the quality of the identified structures, systems, and components, to an extent consistent with their importance to safety.

Duke's Appendix B QA program is described in the Duke Energy Carolinas Topical Report Duke 1-A, "Quality Assurance Program" (Reference 7). The Duke Energy Carolinas QA Program conforms to applicable regulatory requirements such as 10CFR Part 50, Appendix B and to approved industry standards such as ANSI N45.2-1977 and ANSI N18.7-1976 and corresponding daughter standards, or to equivalent alternatives. The Duke Energy Carolinas QA Program also conforms to the regulatory position of the NRC RGs listed in Table 17-1 of the QA Topical Report with the exception of the clarifications, design changes, and alternatives stated therein.

4.2.2 Regulatory Guidance

Note that in many instances, the IEEE Standards endorsed by NRC RGs have been superseded by a later revision of the standard. Later editions of IEEE Standards are acceptable or may be used provided the regulatory positions in the RGs are also addressed.

(1) NEI 06-02 –"License Amendment Request Guidelines," December 2006

(2) EPRI Topical Report (TR)-102348, Revision 1 - "Guideline on Licensing Digital Upgrades, " March 2002

(3) SECY 93-087 - "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," April 2, 1993

(4) Standard Review Plan Branch Technical Position 7-19 - "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," Revision 5, March 2007

(5) Standard Review Plan Branch Technical Position 7-14 - Guidance On Software Reviews For Digital Computer-Based Instrumentation And Control Systems," Revision 5, March 2007

(6) RG 1.47 – "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems," Revision 0, May 1973

(7) RG 1.53 – "Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems," Revision 2, November 2003

(8) RG 1.62 – "Manual Initiation of Protective Actions," Revision 0, October 1973

(9) RG 1.75 – "Physical Independence of Electric Systems," Revision 3, February 2005

(10) RG 1.118 – "Periodic Testing of Electric Power and Protection Systems," Revision 3, April 1995

(11) RG 1.152 - "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2, January 2006

(12) RG 1.153 - "Criteria for Safety Systems" and IEEE Std 603-1991 - "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Revision 1, June 1996

(13) RG 1.168 – "Verification, Validation, reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 1, February 2004

(14) RG 1.169 – "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

(15) RG 1.170 – "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

(16) RG 1.171 – "Software Unit Testing for Digital Computer Software in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

(17) RG 1.172 – "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

(18) RG 1.173 – "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Revision 0, September 1997

(19) RG 1.180 – "Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety Related Instrumentation and Control Systems," Revision 1, October 2003

(20) RG 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)," Revision 0, June 2007; specifically, C.1.7, "Instrumentation and Controls."

(21) RG 1.209 – "Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants," Revision 0, March 2007

4.3 Precedent

The NRC has provided generic safety evaluations for three digital systems for use in safety related applications at nuclear plants; Common Qualified Systems, Tricon Triple Modular Redundant Programmable Logic Controller System, and the TXS Digital Protection System. Duke is using the precedent set by approval of the TXS Digital Protection System to support review and approval of the ONS application of this system. The NRC indicated in the cover letter transmitting the SER for the TXS System that the NRC will not repeat its review and acceptance of the matters described in the report, when the report appears as a reference in license applications, except to assure that the material presented is applicable to the specific plant involved. Section 6.0, Plant Specific Action Items, of the SER identifies actions that must be performed by an applicant when requesting NRC approval for installation of a TXS system. Duke has addressed these action items as indicated in Table 1-1 of this enclosure. Additional discussion of the generic precedent is provided in Section 4.3.1 below.

The NRC has also approved several limited digital applications in safety related systems at nuclear stations. These include the digital upgrade of the Core Protection Calculator which is a part of the Reactor Protection System at Palo Verde Nuclear Station. Duke's review of the Palo Verde application and associated SER concluded that this application was based on an approved generic SER (Common Q) and that Arizona Public Service (APS) Company was required to address a set of plant specific action items for the Palo Verde application of the Common Q system and address any differences in the approved system. This is similar to what Duke has done for the ONS application of the TXS system. Additional discussion of the Palo Verde precedent is provided in Section 4.3.2 below.

4.3.1 Generic

The TXS system, as described in Siemens (FANP) Topical Report EMF-2110 (NP), Revision 1, "TXS: A Digital Reactor Protection System" (Reference 2), will replace the existing RPS and ESPS as described in ONS UFSAR Chapter 7. The signal processing, the signal validation, and the protection logic for these systems will be performed by the TXS System.

By letter dated May 5, 2000, the NRC issued a SER which found the TXS System as described in Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," acceptable for referencing in license applications to the extent specified in the topical report and NRC SER. Based on the information provided and the review conducted, the NRC staff concluded that the design of the TXS system is acceptable for safety-related I&C applications and meets the relevant regulatory requirements. The cover letter to the SER indicates that the NRC staff will not repeat its review and acceptance of the matters described in the report, when the report appears as a reference in license applications, except to assure that the material presented is applicable to the specific plant involved. The cover letter further states that the NRC staff's acceptance applies only to the matters described in the report.

The SER requires the several plant specific actions to be performed by an applicant when requesting NRC approval for installation of a Siemens (AREVA NP) TXS system. The installation prerequisites listed in the SER have been met as noted in Table 1-1. Information provided in Chapters 2 and 3 of this Enclosure also identifies and justifies the differences between the system being installed at ONS and the TXS System approved by the NRC.

4.3.2 Plant Specific

Duke reviewed several plant specific LARs associated with digital upgrades in safety related systems. None involved the complete replacement of the RPS/ESPS. However, one did involve replacement of a portion of the RPS. APS submitted a LAR on November 7, 2002, that supported the replacement of the legacy Core Protection Calculator System (CPCS), which was a part of the Palo Verde RPS, with a Westinghouse Common Qualified (Common Q) digital platform CPCS. APS replaced the CPCS in all three Palo Verde Nuclear Generating Station (PVNGS) units due primarily to parts obsolescence associated with the existing equipment.

The CPCS was replaced with a functionally equivalent, digital Common Qualified (or Common-Q) CPCS provided by Westinghouse Electric Power LLC.

There are many similarities between the Duke LAR for RPS/ESPS and the APS LAR for the CPCS. The APS LAR was based on an NRC approved platform (NRC Common Q SER dated August 11, 2000). As such, APS was required to respond to plant specific action items associated with application of the generic SER. APS also was requested to identify differences between the platform approved by the NRC and the one to be installed at Palo Verde. The NRC used SRP, Revision 4, dated June 1997, which defines the acceptance criteria for this review. Specifically, Section 7 of the SRP addresses the requirements for I&C systems in light-water nuclear power plants. The NRC states that the procedures for review of digital systems appear principally in SRP Appendices 7.0-A, 7.1-A; Sections 7.1, 7.8, and 7.9; and Branch Technical Positions (BTPs) HICB-14, HICB-17, and HICB-21. SRP Appendix 7.1-C and Sections 7.2 through 7.7 provide additional criteria that the NRC staff applied in the review.

Similarly, Duke is using an NRC approved platform (NRC TXS SER dated May 5, 2000). This SER has its own set of plant specific action items that are being addressed as a part of this LAR. As indicated in Section 4.3.1, above, the installation prerequisites listed in the SER have been met as noted in Table 1-1 of the enclosure. Information provided in Chapters 2 and 3 of this enclosure also identifies and justifies the differences between the system being installed at ONS and the TXS System approved by the NRC in the SER.

4.4 Conclusions

Duke has made the determination that this amendment request involves a No Significant Hazards Consideration by applying the standards established by the NRC regulations in 10 CFR 50.92 in Section 4.1 of this Enclosure.

The regulatory requirements and guidance applicable to this LAR are identified in Section 4.2 above. As indicated in Chapter 1 of this enclosure, Duke and NRC collaborated and agreed on the applicable regulatory requirements and guidance for this LAR.

Duke's replacement of the RPS/ESPS is a first of a kind license application. Duke has established precedent regarding the generic TXS system approval and the NRC review and approval scope associated with a plant specific application of this system. Duke also identified a plant specific application involving a safety related digital upgrade with a similar basis for review and approval and used it to the extent practical and applicable for developing this LAR.

5. Environmental Considerations

Duke has evaluated this LAR against the criteria for identification of licensing and regulatory actions requiring environmental assessment in accordance with 10 CFR 51.21. Duke has determined that this LAR meets the criteria for a categorical exclusion set forth in 10 CFR 51.22(c)(9). This determination is based on the fact that this change is being proposed as an amendment to a license issued pursuant to 10 CFR 50 that changes a requirement with respect to installation or use of a facility component located within the restricted area, as defined in 10 CFR 20, or that changes an inspection or a surveillance requirement, and the amendment meets the following specific criteria.

(i) The amendment involves no significant hazards consideration.

As demonstrated in Section 4.1 of this Enclosure, this proposed amendment does not involve significant hazards consideration.

(ii) There is no significant change in the types or significant increase in the amounts of any effluent that may be released offsite.

This LAR will not change the types or amounts of any effluents that may be released offsite.

(iii) There is no significant increase in individual or cumulative occupational radiation exposure.

This LAR will not increase the individual or cumulative occupational radiation exposure.

6. References

1 NRC letter dated May 5, 2000, "Acceptance for Referencing of Licensing Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System."

2 Topical Report EMF-2110(NP), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," dated September 1, 1999.

3 NRC Memorandum dated August 1, 2007, "Summary of July 10, 2007, Conference Call to Discuss the Licensing Plan for the Digital Upgrade to the Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS)."

4 NRC Letter to Duke Energy Corporation dated January 11, 2006, "Review Issues for Digital Upgrade of RPS/ESPS for Oconee Nuclear Stations, Units 1, 2, and 3."

5 Duke letter to NRC dated March 20, 2003, "Defense in Depth and Diversity Assessment Associated with the Digital Upgrade of Oconee's Reactor Protective System and Engineered Safeguards Protective System."

6 The Duke Energy Carolinas Topical Report (Topical Report), Quality Assurance Program.

7 EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety Related Applications in Nuclear Power Plants," December 1996.

8 NUREG 0700, "Human-System Interface Design Review Guidelines," Rev. 2, May 2002.

9 NUREG 0711, "Human Factors Engineering Program Review Model," Rev. 1, 2002.

10 AREVA NP ANP-10272, Software Program Manual for TELEPERM XS™ Safety Systems Topical Report, December 2006.

11 AREVA NP Quality Management Manual, 56-5015885-007, dated June 1, 2007.

Oconee Nuclear Station
Digital RPS/ESPS
License Amendment Request
2007-09

January 2008

Enclosure 8

Evaluation of Proposed Technical Specification Change

Non Proprietary

Description of the Technical Specification Change

The proposed Technical Specification (TS) change revises TS 1.1, 3.3.1, 3.3.3, 3.3.4, 3.3.5, and 3.3.7 and their associated Bases. The TS Bases for 3.3.6 are also revised to reflect changes associated with the RPS/ESPS digital upgrade. The markups of the changes to the Technical Specifications and Bases are included in Attachment 1. Since Oconee Nuclear Station (ONS) TSs are common to three Oconee Units, notes and qualifiers are used where appropriate to distinguish between requirements of Unit(s) with the RPS/ESPS digital upgrade complete and Unit(s) with the RPS/ESPS digital upgrade not complete. The proposed changes to the TS for ONS are described and justified below.

To clearly differentiate TS Bases discussion associated with the old "analog" system and the new "digital" system, the text associated only with the old system is in bold font while the text associated only with the new system is in italics font. This font distinction is being used on a temporary basis as a user aid and will be removed after the last implementation of the change. The font change is not identified as a change in the TS Bases markups provided in Attachment 1.

1. TS 1.1 Definitions

The definition of CHANNEL FUNCTIONAL TEST (CFT) is revised to provide a separate definition for digital computer channels. The revised definition is consistent with the Combustion Engineering Owners Group (CEOG) Standard Technical Specification (STS) definition for CFT and is appropriate for ONS's plant specific application. The revised definition is as follows:

"A CHANNEL FUNCTIONAL TEST shall be:

a. Analog and bistable channels - the injection of a simulated or actual signal into the channel as close to the sensor as practicable to verify OPERABILITY of all devices in the channel required for channel OPERABILITY, and

b. Digital computer channels – the use of diagnostic programs to test digital computer hardware and the injection of simulated process data into the channel to verify channel OPERABILITY.

The CHANNEL FUNCTIONAL TEST may be performed by means of any series of sequential, overlapping, or total channel steps so that the entire channel is tested."

The TELEPERM XS (TXS) SER from the NRC, dated May 5, 2000, Section 4.2 "Surveillance Testing of the TXS System," provides the measures for the TXS implementation of the testing. As referenced in the TXS SER, Report EMF-2341 (P), "Generic Strategy for Periodic Surveillance Testing of TELEPERM XS Systems in U.S. Nuclear Generating Stations," provides the methods for performing the various surveillance testing by TXS. Table 1.1 of EMF-2341 (P) provides a listing of the various surveillance testing and how TXS performs those tests. Functional testing is accomplished by three tests: 1) Continuous self monitoring (Section 2 of EMF-2341 (P)), 2) Periodic input channel tests (Section 5 of EMF-2341 (P)), and 3) Periodic output channel tests (Section 6 of EMF-2341 (P)). Logic System Functional Tests are accomplished by continuous self monitoring (Section 2 of EMF-2341 (P)).

Section 4.1 of EMF-2341 (P) describes the periodic functional tests that must be performed for a TXS system during a refueling outage. Section 2 of EMF-2341 (P), "Continuous Self Monitoring of the TELEPERM XS System," provides the details of the self monitoring features of the TXS. In addition to the continuous self monitoring described in Section 2 of EMF-2341 (P), Section 3 describes the start-up self tests. The periodic functional tests that must be performed are the continuous self-monitoring (Section 2 of EMF-2341 (P)), start-up self tests (Section 3 of EMF-2341 (P)), manual verification of the correct version of the software installed in the individual CPUs by reading the Cyclic Redundancy Check (CRC)-sums, and manual verification of the changeable parameters stored in the Electronically Erasable Programmable Read Only Memory (EEPROM).

2. TS 3.3.1, Reactor Protective System (RPS) Instrumentation

The proposed change revises the Completion Time (CT) for TS 3.3.1 Required Action (RA) A.1. to specify 1 hour for ONS Unit(s) with the RPS digital upgrade not complete and 4 hours for Unit(s) with the RPS digital upgrade complete. The justification for increasing the completion time from 1 hour to 4 hours is provided Section 7 of this Enclosure. A justification to allow automatic tests to fulfill the CHANNEL CHECK requirement is provided in Section 8 of this Enclosure. The CHANNEL FUNCTIONAL TEST is extended by adding a note to SR 3.3.1.4 to indicate that the SR is not applicable to Unit(s) with the RPS digital upgrade complete. Since the CHANNEL FUNCTIONAL TEST is a subset of the CHANNEL CALIBRATION, which is required by SR 3.3.1.5 to be performed on an 18 month frequency, this effectively extends the CHANNEL FUNCTIONAL TEST frequency to 18 months. The justification for extending the CHANNEL FUNCTIONAL TEST frequency to 18 months is provided in Section 9 of this Enclosure. TS Bases 3.3.1 are revised to reflect the above changes and to distinguish where necessary the design differences between Unit(s) with the RPS digital upgrade complete and Unit(s) with the RPS digital upgrade not complete.

3. TS 3.3.3, Reactor Protective System (RPS) – Reactor Trip Module (RTM)

The proposed change revises the TS title to "Reactor Protective System (RPS) – Reactor Trip Component (RTC)" to accommodate the Reactor Trip Module (RTM) of the existing design and the Reactor Trip Relay (RTR) of the new digital system. A note was added to RA A.2 to indicate that it is not applicable to Unit(s) with the RPS digital upgrade complete since the removal of the RTC is only valid for Unit(s) without the RPS digital upgrade. Physical removal of the inoperable RTC is not necessary as the trip signal is registered in the other channels by inter-channel communications. This action causes the electrical interlocks to indicate a tripped channel in the remaining three RTCs.

Each RPS channel powers four Reactor Trip relays associated with that channel. These relays are physically located one per cabinet in RPS A, B, C, and D. RPS channel A cabinet includes relays AA, AB, AC, and AD. AB relay coil is powered by an RPS B binary output, AC coil powered by an RPS C binary output, etc. Each channel's associated relay and wiring is physically separated from the other channels. In each RPS Channel cabinet, the contacts of the four reactor trip relays are wired to provide "two-out-of-four relays de-energized to trip" logic to the Control Rod Drive Breaker undervoltage circuit wired to that channel. RPS A provides "two-out-of-four trip" relay logic to CRD breaker A, RPS B provides "two-out-of-four trip" relay logic to CRD breaker B, etc. The reactor trip relay circuitry is a "de-energize to trip" fail safe design. For loss of power and fail low binary output failure modes, the affected reactor trip relays fail to the tripped condition.

4. TS 3.3.4, Control Rod Drive (CRD) Trip Devices

The TS has been revised to reflect completion of the Digital Control Rod Drive Control System (DCRDCS) upgrade. This revision is based on the fact that all units will have the DCRDCS system installed when the first RPS digital upgrade is installed. This change is administrative since the requirements being removed will no longer apply after completion of the design change on all three ONS Units. The TS bases are also revised to delete all references to the old CRD system. Removal of references to the old system simplifies the TS bases revision need to describe the RPS digital upgrade.

5. TS 3.3.5, Engineered Safeguards Protective System (ESPS) Analog Instrumentation

The proposed change replaces the term "analog" with "input" throughout the TS to accommodate the old and new ESPS design. As such, the title of the TS is change to "Engineered Safeguards Protective System (ESPS) Input Instrumentation." The CT for RA A.1 is revised to specify 1 hour for units the RPS digital upgrade not complete and 4 hours for units with the RPS digital upgrade complete. The justification for increasing the CT from 1 hour to 4 hours is provided in Section 7 of this Enclosure. A note is added to SR 3.3.5.1 to indicate that the SR is not applicable to Unit(s) with the ESPS digital upgrade complete. A justification to allow automatic tests to fulfill the CHANNEL CHECK requirement is provided in Section 8 of this Enclosure. The CHANNEL FUNCTIONAL TEST is extended by adding a note to SR 3.3.5.2 to indicate that the SR is not applicable to Unit(s) with the ESPS digital upgrade complete. Since the CHANNEL FUNCTIONAL TEST is a subset of the CHANNEL CALIBRATION which is required by SR 3.3.5.2 to be performed on an 18 month frequency this effectively extends the CHANNEL FUNCTIONAL TEST frequency to 18 months. The justification for extending the CHANNEL FUNCTIONAL TEST frequency to 18 months is provided Section 9 of this Enclosure. TS Bases 3.3.5 is revised to reflect the above changes and to distinguish where necessary the design differences between Unit(s) with the ESPS digital upgrade complete and Unit(s) with the ESPS digital upgrade not complete.

6. TS 3.3.7, Engineered Safeguards Protective System (ESPS) Digital Automatic Actuation Logic Channels

The proposed change replaces the term "digital automatic actuation logic channels" with "automatic actuation output logic channels" throughout to accommodate the old and new ESPS design. As such, the TS Title is changed to "Engineered Safeguards Protective System (ESPS) Output Logic Channels." The proposed change extends the CHANNEL FUNCTIONAL TEST frequency. This is accomplished by modifying the existing 92 day Frequency of SR 3.3.7.1 to indicate it is applicable to Unit(s) with the ESPS digital upgrade not complete and adding an 18 month Frequency to SR 3.3.7.1 indicating it is applicable to Unit(s) with the ESPS digital upgrade complete. The justification for extending the CHANNEL FUNCTIONAL TEST frequency to 18 months is provided in Section 9 of this Enclosure. TS Bases 3.3.7 are revised to reflect the above changes and to distinguish where necessary the design differences between Unit(s) with the ESPS digital upgrade complete and Unit(s) with the ESPS digital upgrade not complete.

7. Justification for Increasing Completion Time from 1 Hour to 4 hours

The digital RPS/ESPS design, which allows continuous automatic CHANNEL CHECKS and system monitoring, provides the basis for extending the Completion Time (CT) for placing an inoperable channel in trip from 1 hour to 4 hours. Continuous cyclic self monitoring features for channel deviations provide prompt notification to the operator. Current TS requirements require operators to perform a CHECK CHANNEL once per shift. Since the operator will become immediately aware, based on alarms in the control room of the inoperability of another channel versus becoming aware during shiftly channel checks, the proposed 4 hours CT is considered appropriate. The additional CT would allow the operator to investigate the trouble alarm and take appropriate action to address the problem.

These design features are described in detail in Sections 8 and 9 below.

8. Justification for Automating CHANNEL CHECKS

The TXS-based RPS/ESPS automatically performs CHANNEL CHECKS many times each second. Analog inputs to TXS are cyclically checked for range violation and deviation from other redundant analog inputs. On the basis of these automatic features, Duke proposes to credit these automatic tests to fulfill the 12 hour CHANNEL CHECK of TS SR 3.3.1.1 and SR 3.3.5.1 These functions are described in more detail below. The TXS automatic method of performing CHANNEL CHECKS is consistent with the recommended surveillance testing provided in Topical Report EMF-2341(P), Revision 1, "Generic Strategy for Periodic Surveillance Testing of TELEPERM XS Systems in U.S. Nuclear Generating Stations," dated March 2000. This recommended surveillance testing was reviewed by the NRC as part of their review and approval of the TXS Topical Report EMF-2110 (NP), Revision 1 (Safety Evaluation Report transmitted by letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay).

8.1 Range Monitoring of Analog Input Signals (Analog Signal Failure Detection)

Analog signals are processed by the TXS software Function Blocks for conversion from electrical units to physical units. In addition to the value conversion, the software Function Blocks monitor the signal for violation of the measuring range.

The neutron flux signals are an exception in that their normal input range is zero to ten volt direct current (VDC), therefore, the detection of the low end of the span fault is ineffective. This is currently checked by the TS required daily comparison of neutron flux signals to secondary calorimetric power and will not be replaced by an automatic the automatic CHANNEL CHECK.

8.2 Consistency Checks of Redundant Channels (Analog Signal Comparisons)

Each analog signal in all measuring channels (i.e., redundant channels) will be cyclically compared to its respective 2.MAX or 2.MIN value to detect and monitor channel signal deviations. Deviation beyond the established acceptance criteria can be an indication of instrument drift (or other instrument failure) in the channel. Excessive drift is alarmed on the Unit Statalarm and input to the plant OAC. The acceptance criteria (parameter settings) were developed using instrument channel uncertainty terms established in the RPS or ESPS instrument uncertainty and setpoint calculations. Uncertainty terms include drift, Measuring and Test Equipment Uncertainty, and calibration procedure setting tolerances.

8.3 The CHANNEL CHECK Setting Criteria and Requirement

The CHANNEL CHECK setting criteria achieve the following goals:

- Minimize the number of spurious alarms due to expected reading variations identified by the instrument channel uncertainty terms associated with the loop components for each individual channel.
- Identification of excess drift (or other failure) in the channel instrument loops.

In the TXS system, the deviating channel (which is alarmed) is not excluded from processing in the safety calculations, 2.MAX or 2.MIN.. However, when deviations are detected, they are alarmed on the Unit Statalarm panel and input to the plant OAC. Furthermore, the CHANNEL CHECK requirement is met automatically and continuously by the signal validation and comparison functions that are performed cyclically by the TXS RPS/ESPS.

9. Justification for Extending the Frequency of CHANNEL FUNCTIONAL TESTS

The purpose of the CHANNEL FUNCTIONAL TEST is to ensure that the channel is operable.

The operating history of TXS modules demonstrates high reliability. Credible failure modes of TXS modules that can only be identified by test were evaluated to support the proposed CHANNEL FUNCTIONAL TEST interval of 18 months. This evaluation considered the factors recommended by IEEE Std. 338-1987. The combination of self-testing features and the reliability of the TXS equipment support the proposed CHANNEL FUNCTIONAL TEST interval of 18 months plus 25%. This interval is consistent with the recommended surveillance testing provided in Topical Report EMF-2341(P), Revision 1, "Generic Strategy for Periodic Surveillance Testing of TELEPERM XS Systems in U.S. Nuclear Generating Stations," dated March 2000. This recommended surveillance testing was reviewed by the NRC as part of their review and approval of the TXS Topical Report EMF-2110 (NP), Revision 1 (Safety Evaluation Report transmitted by letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay).

Self-testing features and TXS equipment reliability are described in more detail below.

9.3 TXS Reliability and Hardware Failure Rates

A quantitative availability analysis of the TXS-based RPS/ESPS was performed in accordance with IEEE Std. 603-1991. This analysis (AREVA document 32-5061241-00, "ONS1 RPS/ESFAS Controls Upgrade TXS HW Availability Analysis.") documents the quantitative study of expected reliability of the TXS RPS/ESPS (hardware) and documents the TXS system susceptibility to various types of faults. Both qualitative analysis (Refer to Table 1-2, Item 6, of Enclosure 1) and quantitative analysis are utilized to identify the possible failure modes, methods for eliminating or reducing the frequency or consequences of the postulated failures, and calculating the probabilities of failures and estimates of reliability and availability. The TXS Availability Analysis demonstrates that the proposed TXS RPS/ESPS system hardware reliability/availability is greater than those values assumed in the ONS Probabilistic Risk Assessment and accident analyses of the existing systems. The availability analysis did not include the TXS output relays. It will be revised to include the output relays and the results of the FMEA.

In accordance with IEEE Std. 338-1987, operating history and reliability data is provided as basis for the proposed test intervals. Specific TXS module operating history in terms of total module years and number of faults or failures were evaluated. All the TXS modules mean time between failure (MTBF) observed data support a CHANNEL FUNCTIONAL TEST at an 18 month plus 25% interval by about two orders of magnitude.

Software is not susceptible to transient, random, aging or environmental related faults. Software does not "fail" in the conventional sense the way a hardware component will fail. Thus, it can be reasonably expected to exhibit no degradation from these factors and no analysis can provide a quantitative analysis of the probability of failure.

This testing is equivalent to CHANNEL FUNCTIONAL TEST verifying that the analog bistable card works electrically because the safety setpoint parameter data is digital and not subject to the drift experienced by analog components.

9.4 FMEA and Periodic Test Recommendations

The TXS FMEA (Refer to Table 1-2, Item 6, of Enclosure 1) makes recommendations for periodic test in cases where the failure mode of a module is not automatically detected or indicated as a result of the failure. These modules and failure modes are listed in AREVA Document 51-9044432-003, "Oconee Nuclear Station RPS/ESPS Surveillance Changes Justification." The failure modes that are not automatically detected or indicated are addressed in this document to support a surveillance interval of 18 months plus 25% for the CHANNEL FUNCTIONAL TEST.