Duke Energy®

DAVE BAXTER
Vice President
Oconee Nuclear Station

Duke Energy Corporation
ON01VP/7800 Rochester Highway
Seneca, SC 29672

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

September 30, 2008

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

Attention: Document Control Desk

Subject: Duke Energy Carolinas, LLC
Oconee Nuclear Station, Units 1, 2, and 3
Docket Numbers 50-269, 50-270, and 50-287
Request for Additional Information for License Amendment Request for Reactor Protective System/Engineered Safeguards Protective System Digital Upgrade, Technical Specification Change (TSC) Number 2007-09, Supplement 5

On January 31, 2008, Duke Energy Carolinas, LLC (Duke) submitted a License Amendment Request (LAR) to address replacement of the existing Oconee Nuclear Station (ONS) analog based Reactor Protective System (RPS) and Engineered Safeguards Protective System (ESPS) with a digital computer based RPS/ESPS. By letter dated August 20, 2008, Duke received request for additional information (RAI) associated with this LAR. Enclosures 1 and 2 contain Duke's responses to the RAI.

Information contained in Enclosure 1 (not including Attachments 1 and 2) and 2 is classified by AREVA NP as proprietary. The appropriate affidavits from AREVA NP are provided in Enclosure 3 in accordance with the provisions of 10 CFR 2.390. Enclosure 4 provides a list of commitments being made as a result of this response. The Unit 1 RPS/ESPS Site Acceptance Test Plan (Item 44 of Table 1-2 of Oconee RPS/ESPS LAR dated January 31, 2008, is provided in Enclosure 5. A non proprietary version of Enclosure 1 has been provided in Enclosure 6.

The responses to RAI questions 28, 40, 80, and 84 describe design features and administrative controls that secure the ONS RPS/ESPS from electronic vulnerabilities. Duke considers this to be sensitive information and request that it be withheld form public disclosure pursuant to 10 CFR 2.390. The sensitive information associated with each response is bracketed.

Enclosures 1 (not including Attachments 1 and 2) and 2 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

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

Very truly yours,

Dave Baxter, Vice President
Oconee Nuclear Station

Enclosures:

1. Duke Response to Request for Additional Information – Proprietary
2. AREVA Documents - Proprietary
3. AREVA NP Affidavit
4. List of Regulatory Commitments
5. Oconee SAT Plan
6. Duke Response to Request for Additional Information – 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

Mr. L. A. Reyes, Regional Administrator
U. S. Nuclear Regulatory Commission - Region II
Atlanta Federal Center
61 Forsyth St., SW, Suite 23T85
Atlanta, Georgia 30303

Mr. G. A. Hutto
Senior Resident Inspector
Oconee Nuclear Station

S. E. Jenkins, Manager
Infectious and Radioactive Waste Management Section
2600 Bull Street
Columbia, SC 29201

Dave 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.

Dave Baxter, Vice President
Oconee Nuclear Station

Subscribed and sworn to me this 30TH day of SEPTEMBER, 2008.

Notary Public

My Commission Expires:

OCTOBER 13, 2015
Date

SEAL

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

bcc: w/enclosures

R. W. Cornett
J. H. Bryan
B. R. Loftis
B. M. Thomas
J. L. Abbott
B. G. Davenport
R. J. Freudenberger
J. E. Burchfield
C. E. Curry
L. F. Vaughn
D. B. Coyle
E. L. Anderson
R. L. Gill – NRI&A
R. D. Hart – CNS
K. L. Ashe - MNS
R. V. Gambrell
D. C. Richardson
M. E. Bailey
B. J. Geddes
NSRB, EC05N
ELL, ECO50
File - T.S. Working
BWOG Tech Spec Committee (5)
ONS Document Management

Enclosure 3

AREVA NP Affidavits for Enclosures 1 and 2

AFFIDAVIT

COMMONWEALTH 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, Supplement 5, Enclosure 1*. The following AREVA NP document is provided 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.

Mandy Bourgeois

SUBSCRIBED before me on this 26th day of September, 2008.

Sherry L. McFaden

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AFFIDAVIT

COMMONWEALTH 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 AREVA NP document is provided and referred to herein as the "Document."

- AREVA NP Operating Instruction OI-1457-05, TELEPERM XS Software Quality Assurance Plan

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.

Marie J Burzynski

SUBSCRIBED before me on this 12th day of August, 2008.

S McFad

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AFFIDAVIT

COMMONWEALTH 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 AREVA NP document is provided and referred to herein as the "Document."

- AREVA NP document 51-9001942-004, Unit 1 RPS/ESFAS Controls Upgrade Software Generation and Download

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 11th day of August, 2008.

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AFFIDAVIT

COMMONWEALTH 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 AREVA NP documents are provided and referred to herein as the "Documents."

- AREVA NP document 51-9052960-003, Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade Factory Acceptance Test Plan
- AREVA NP document 51-9010419-007, 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 this Document 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 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 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 Burzynski

SUBSCRIBED before me on this 12th day of August, 2008.

S McFad

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AFFIDAVIT

COMMONWEALTH 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 AREVA NP document is provided and referred to herein as the "Document."

- AREVA NP document 32-5061241-001, Oconee Nuclear Station, Unit 1, RPS/ESFAS TXS Upgrade, Availability Analysis

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 11th day of August, 2008.

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AFFIDAVIT

COMMONWEALTH 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 AREVA NP document is provided and referred to herein as the "Document."

- AREVA NP document 32-9009296-004, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Response Time Calculation

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 11th day of August, 2008.

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AFFIDAVIT

COMMONWEALTH 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 AREVA NP document is provided and referred to herein as the "Document."

- AREVA NP document OI-1460-07, TELEPERM XS Software Configuration Management Plan

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 Buzynski

SUBSCRIBED before me on this 12th day of August, 2008.

S McFad

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

AFFIDAVIT

COMMONWEALTH 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 AREVA NP document is provided and referred to herein as the "Document."

- AREVA NP document 51-9044432-004, Oconee Nuclear Station RPS/ESPS Surveillance Change Justification

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 Buzynski

SUBSCRIBED before me on this 12th day of August, 2008.

S McFad

NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA

SHERRY L. MCFADEN
Notary Public
Commonwealth of Virginia
7079129
My Commission Expires Oct 31, 2010

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.

List of Regulatory Commitments

Commitment	Completion Date
Revise the Software Requirements Specification to clarify the treatment of the software for the TELEPERM XS (TXS) Gateway software, Monitoring and Service Interface (MSI), and the Reactor Protection System (RPS) Channel E functions (Ref. 65(a) & 66).	TBD

Enclosure 5
TSC 2007-09, Supplement 5
September 30, 2008

Oconee SAT Plan

Enclosure 6 – Non-Proprietary
Duke Response to Request for Additional Information

Duke Energy Oconee Nuclear Station Unit 1 **Unit 1 RPS & ES Replacement Project** **Site Acceptance Test (SAT) Plan** **Reference Use**	Revision No. 00 Electronic Reference No. OD100066/67

Table of Contents

1.0 Introduction

1.1 Purpose

The purpose of the Site Acceptance Test Plan is to establish the framework for conducting Site Acceptance (SAT) Testing on the RPS/ES TXS System. The SAT Plan shall insure the RPS & ES replacement system is functionally tested. The SAT Plan provides top level specification for the development of the SAT procedure, individual enclosures, the Test Log, the Test Incident report, and the SAT Summary Report. The SAT will functionally test the system to insure that the requirements in the Equipment Specifications and the Functional Requirements Specification are met.

Testing activities will follow the guidance of IEEE Std. 829-1983, reference 14, as endorsed by Regulatory Guide 1.170, reference 6. This SAT Plan addresses the applicable subjects of IEEE Std. 7-4.3.2-2003, reference 10, as endorsed by Regulatory Guide 1.152, reference 3.

The SAT Plan outlines planning, testing, and administrative control requirements to validate the RPS/ESFAS design. Therefore, the total program to perform the SAT includes both administrative and technical activities.

The SAT Plan organizes aspects of the RPS/ES design to align with administrative controls required to plan and prepare for design validation of the Oconee RPS/ESFAS system. Upon completion of the SAT, the RPS/ES system is ready for installation at ONS. Availability Testing and FAT are to be completed prior to SAT.

Hardware and software are inspected and/or tested to systematically validate functionality and site procedure accuracy under comprehensive operating conditions.

1.2 Background

RPS

The Bailey Meter Company manufactured the existing system. It is a Bailey 880/881/885 based Nuclear Instrumentation and Reactor Protection System. The existing system has been modified and now contains component Source and Wide Range NIs and Flux Imbalance Flow trip string hardware manufactured by Thermo Fisher Scientific and Framatome Technologies, Inc., formerly BWNT, respectively. Bailey Meter Company does not exist in the same capacity as it previously did, and spare parts are not being produced and/or are in limited supply. In addition to parts obsolescence, there is a lack of vendor support available. Additionally, the system is technically obsolete in relation to current technologies and capabilities.

ESFAS

The Bailey Meter Company manufactured the existing system. It also is a Bailey 880/881/885 based Engineering Safeguards Features Actuation System. The same concerns addressed in the previous section (RPS) apply to the ESFAS.

RPS and ESFAS

Oconee must address the system technical obsolescence and life cycle management (LCM) issues commensurate with long term operational objectives. Currently, modern technology systems are being produced that will meet nuclear safety and regulatory standards. This project will refurbish and modernize the RPS/ESFAS by replacing obsolete hardware and by functionally upgrading the systems.

1.3 Scope

The scope of the SAT includes testing the "as-built" hardware and software supplied by AREVA NP Inc. for the ONS RPS/ESFAS TXS System, from the cabinet input terminals to the output terminals. The scope also includes the OAC, Service Unit, Port Tap, Media Converter, Gateway, OAC Client, and Ethernet Switch. The "as-built" configuration represents the actual assembled TELEPERM (TXS) System as it is configured during the following phases leading up to commencement of the SAT as follows:

- Completion of FAT
- Post manufacturing modifications complete
- Shipment from manufacturer to ONS (i.e., "as-delivered")
- Physical Audit Configuration complete and satisfactory
- Completion of Availability Testing

The ONS Site RPS & ES (SAT) shall:

- Ensure that the RPS ES equipment is functionally tested to verify that the Equipment Specifications and Functional Requirements are satisfied in accordance with the guidance of EDM601 Appendix U
- Test the OPC Client interface
- Provide a platform/basis for development of RPS/ES periodic test and calibration procedures
- Provide a platform for validation of RPS/ES operations (ONS Operations will not be involved in test setups) and maintenance procedures
- Ensure ONS technical personnel are thoroughly familiar with the new replacement RPS/ES

The LabVIEW Data Acquisition Equipment, Test Machines and additional test equipment are used to simulate plant conditions and to monitor system outputs. This test equipment is not included in the overall scope of supply but shall be available for performing the SAT. Actual field devices/cabling and equipment shall be utilized in the SAT test setups when applicable.

Tests shall be performed to verify functions required by the RPS and ES specifications and the Functional Requirements Specification, references 19, 18, 20 respectively. These tests will verify that the System Software and plant specific Application Software performs as required.

The SAT Procedure shall consider OE for system interactions. Refer to OE from Keowee Exciter Replacement project (PIP # 06-6935) and Digital Control Rod Drive System Replacement project (PIP # 05-5613 and 06-5224). The SAT Procedure shall verify interactions with plant systems as part of a test setup, (ICS/NI) where practical.

1.4 Project Authorization

The replacement of the Oconee RPS and ES is being performed per the following Oconee design change packages:

- Unit 1 RPS OD100067 EC0000090482
- Unit 1 ES OD100066 EC 0000090423

The Purchase Order for the RPS/ES replacement System is NS0009336.

1.5 Project Plan

The Project Plan, reference 29, is AREVA document number 102-5016868-01 "AREVA Project QA & Execution Plan (Duke Energy Version), Oconee Reactor Protection System (RPS) and Engineered Safeguards Features Actuation System (ESFAS) Replacement Project."

1.6 Quality Assurance (QA) Plan

Components and implementation of this project are QA1. The software for the RPS and ES systems is QA1 and shall be controlled in accordance with NSD-806, reference 24. The SAT Plan and subsequent implementing documents comply with 10CFR50 Appendix B, reference 2, requirements for Design Control and Test Control.

1.7 Software Configuration Management Plan (SCMP)

The SCMP, reference 30, applies to SAT activities. The SCMP applies to test documentation related to the application software throughout the life cycle phases of the RPS/ESFAS project in accordance with IEEE Std 829-1983. Test documents not relating to application software (e.g., operating system software) is controlled with ONS design control and implementing procedures.

1.8 Software Verification and Validation Plan (SVVP)

The SVVP, reference 38 applies to documentation related to the application software throughout the life cycle phases of RSP/ESFAS project. Inspection and test documents that validate application software shall comply with the SVVP. The SAT Plan relies on a comprehensive and accurate accounting of the design from previous design and development phases.

1.9 Software Safety Plan (SSP)

The SSP, reference 37 applies to documentation for the design or modification of TELEPERM (TXS) application software throughout the life cycle phases of the

RPS/ESFAS project. Inspection and test documents associated with the SAT Plan shall comply with the SSP.

1.10 Change Control

The SAT Plan is a controlled life cycle document and shall be, upon approval, reviewed and revised in accordance with NSD-301, reference 22, for design change control and NSD-806, reference 24, for software change control and development. Additional guidance is provided in EM 4.23, reference 26

1.11 SAT Report

The SAT Procedure governs the test report by requiring a summary of all testing activities and an evaluation based on the results. The Duke Test Supervisor prepares the report with verification by QA/QC to comply with IEEE Std. 829. Test documentation is organized for transmittal as permanent documents or records in accordance with NSD-106 and EDM-601.

The Engineering Supervisor approves the SAT Report. Completion of the SAT signifies completion of the testing phase and establishes a final installation configuration.

Post-SAT Pre-Installation Storage:
Protective measures shall include a suitable environment and security for the storage of the "Post-SAT" system prior to installation in the plant. Additional measures in accordance with ANSI/ASME N45.2.2, reference 7, insure storage and handling conform to requirements; the "Post-SAT" system configuration shall remain under control of AREVA until turned over to ONS for commissioning into the Station.

1.12 References

1. NUREG 0700, Revision 1, "Human System Interface Design Review Guideline"
2. 10CFR Part 50 "DOMESTIC LICENSING OF PRODUCTION AND UTILIZATION FACILITIES" Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants" Criteria I "Organization", II "Quality Assurance Program", III "Design Control" V "Instructions, Procedures, and Drawings", VI "Document Control", XI "Test Control" and XVII "Quality Assurance Records"
3. Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
4. Regulatory Guide 1.153, "Criteria for Safety Systems"
5. Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"
6. Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

7. ANSI Std. N45.2.2-1978, "Packaging, Shipping, Receiving, Storage and Handling of Items for Nuclear Power Plants"
8. ANSI Std. N45.2.13-1976, "Quality Assurance Requirements for Control of Procurement of Items and Services for Nuclear Power Plants"
9. ANSI / ASME N45.2.6 – 1978, "Qualification of Inspection, Examination, and Testing Personnel for Nuclear Power Plants"
10. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
11. IEEE Std. 279-1971, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations"
12. IEEE Std. 498-1985, "Requirements for the Calibration and Control of Measuring and Test Equipment Used in Nuclear Facilities"
13. IEEE Std. 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
14. IEEE Std. 829-1983, "IEEE Standard for Software Test Documentation"
15. Siemens Power Corp Topical Report EMF-2110(NP), Rev. 1; "TELEPERM XS: A Digital Reactor Protection System"
16. USNRC: Safety Evaluation by the Office of Nuclear Reactor Regulation – Siemens Power Corporation Topical Report EMF-2110(NP), Rev. 1; ADAMS Accession No. ML003711856
17. Oconee Nuclear Station 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 (TSC) Number 2007-09"
18. OSS-0311.00-00-0012, "Duke Power Company Oconee Nuclear Station Units 1, 2, & 3, Engineered Safeguards Features Actuation System (ESFAS) Replacement Project Specification," AREVA Document 08-1182355-05
19. OSS-0311.00-00-0013, "Duke Power Company Oconee Nuclear Station Units 1, 2, & 3 Reactor Protective System (RPS) Replacement No. Project Specification," AREVA Document 08-1182356-04
20. OSC-8623, "RPS & ESFAS System Functional Description Oconee Nuclear Station Unit 1 for FANP Teleperm XS, Revision 3," AREVA Document 32-5061401-04
21. NSD-106, "Configuration Management"
22. NSD-301, "Engineering Change Program"
23. NSD-800, "Software and Data Quality Assurance Program"
24. NSD-806, "Digital System Quality Program"
25. EDM-601, "Engineering Change Manual"
26. EM-4.23, "Software Control for Digital Control Systems"
27. OD100066, "U1 ESFAS Replacement Modification"

28. OD100067, "U1 RPS Replacement Modification"
29. AREVA Document 102-5016868-001 "Project QA & Execution Plan, Oconee Reactor Protection System and Engineered Safeguards Features Actuation System Replacement Project"
30. AREVA Document 51-9006444-05 "ONS Units 1, 2, & 3RPS/ESFAS Controls Upgrade Software Configuration Management Plan"
31. AREVA Document 01-5067765-01, "Maintenance and User Manual"
32. AREVA Document 51-5023886-002, "Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Failure Modes and Effects Analysis"
33. AREVA Document 66-5065212-001, "Oconee Nuclear Station RPS/ESFAS Replacement Project EQ Summary Test Report"
34. AREVA Document 52-9062040-002, "Oconee Unit 1 RPS/ESFAS Controls Upgrade Requirements Traceability Matrix Report"
35. AREVA Document 51-9052960-003 "Oconee Nuclear Station, Units 1, 2, & 3 RPS/ESFAS Controls Upgrade Factory Acceptance Test Plan"
36. AREVA Document 15-5016715-00 "Oconee Nuclear Station, Unit 1-3 Conceptual Design of the Communication Bridge between TELEPERM XS and the OAC"
37. AREVA Document 51-9005043-005 "Oconee Nuclear Station, Unit 1, 2, & 3 RPS/ESFAS Controls Upgrade Software Safety Plan"
38. AREVA Document 51-9010419-006 "Oconee Nuclear Station, Unit 1, 2, & 3 RPS/ESFAS Controls Upgrade Verification & Validation Plan"
39. AREVA Document 51-9054435-002 "Oconee Nuclear Station, Unit 1, 2, & 3 RPS/ESFAS Controls Upgrade Software Requirements Specification"
40. AREVA Document 51-5065423-007 "Oconee Nuclear Station, Unit 1, 2, & 3 RPS/ESFAS Controls Upgrade Software Design Description"
41. AREVA Document 51-9001942-004 "Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Generation and Download"
42. NSD-704, "Procedure Use and Adherence"
43. MTF Control/Access Agreement for RPS/ES Unit 1, Rev. 1, dated April 10, 2007

1.13 Definitions

- **As-Built** – Designates a known assembled system configuration at a specified phase of testing. The primary "as-built" milestones include "as-delivered", "post-integration" (includes PMMs), and ""Post-FAT".
- **As-Delivered** – Designates the "as-built" system configuration at the time it is shipped from the manufacturer to ONS.
- **Availability Testing** – Performed after completion of FAT to demonstrate a continuous operation of the safety system Related Functions over a period of 30 days with an availability of 99.999 percent or more.

- **Class 1E** - The safety classification of electric equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment. Equipment and systems shall be classified Class 1E only if they fulfill the functions listed in the definition. Identification of systems or equipment as Class 1E based on anything other than their function is an improper use of the term and should be avoided.
- **Control-** designates that a document exists under an administrative configuration management process that ensures quality
- **D in D&D Analysis**- Diversity and Defense in Depth Analysis based on NUREG CR-6303
- **Factory** - Supplier's facility used to integrate the system and perform the FAT
- **FMEA** - Failure Modes and Effects Analysis based on IEEE Std. 352-1987
- **Firmware** - The combination of software and data that resides in read-only memory
- **HMI** - Human-Machine Interface consisting of all hardware and/or software used to convey information to plant personnel. This includes color display devices, display processors, alarm annunciators, analog and digital display devices, recorders, plant computer (OAC) displays, etc
- **Integration Testing** – Testing performed on the TELEPERM (TXS) at AREVA GmbH prior to the FAT for the purpose of declaring the system "Ready for FAT". Includes installation and testing of PMMs
- **LabVIEW Data Acquisition System** - Test Equipment (actually National Instruments equipment with LabVIEW implemented as recorder and simulations tool) used to monitor outputs on the ONS RPS/ESFAS TXS System and simulate the checkback signals of the individual ESFAS components.
- **On-Site (or Site)** - Locations within the Oconee Station facility that are controlled with respect to access by the general public
- **Operating Environment** - The hardware and/or software that are needed to support the use of a software application or system. (e.g. - operating system software, communications software and hardware, compiler, tools, etc.)
- **Station** - Oconee Station Unit
- **Post-FAT** – Designates the "as-built" system configuration at the time FAT testing is successfully completed
- **Post Manufacturing Modification (PMM)** – changes made to the system after manufacturing, but before the start of availability testing
- **Purchaser** – Duke Energy Corporation, Oconee Station
- **Quality Assurance** – All those planned and systematic actions necessary to provide adequate confidence that a system or component will perform satisfactorily in service
- **Response Time (Display)** - The time interval from the request of a new HMI screen display to the completion of the display
- **Response Time (System)** - An output expressed as a function of time, resulting from the application of a specified input under specified operating conditions
- **Site Acceptance Test (SAT)** – Performed by station personnel upon completion of FAT and prior to station installation

- **Safety System** – A system that is relied upon to remain functional during and following design basis events to ensure: (**A**) the integrity of the reactor coolant pressure boundary, (**B**) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (**C**) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines NOTE: The electrical portions of the safety systems, that perform safety functions, are classified as Class 1E. This definition of "safety systems" agrees with the definition of "safety-related systems" used by the American Nuclear Society (ANS) and IBC 60231A (1969-01[B7]
- **Software** - Sequence of instructions suitable for processing by a computer along with procedures, rules and associated documentation and data pertaining to that processing
- **Software Configuration** - A collection of software elements treated as a unit for the purposes of control
- **Supplier** - The Company (i.e., AREVA) contracted to furnish the system
- **System** - The entire assembled equipment
- **Test Machine** - Test equipment used to simulate field inputs and monitors outputs on the ONS RPS/ESFAS TXS System
- **Validation** - The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements
- **Verification** - The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase
- **Verification and Validation (V&V)** – The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements

1.14 Acronyms/Abbreviations

AC	Alternating Current
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
BOM	Bill of Materials
CD	Compact Disc
CFR	Code of Federal Regulations
DC	Direct Current
DHPIAS	Diverse High Pressure Injection Actuation System
DLPIAS	Diverse Low Pressure Injection Actuation System
DVD	Digital Video Disc
EPRI	Electric Power Research Institute
ESF	Engineered Safety Feature
ESFAS	Engineered Safety Feature Actuation System
ESPS	Engineered Safeguards Protective System
EQ	Equipment Qualification

EUT	Equipment under Test
FAT	Factory Acceptance Test
GSM	Graphic Service Monitor
HRM	Hardware Requirements Matrix
I/O	Input/Output
ICS	Integrated Control System
IEEE	Institute of Electrical and Electronics Engineers
ISA	The Instrumentation, Systems and Automation Society
LAN	Local Area Network
HMI	Human-Machine Interface
M&TE	Measuring and Test Equipment
MAC	Media Access Control
MSI	Monitoring and Service Interface
MTF	Maintenance Training Facility at ONS
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulation
OAC	Operator Aid Computer or the Main Plant Computer System
OLE	Object Linking and Embedding
ONS	Oconee Nuclear Station
OPC	OLE for Process Control
OEM	Original Equipment Manufacturer
PCA	Physical Configuration Audit
PMM	Post Manufacturing Modification
Pre-FAT	Before Factory Acceptance Test
QA	Quality Assurance
QC	Quality Control
RCPPM	Reactor Coolant Pump Power Monitor
R.G.	Regulatory Guide
RH	Relative Humidity
RPS	Reactor Protection System
RTM	Requirements Traceability Matrix
SAT	Site Acceptance Test
SCMP	Software Configuration Management Plan
SER	Safety Evaluation Report
SMTA	Simulation Test Apparatus (a voltage, current injector or reading device)
SSP	Software Safety Plan
SCMP	Software Configuration Management Plan
SDD	Software Design Description
SMS	Service Monitor Server
SPACE	Specification and Coding Environment
SRM	Software Requirements Matrix
SRS	Software Requirements Specification
SSP	Software Safety Plan
SVVP	Software Verification and Validation Plan
TR	Topical Report

TXS	TELEPERM XS
USB	Universal Serial Bus
V&V	Verification and Validation
USNRC	United States Nuclear Regulatory Commission

2.0 Test Items

The completely assembled system will be tested during SAT. Test items will be the TXS System with platform and application software installed and ready for operation. The items will be tested using procedures developed for normal operation and maintenance of the RPS & ESFAS systems. The SAT will be used to validate the operation and maintenance procedures where possible.

Software and Hardware for this project was procured in accordance with Duke Energy Equipment Specifications OSS-0311.00-00-0012 and OSS-0311.00-00-0013, references 18 and 19 respectively.

2.1 Software

The Project-Independent (TXS Platform) software operates with the Project-Specific software (ONS Application) in order to meet the requirements of the project specifications.

The following Project-Independent software is installed for the RPS & ESFAS system:

- TXS System Platform Software version 3.0.7A
- TXS Service Unit Software version 3.0.7A
- TXS Gateway Software version 1.0.4
- Graphic Service Monitor Application 3.0.7A
- OPC Server and Gateway Historical Application version 1.0.0
- TXS Test Machine Software version 1.2.1

The following Project-Specific software is installed for the RPS & ESFAS system:

- Application Software (includes project-specific Gateway software)
- GSM Screens

Note: Versions shall be the latest approved and installed and recorded in the corresponding test procedure/enclosure.

The requirements for the Application Software are detailed in the Software Requirements Specification, reference 39. The design for the Application Software is detailed in the Software Design Description, reference 40.

The software items under test will have been transferred to the test field on electronic media in accordance with AREVA NP processes by AREVA prior to the start of SAT. Installations or updates to the all RPS & ES Systems software will be performed in accordance with the Software Generation and Download Procedure, reference 41.

Software user manuals and guides are located in Volume 4 of the Maintenance and User Manual, reference 31.

2.2 Hardware

Inspection and test activities for hardware and software shall overlap where applicable. Software that is necessary to support hardware validation is installed as required.

The hardware for the ONS RPS/ES TXS System consists of items that are specifically designed for use in TXS applications. Such items include TXS subracks and the modules that populate the subracks. Other hardware in the ONS RPS/ES TXS System is either purchased from approved suppliers or is dedicated for use in nuclear safety related applications. Such items include cabinet power supplies, isolation devices, etc.

2.2.1 The hardware items to be tested are as follows:

- CPU Modules
- Communication Modules
- I/O Modules
- Isolation Modules
- Signal Conditioning Modules
- Subracks
- Subrack Power Supplies.
- Keyswitches
- Miscellaneous TXS Support Modules

2.2.2 Peripheral Equipment to be tested includes:

- Isolation Devices (relays, optocouplers, etc.)
- Breakers
- Nuclear Instrumentation Equipment
- Diverse Low Pressure Injection Actuation System (DLPIAS) Equipment
- Diverse High Pressure Injection Actuation System (DHPIAS) Equipment
- Fiber Optic Cables
- Internal Wiring and Cabling
- Miscellaneous Support Equipment

The version/revision levels of the hardware items to be tested are listed in the EQ Summary Test Report, reference 33. Hardware user manuals and guides are in Volume 4 of the Maintenance and User Manual, reference 31.

Field equipment (sensors, actuators), power cables, control room panels, and the OAC are not available as original equipment in the test field; they must be simulated or substituted by equipment with appropriate properties. This equipment is considered equipment supporting the test environment.

The following equipment is considered part of the HMI:

- GSM screen displayed on the TXS Service Unit
- Keyswitches and push buttons on the temporary control panels in the test field
- Indicators and lamps on the temporary control panels, the signaling of which is provided via the LabVIEW equipment
- Data submitted via the Gateway computer to the OAC (an OPC client is to be available in the test field)

3.0 Features to be Tested

The SAT Test is designed to follow the Guidance of EDM-601 Appendix U and NSD-408 to validate the correct functionality of the RPS/ES System. Each enclosure will test specific items/features of the equipment and software. In addition to functions not tested during FAT the plant procedures will be validated to the extent possible during SAT. Interface with peripherals (OAC, Service Unit, Port Tap, Media Converter, Gateway, OAC Client, and Ethernet Switch) will be tested or simulated.

3.1 System Interfaces

In addition to validation of the plant procedures the SAT should validate:

- User Interfaces
- Hardware Interfaces
- Software Interfaces
- Communications Interfaces

3.2 RPS Functions

The following RPS functions will be tested during SAT:

- Function 1 - RPS Trip #1: Nuclear Overpower (Neutron Flux) Trip
- Function 3 - RPS Trip #3: Nuclear Overpower Flux/Flow/Imbalance Trip
- Function 4 - RPS Trip #4: RCS High Pressure Trip
- Function 5 - RPS Trip #5: RCS Low Pressure Trip
- Function 6 - RPS Trip #6: RCS Variable Low Pressure Trip
- Function 7 - RPS Trip #7: RCS High Outlet Temperature Trip
- Function 8 - RPS Trip #8: Reactor Building High Pressure Trip
- Function 9 - RPS Trip #9: Loss of Both Main Feedwater Pumps Trip
- Function 10 - RPS Trip #10: Main Turbine Trip
- Function 11 - RPS Trip #11: Reactor Coolant Pump Power/Flux Trip
- Function 13 - RCS Delta Pressure Average Function
- Function 14 - RPS Miscellaneous Functions
- RPS Channel E/MSI Functions

Trouble alarm testing to include Trip / Reset, Manual / Auto, Bypass including control room interactions.

3.3 ES Functions

The following ES functions will be tested during SAT:

- Function 15 - ESFAS Trip #1: RCS Pressure Low Trip
- Function 16 - ESFAS Trip #2: RCS Pressure Low Low Trip
- Function 17 - ESFAS Trip #3: Reactor Building Pressure High Trip
- Function 18 - ESFAS Trip #4: Reactor Building Pressure High High Trip
- Function 19 - ESFAS Miscellaneous Functions

As a minimum, ESFAS Set 1 and 2 Independence (remove Set 2 from service and prove Set 1 is OK / remove Set 1 and prove Set 2 is OK) Trouble alarm testing to include Trip / Reset, Manual / Auto, Bypass including control room interactions.

3.4 Additional Features to Test

In addition to the RPS and ES Functions tested during FAT, tests shall be performed to verify the functionality of support equipment, monitoring equipment, and other design functionality. The additional features tested are:

1) Cabinet Alarm Monitoring
2) Diverse Low Pressure Injection Actuation System
3) Diverse High Pressure Injection Actuation System
4) Nuclear Instrumentation
5) RPS/ES Hardware Failures
6) Cyber Security
7) Power Alignments & simulated single failure of power supplies.
8) Electrical isolation shall be verified between Station Ground (cabinet, general framework) Buss and Instrument Ground Buss (drain wires/shield, instrument reference ground)
9) ESFAS Odd & Even Channel GO/NO GO Testing
10) Odd & Even Voter Alarm Verification
11) RPS/ESFAS Digital Equipment Calibrations and Functional Tests
12) HPI/LPI Bypass Functions
13) TXS System Processor Verifications
14) DLPIAS/DHPIAS System Calibrations and Testing
15) RPS/ESFAS Statalarm, Event Recorder, and OAC testing
16) RPS Anticipatory Calibrations and Testing
17) Perform a test to check current draw of the system using Power and Mass Calculation data for acceptance criteria

4.0 Features not to be Tested

Features not to test are those associated with a function not within the scope of supplier equipment, validated by other means, or of a nature that does not impact overall system functionality. The SAT Procedure shall impose further requirements to delineate non-tested functional items from the design. The RTM is used as a tool during on-going test scope reviews. These items are associated with, but not limited to the following categories:

a. Features validated by inspection (Note 1)
b. Features validated by analysis including the Failure Modes & Effects Analysis, reference 32 (Note 2)
c. Plant external I/O interface devices (e.g., status lamp/light) or equipment (e.g., control room alarms, control rod trip relays, transmitter)
d. EQ related performance previously verified
e. Accuracy, stability, and sensitivity previously verified by AREVA NP, Inc. in 95/95 testing

Notes:

1) *The SRM and HRM trace the requirements verified through inspections from the specification through to the respective inspection document.*
2) *The SRM and HRM trace the requirements verified through analysis from the specification through to the respective inspection document.*

5.0 Approach

5.1 General

Test activities shall be non-intrusive and non-destructive to the safety related equipment and system under test. The following is a general overview of the SAT activities and support activities:

1) Issue of COC #1, Quality Receipt of equipment and software on site to include Itemized Spare Parts List.
2) Areva to complete availability testing
3) Areva to complete I/O to Field Testing.
4) Plan the SAT activities (this SAT plan)
5) Determine operation and maintenance procedures to be validated in the MTF
6) Prepare test field and test equipment for SAT
7) Complete SAT prerequisites (physical configuration inspections, etc.)
8) Perform SAT
9) Evaluate SAT results
10) Develop SAT Summary Report

5.2 Comprehensiveness

The SAT shall validate to the extent possible all plant operations and maintenance procedures for the RPS and ES Systems.

5.3 Major Activities

5.3.1 SAT Plan

The SAT Plan establishes the framework for conducting SAT on the ONS RPS/ES TXS System. The SAT Plan is the highest tier test document.

5.3.2 Test Field Installation

The connection and setup required to perform SAT shall be done by Duke and AREVA NP, Inc. in the MTF. This will include power and grounding connections and connections to the test field peripherals.

5.3.3 Equipment Power-Up

Prior to SAT, Duke and AREVA NP, Inc. shall power up the ONS RPS/ES TXS System. This shall include verification of appropriate voltages are present and distributed to the correct terminal points throughout the equipment.

5.3.4 Software Generation and Download

Prior to the commencement of SAT, Duke and AREVA NP, Inc. shall install or verify installed all system software in accordance with reference 41.

5.3.5 Availability Testing

Prior to SAT commencement, AREVA NP, Inc. shall complete the Availability Testing.

5.3.6 SAT Procedure

The SAT procedure shall be a single document that includes a series of enclosures. The SAT procedure shall make use of the FAT, Maintenance and Operations procedures (IP's & OP's). Each enclosure shall be a discrete test that can be repeated with consistent results. If possible, the enclosures shall be written such that they can be performed in any logical order to facilitate scheduling. The SAT enclosures should include:

1) Purpose of enclosure
2) Function(s) to be tested
3) Exact procedures to be followed when applicable (AREVA, Maint. & Ops procedures)
4) Precautions and Pre-Job briefing
5) Prerequisites – See sections 5.4.2 through 5.4.
6) A list of any special test equipment needed

7) Test software descriptions and listings, if any
8) Expected results
9) Pass/Fail criteria
10) Suspension Criteria and Resumption Requirements
11) Qualitative and Quantitative acceptance criteria

The procedures (enclosures) to be validated during SAT shall be written by the applicable ONS groups; maintenance, operations, engineering. The list of SAT Enclosures shall be submitted for approval and approved by the OMP Electrical Engineering Supervisor as part of the SAT Procedure approval. Performance of the SAT shall be conducted by qualified Duke and AREVA NP, Inc. personnel as determined by the SAT Test Engineer.

The controlled SAT procedure identifies steps required to operate the system to perform the necessary inspection, testing, and reporting. Each enclosure shall specify its initial conditions prior to performance. The SAT Procedure complies with IEEE Std. 829-1998 guidance, reference 14.

5.5 SAT Reports/Documents

5.5.1 Test Log

The Test Log is the chronological record of activities in the test field. This includes a record of start and stop times of individual tests/enclosures, some test steps, all encountered errors, and day-to-day activities.

5.5.2 Test Incident Report

The Test Incident Report documents any event that occurs during the testing process which requires investigation and resolution. If the event resulted in an Open Item (OI) and/or PIP then the corresponding number from those items shall be listed in the Test Incident Report and Test Log.

5.5.3 SAT Summary Report

The SAT Summary report is a document summarizing testing activities and results. The SAT Summary Report also contains an evaluation of the corresponding test items (enclosures). The completed SAT Procedure or SAT Procedure enclosures should be attached to the SAT Summary Report.

5.5.4 Test Data Retention

Upon successful completion of SAT, the resultant data files from all test/enclosure runs of the SAT Procedure shall be collected on electronic media (CD, DVD, flash drive). The electronic media shall then be stored in accordance with Oconee station policies.

5.5.5 Signature Log

The signature log is a running accumulation of all test personnel and the contained information is only required to be recorded one time by each person involved in the test. Individual information must be entered prior to performing any SAT activities. The Signature Log provides a means for identifying the individual(s)who performed specific test steps or who documented any activities in any log, test procedure or activity. The Signature Log documents the date, printed name, signature, and Initials of all personnel involved in SAT activities.

5.6 Constraints

Constraints include test item availability and test resource availability. The Test Lead is responsible for identifying and resolving constraints with regard to testing. Availability of specialized test equipment and plant support personnel present a specific constraint to testing.

6.0 Item Pass/Fail Criteria

Each enclosure shall detail the specific required qualitative or quantitative acceptance criteria for the ONS RPS/ES TXS System in accordance with RPS and ES Replacement Project Specifications Section 9.3 (OSS-0311.00-00-0012/0013), references 18 and 19 respectively, in order to determine if the test is completed successfully. Test results shall be evaluated during testing to insure compliance with the stated project specifications' test requirements.

Any deviations between the test results and the acceptance criteria shall be dealt with in accordance with section 7.0.

7.0 Suspension Criteria and Resumption Criteria

7.1 General

An orderly approach to suspend and resume validation activities is required during testing in accordance with IEEE Std. 829-1998, reference 14. Procedures being validated are not subject to the requirements of NSD-704 section 7.2. The following sections provide details for the test suspension and resumption criteria.

7.2 Test Suspension Criteria and Resumption Requirements

The performance of SAT shall follow the guidance of NSD-704, "Procedure Use and Adherence," reference 42. Sections 7.2.1 and 7.2.2 are excerpts from NSD-704.

When a procedure discrepancy exists, the system or part thereof shall be placed in a known safe condition. It shall be evaluated to determine if the discrepancy constitutes a procedure deficiency. If the discrepancy does **NOT** affect the scope, intent, or

acceptance criteria of the procedure **OR** prevent satisfactory completion of the procedure, a deficiency does not exist. If the discrepancy affects the scope, intent, or acceptance criteria of the procedure **OR** prevents satisfactory completion of the procedure, the discrepancy is a deficiencies. All discrepancies and deficiency shall be recorded in the Test Log along with personnel that identified the discrepancy or deficiency.

7.2.1 If the procedure discrepancy is not a deficiency:

A. If the discrepancy is with the procedure:
1) If the procedure discrepancy is an obvious typographical or editorial error, a procedure change does not have to be completed prior to completing the procedure.
2) If a procedure change is not needed prior to completion, perform the following:
2.1) Before continuing with the procedure, document as follows:
a. Correct the discrepancy with a black ink pen
b. Initial the correction
c. Obtain Supervisor approval and initials
d. Document the discrepancy in the Test Log
2.2) Initiate a procedure change request
3) If a procedure discrepancy is not editorial, the performer and supervisor should evaluate the need for a procedure change. NA and out of sequence are processes available and may be an option as long as the intent of the procedure is not changed.

B. If the discrepancy is with equipment:
1) Corrective action shall be initiated but does not have to be completed prior to approval of the completed procedure.
2) Determine necessary corrective action. This action may include:
- Performing corrective actions as specified by the procedure
- Requesting "Procedure Changes" to be done in accordance with NSD 703
- Issue a Work Request/Work Order
- Completing other corrective actions as specified by Site Policies (e.g., initiate a PIP)

3) The completion date will be the date:
- Work Request/Work Order was written
- Procedure Change was requested
- PIP was written

4) Complete procedure and obtain final approval.

7.2.2 If the procedure discrepancy is a deficiency:

A If the deficiency affects the acceptance criteria, the supervisor shall evaluate the need for a procedure change prior to completion of the procedure.
1) NA and out of sequence are processes available and may be an option as long as the intent of the procedure is not changed

2) PIPs with operability determinations documented may be justification to complete procedure

B If deficiency affects the successful completion or changes the intent of the procedure, a procedure change shall be approved prior to continuing.

C Procedure deficiencies shall be handled as follows:

1) Stop Work
2) Evaluate condition and place test and equipment in known and controlled condition
3) Enter relevant information in Test Log
4) Notify the Test Supervisor
5) Perform troubleshooting if necessary - see section 7.2.2.1
6) Initiate corrective action including PIP initiation
7) Perform corrective action including a Test Incident Report
8) Verify adequacy of corrective action
9) Complete procedure and obtain final approval

7.2.3 Troubleshooting activities shall:

- Not alter test objectives or acceptance criteria
- Align with an existing test section or validation activity
- Restore the hardware and software configuration to original state prior to completion of activities
- Place the test and equipment in a known and controlled condition upon completion of troubleshooting activities

The names of all personnel that perform and witness troubleshooting activities shall be recorded in the Test Log.

7.3 Test Resumption Criteria

The SAT Procedure shall impose criteria for resuming validation activities and integrate with a process that includes, but is not limited to, the following:

1) Evaluate and disposition applicable open item(s). The disposition shall document the required actions and conditions to resume SAT
2) Verify actions specified in the approved open items resolution are complete to the extent necessary to continue SAT
3) Enter relevant information in the Test Log
4) Resume testing and retesting as applicable

The Test Supervisor shall determine if another SAT enclosure may be performed after one enclosure has been suspended provided that no adverse conditions exist that impact testing commencement/continuation. This action shall be recorded in the Test Log.

8.0 Test Deliverables

Test deliverables are outputs from the test document set. These include, but are not limited to, the following:

- SAT Plan
- SAT Procedure with all Enclosures
- Test Log
- Test Incident Reports including references to PIPs
- Open Items Documentation
- SAT Summary Report

The SAT is a test of the entire RPS and ES systems and does not differentiate between hardware and software testing.

8.1 SAT Procedure

The SAT Procedure shall have the same information and structure as Step 5.3.6:

Each enclosure shall provide the same information if it is not provided for in the body of the SAT Procedure.

It may be necessary to utilize test scripts to perform some of the SAT testing. If test scripts are utilized then they shall be entered in the applicable SAT enclosure in the exact format in which they exist without modification. It is acceptable to utilize AREVA NP, Inc. personnel to develop the test script portion of the SAT enclosure.

8.2 Test Log

The Test Log provides a chronological record of relevant details about the execution of tests following the guidance of IEEE Std 829-1983, reference 14. The Test Log shall have the following format:

- ONS Document or File Number
- Description
- Activity and event entries

8.3 Test Incident Report

The Test Incident Report shall have the following information and structure:

- ONS Document or File number
- Incident Description
- Impact to the test
- Reference to the PIP number
- Summary of the resolution

SAT Summary Report

The SAT Summary Report will be generated to document the successful completion of the SAT and to document any variances incurred during the testing process. The SAT Summary Report shall have the following information and structure:

- ONS Document or File number
- Summary
- Variances
- Summary of Results
- Comprehensive Assessment
- Evaluation
- Summary of activities
- Approvals

The SAT Summary Report shall include the following reviews and approvals:

- Test Lead
- Project Engineer
- Project Manager
- Engineering Supervisor

9.0 Testing Tasks

Test Procedures and Tasks, as identified in the SAT Plan, are based on general areas that encompass the duration from issuance of the SAT Plan to approval of the SAT Test Summary Report. The Tasks are identified and organized in accordance with IEEE Std. 829-1983 guidance, reference 14. The prerequisites are those activities listed in sections 5.4.1 through 5.4.5. The SAT Plan shall encompass all phases of SAT from Planning through issuance of the SAT Summary Report.

There are intertask dependencies between the performance of the prerequisites and SAT Procedures as follows:

1. The SAT Plan must be approved and released before performing any of the SAT Procedure or prerequisites
2. The SAT Prerequisites listed above paragraph must be completed prior to performing any of the SAT procedure or the SAT enclosures
3. The SAT enclosures may be performed in any reasonable order

10.0 Environmental Needs

10.1 Physical Control

The ONS RPS/ES TXS System shall be placed in a controlled environment in accordance with ANSI Standard N45.2.2-1978, Level B, reference 7. Authorized personnel shall be listed on the MTF Control/Access Agreement for RPS/ES Unit 1, reference 43. These requirements include but are not limited to the following:

- The controlled environment shall be well ventilated, protected from intrusion, and protected from fire, flooding, or animal intrusion

- The controlled environment shall be secure in that is protected from vandalism and tampering
- The cabinets shall remain locked whenever the test area is unoccupied or unauthorized personnel are not present
- Only authorized personnel shall have access to the TXS cabinet internals

10.2 Environmental Control

The location of the ONS RPS/ES TXS System under test shall comply with the design requirements regarding environmental requirements for safety related equipment per ANSI Standard N45.2.2-1978, Level B, reference 7, and design specifications, references 18 and 19. These requirements include but are not limited to the following:

- Electrostatic protection measures shall be employed whenever cabinet doors are open
- Environment shall be provided with uniform temperature and humidity controls to prevent condensation within the cabinets. The acceptable ranges are:
  1. Temperature Limits of 60°F to 100°F
  2. Relative humidity Limits of 30 to 80 percent relative humidity, non-condensing

10.3 Access Control to Test Field

Access to the Test Field shall be controlled by the Test Supervisor to insure an orderly and safe conduct of testing. These requirements include but are not limited to the following:

- Personnel access to the test fields shall be minimized to reduce disturbances to testing activities
- No personnel shall enter the test field without Test Supervisor authorization
- Only authorized personnel shall access the test field without escort

10.4 Special Test Tool Needs

Special tools needed for performance of SAT are the Test Machine and LabVIEW Data Acquisition Equipment.

Calibrated equipment shall be available to record the temperature and relative humidity levels of the test field environment throughout the course of the SAT. This equipment shall be able to display the current temperature and relative humidity levels and record the peak values of each. Other special tools include calibrated low level current sources (in the μA range) and fast response recording devices for performing the NI tests. The requirements for all required SAT equipment shall be specified in the applicable enclosure if not specified within the body of the SAT Procedure.

10.5 Other Testing Needs

There shall be a document library readily accessible to the test field. This library shall contain software and hardware detailed design documentation and general product information and/or user manuals. These documents are only intended to be used for reference. A means of connecting to ONS NEDL shall be available in close proximity to the test field.

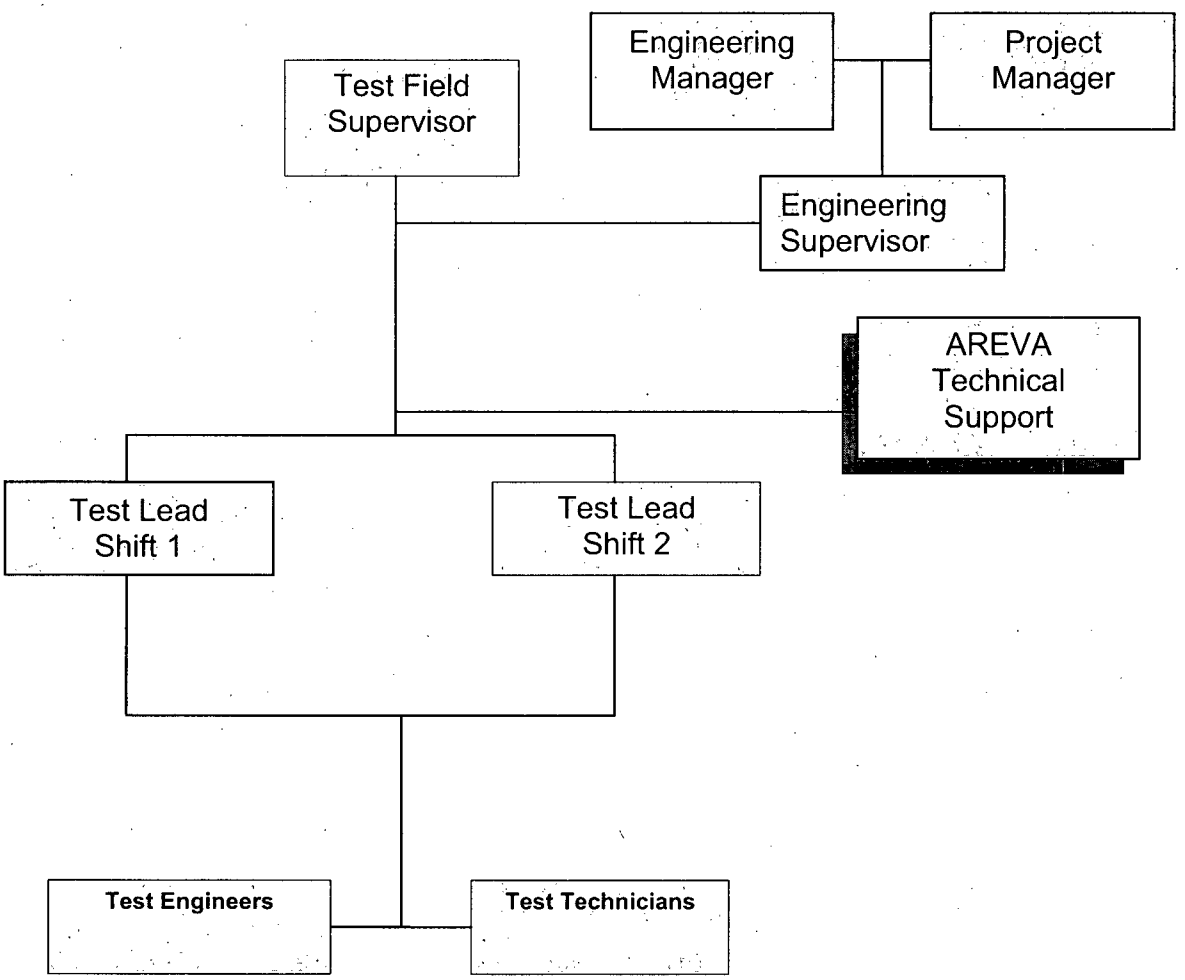
Office space shall be available at or near the test field for test personnel to perform validation of the recorded resultant test data from the operation of the SAT Procedure. The evaluation of results may be performed outside of the test field to allow for other tests/enclosures to be performed.

Any need (tool, document, etc.) that is not readily available to the test team shall be obtained by the Test Lead. Each enclosure of the SAT Procedure shall identify the tools, documents, and equipment required to perform the enclosure steps. The use of calibrated test equipment shall be recorded in the body of the SAT Procedure or the applicable SAT enclosure. Accuracy requirements shall meet general industry practices or be specified in the applicable SAT enclosure.

11.0 Responsibilities

11.1 Organization

The SAT is conducted by test leads and test engineers or technicians from Duke. AREVA NP, Inc. technical support is required at all times during the SAT. The Test Field Supervisor is responsible for enforcing the SAT Plan and SAT Procedure. Responsibilities are reflected by the organization.



11.2 Responsibilities

11.2.1 Supplier – AREVA NP, Inc.

- Provides components of the replacement RPS/ES
- Provides 24/7 RPS/ES hardware and software technical support during SAT
- Provides special test and calibration equipment
- Provides NSS testing simulator
- Reviews/Inspects SAT Plan

11.2.2 Engineering Manager

- Engineering Changes
- Engineering Approvals
- Engineering Reviews

11.2.3 Project Manager

- Plans and schedules SAT activities
- Approves and accepts SAT test results
- Approves Open Item resolutions

11.2.4 Engineering Supervisor

- Approves SAT Plan
- Approves SAT procedure
- Supervises implementation of SAT Plan
- Approves SAT Test Report
- Approves Open Item resolutions

11.2.5 ONS Plant Engineering

- Review/Inspect SAT Plan
- Prepare applicable enclosure(s)
- Perform applicable SAT activities

11.2.6 ONS Operations

- Review/Inspect SAT Plan
- Prepare applicable operations procedures for validation
- Perform applicable SAT activities

11.2.7 ONS Maintenance

- Review/Inspect SAT Plan
- Prepare applicable maintenance procedures for validation
- Perform applicable SAT activities

11.2.8 Test Field Supervisor(s)

- Reviews and implements SAT Plan
- Prepares SAT procedure and/or enclosures
- Coordinates SAT activities
- Reviews SAT results

11.2.9 Test Lead

- Assigns Sat Procedures to the Test Engineers/Technicians
- Ensures proper test conduct
- Conducts pre-job briefs

11.2.10 Test Engineers

- Reviews and implements SAT Plan
- Prepares SAT procedures and/or enclosures
- Performs SAT activities

11.2.11 Test Technician

- Provides maintenance and test support for SAT

12.0 Staffing and Training Needs

12.1 Personnel Staffing

a) 1- Project Manager
b) 1- Engineering Manager
c) 1- Engineering Supervisor
d) 1- Test Supervisor *
e) 1- Test Lead *
f) 2- Test Engineer *
g) 2- Test Technician *
h) 2- AREVA Technical support for 24/7 coverage

* per shift minimum as required and shall be staffed as applicable by maintenance, operations, and engineering personnel.

12.2. Training

The Duke engineering supervisor and Duke Project Lead Engineer shall determine specific training requirements, if any, for personnel performing SAT activities.

13.0 Schedule

The SAT Schedule corresponds to major project milestone events that include:

a) SAT Plan Issuance

b) SAT Plan procedure and enclosure development

c) SAT Prerequisite activities

d) SAT performance

e) SAT Summary Report

The preparation of the SAT Procedure and enclosures as well as the SAT activities themselves is not controlled by this SAT Plan, but by the overall project schedule. Therefore, dates and duration must be retrieved from the overall project schedule.

Milestones are established based on the following logic:

a) SAT Plan is basis for the SAT Procedure

b) FAT completed and system shipped to ONS

c) TXS System, including spare parts list C of C Receipt

d) Completion of 30 continuous days of Availability Testing

e) Completion Areva System I/O to Field Test Run

f) System must be fully assembled prior to SAT

g) SAT completion is signified by the Approval of the SAT Results Report

14.0 Risks and Contingencies

The Project QA and Execution Plan, reference 29, documents the risk assessment for the ONS RPS/ES replacement. The SAT Plan will not control risk management, the Project QA and Project Execution Plan will control risk management.

The testing team is responsible for identifying activities that change the assumed risk.

15.0 Approvals

Prepared by: K. D. Ward Date: 9/11/2008
Name/Title: Kevin Ward / OMP Engineer

Checked by: Joe O'Brien Date: 9/11/2008.
Name/Title: JOE O'BRIEN / OMP ENGINEER.

OPs CDI by: K.D. Ward for Ryan Bowman via telecon Date: 9/11/2008
Name/Title: Ryan Bowman / Sr Operation Spec

Maint CDI by: James H Taylor, Jr. Date: 9-11-2008
Name/Title: JAMES H TAYLOR RPS-ES MAINT PROCEDURE LEAD

ES Eng CDI by: JH Bryan Date: 9/11/08
Name/Title: JH Bryan RES - ES System Engr.

RPS Eng CDI by: ME Bailey Date: 9/16/2008
Name/Title: ME Bailey RES - DPS Supervisor

AREVA CDI by: [signature] Date: 9/11/2008
Name/Title: TOMMY REITER SR. ENGINEER

Approved by: DE Taylor Date: 9-16-08
Name/Title: D. E. Taylor - OMP-ELEC - Supvr.

Enclosure 6 – Non Proprietary
Duke Response to Request for Additional Information

RAI 1
Please provide a description of how adding diverse low-pressure injection (LPI) and high-pressure injection (HPI) have changed the results and conclusion of the D3 analysis.

Duke Response to RAI 1

Duke reviewed the Defense-in-Depth & Diversity (D3) transients presented in the March 20, 2003 submittal to identify the transients in which a diverse Low Pressure Injection (LPI) or a diverse High Pressure Injection (HPI) actuation system would initiate the LPI or HPI Systems, respectively. This review determined that a diverse actuation is not expected to occur for the following events: control rod bank withdrawal at zero power, boron dilution, a two or four pump loss of coolant flow, locked rotor, dropped control rod, turbine trip, steam generator tube rupture, large or small steam line break, loss of main feedwater, loss of offsite power, or main feedwater line break.

The review determined that a diverse actuation may occur for the following events: control rod bank withdrawal, control rod ejection, and small break and large break Loss of Coolant Accidents (LOCAs). For these events, the effect of a diverse actuation of LPI and HPI on the analysis is discussed below.

The control rod bank withdrawal transient is terminated by a Diverse Scram System (DSS) actuation. Following the DSS actuation, a diverse HPI actuation would be expected due to the subsequent decrease in Reactor Coolant System (RCS) pressure. The additional inventory would help replace the fluid lost through the pressurizer relief valves, but would not alter the transient conditions evaluated. The results presented in the D3 assessment during the time frame of interest will not be affected by the addition of either the diverse LPI actuation system or the diverse HPI actuation system.

The control rod ejection transient includes an associated small break LOCA. The reactivity insertion caused by the ejected rod from hot zero power results in an initial pressure increase that ensures DSS actuation. The associated small break LOCA will reduce RCS pressure such that a diverse HPI actuation occurs. The initial reactivity excursion and resulting source term would not be affected by the diverse HPI actuation. Therefore, the results presented in the D3 assessment will not be affected by the addition of the diverse HPI actuation system. A diverse LPI actuation is not expected for this transient. Thus, the diverse LPI actuation system would not affect the results presented in the D3 assessment.

The limiting small break LOCA considered in the D3 analyses is a core flood line break. This break location would result in a rapid diverse HPI actuation, and an early diverse LPI actuation. The transient response crediting these systems would be much improved from the results previously published due to a relatively early actuation time and a significant increase in the ECCS flow being injected into the RCS. For smaller less limiting small break LOCAs,

the diverse HPI actuation would be expected to occur for the entire break spectrum as RCS pressure would be expected to remain monotonic due to the absence of an RPS actuation. The resulting transient response would be bounded by the UFSAR Section 15.14 due to the absence of single failures affecting ECCS flow.

A large break LOCA will result in essentially an immediate diverse HPI actuation and a diverse LPI actuation. For Oconee, the passive core flood tanks accomplish the initial core reflood; pumped ECCS ensures long term core cooling. No credit for a reactor trip is taken to shutdown the reactor in the current UFSAR Section 15.14 analyses. Following the addition of the diverse HPI and LPI actuation systems, the core cooling results would be bounded by those presented in UFSAR Section 15.14. This expectation is based upon limiting conditions being assumed in UFSAR Section 15.14 and best-estimate core conditions would be present for a D3 analysis.

RAI 2

Please provide setpoints for actuation of the LPI and HPI systems that were used in the D3 analysis

Duke Response to RAI 2

The setpoints for the diverse LPI and HPI actuation systems are 462 psig and 1550 psig respectively.

RAI 3

Please provide a summary of the D3 assessment that includes the following:

(a) Explanation that the two-minute reactor trip has always been a part of the Oconee licensing basis and is currently required with the RPS/ESPS system and will continue to be required after the new digital system is installed.

(b) Description of what diverse indications are available to the operator and describe any affect that a software common mode failure would have on operator interpretation of the event.

(c) Describe the built-in conservatism of the D3 best-estimate analysis program regarding the analyzed plant responses to Chapter 15 design-basis accidents (DBAs) with a software common cause failure (SWCCF).

Duke Response to RAI 3

D3 Submittal History

Duke submitted a defense-in-depth & diversity (D3) assessment for the RPS/ESPS digital upgrade by letter dated March 20, 2003. The initial submittal was supplemented by letters dated September 23, 2004, October 6, 2005, October 26, 2005, December 14, 2005, and April 26, 2006, in response to NRC Requests for Additional Information (RAIs).

In these RAI responses, Duke:

1) committed to install a Diverse Low Pressure Injection Actuation System (DLPIAS),
2) provided an assessment of the control rod (CR) ejection event and small break loss of coolant accident (SBLOCA) that identified alarms and indications (and their location) the operator uses to determine required manual operator actions, the manipulations required to perform these actions, and verification that the controls to perform these actions will be available and unaffected by a RPS/ESPS software common mode failure (SWCMF),
3) provided the results of simulator validation runs to provide a level of assurance that the proposed operator actions are feasible,
4) provided the results of a sensitivity study that indicated additional time is available beyond what was assumed in the D3 analysis for operator action, and
5) confirmed that simulator performance for the SBLOCA scenario accurately reflects actual plant performance.

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.

Summary of ONS D3 Assessment

The Oconee D3 assessment 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 committed to install a diverse LPI actuation system to mitigate this beyond DBE.

The D3 assessment assumed a manual reactor trip at two minutes, manual actuation of HPI and LPI at five minutes, and manual RBCS and RBS actuation at eight minutes for a SBLOCA. For the Control Rod Ejection event, the D3 assessment credited a manual HPI actuation at five minutes and manual RBCS and RBS actuation at eight minutes.

In response to questions from the NRC Staff, Duke performed a sensitivity study to demonstrate that manual HPI actuation was not required for at least eight minutes and manual RBCS and RBS actuation was not required for at least one hour. Subsequent to this study, Duke committed to install a diverse HPI actuation system.

As described in the response to RAI 1, the addition of the diverse LPI and HPI actuation systems in some cases improve the results of events assessed in the D3 assessment. In all cases, the effects of the diverse systems on events analyzed are bounded by the original D3 assessment.

The only remaining manual operator action credited in the D3 assessment that is required within 30 minutes is the manual reactor trip.

Response (a) The two-minute operator response to trip the reactor is based on a current licensing basis requirement to trip the reactor coolant pumps within two minutes of a loss of subcooled margin. The two-minute operator action time was granted to the Babcock and Wilcox (B&W) plants in the Safety Evaluation Report (SER) for Generic Letter 86-05. The current emergency procedures require that the operator verify that the reactor and turbine have been tripped prior to taking this action. If a reactor trip had not occurred at this point, the operator would manually trip the reactor before tripping the reactor coolant pumps. For the limiting small break LOCA, subcooling margin would be lost within seconds of the break initiation. The current requirement to trip the reactor coolant pumps is a NUREG-0737 requirement. The NRC provided the operator action time used by the operators of B&W plant as part of Generic letter 86-05. This requirement ensures that acceptable LOCA results are obtained using Appendix K methods. This requirement is not affected by the digital replacement of the RPS and ESPS equipment.

The requirement to manually trip the RCPs within two minutes (and manually trip the reactor prior to tripping the RCPs) of loss of subcooling margin applies now and will continue to apply to the plant after the digital RPS/ESPS is installed. The symptoms and indications that prompt the operator to take this manual action are not affected by a common cause failure (CCF) that may arise with the use of a digital RPS/ESPS. These indications are further described below.

Response (b) Oconee operators will continue to use Reactor Coolant System (RCS) pressure, pressurizer level, RCS makeup flow, and/or subcooling margin indications to determine whether a reactor trip is required. The operators will continue to use RB pressure indications to initiate Reactor Building Cooling (RBC) and Reactor Building Spray (RBS) Systems. Alarms that will actuate are not used by operators to mitigate the event or to take actions but rather to reinforce their recognition of the conditions that exist.

These indications and alarms will continue to be available and unaffected by an RPS/ESPS Software Common Mode Failure (SWCMF). They are located on the front control board in the control room. With the exception of RCS makeup flow, the indications identified above are Regulatory Guide (RG) 1.97 post accident instrumentation.

Operators are required to push one button to initiate a reactor trip. The manual reactor trip function is independent of the automatic RPS trip function and will be unaffected by the RPS/ESPS SWCMF. The manual reactor trip pushbutton is located on the main control board. This is true for the current and the proposed RPS/ESPS design.

The SBLOCA scenario would prompt entry into the abnormal procedure (AP) for excessive RCS leakage due to exceeding the Technical Specification (TS) RCS leakage limit. This would be recognized by decreasing RCS pressure, rapidly decreasing pressurizer level, increasing HPI makeup flow, and/or loss of subcooling margin. The Immediate Manual Actions (IMAs) of the AP require a reactor trip if normal RCS makeup capability is exceeded. The reactor trip prompts entry into the IMAs of the EOP and subsequent Rules. For the control rod ejection scenario, the Diverse Scram System (DSS) would automatically trip the reactor, which would prompt entry into the Emergency Operating Procedure (EOP) IMAs.

EOP Rule 2 (Loss of Subcooling Margin) requires HPI to be manually actuated (or confirm that it has been automatically actuated). Once IMAs are complete, the SRO transfers to Subsequent Actions (SAs). Once the operator recognizes the need for ESPS, the SRO will direct the performance of Enclosure 5.1. Enclosure 5.1 requires operators to verify that all required ESPS channels have actuated. If they have not, the EOP directs the operators to actuate the affected ESPS channels. Operations procedures direct the operators to actuate the channels when the actuation setpoints have been exceeded. HPI would be manually actuated when RCS pressure is $\leq$ 1600 psig (ESPS actuation setpoint). RBCS and RBS would be manually actuated when RB pressure $\geq$ 3 psig and 10 psig respectively (ESPS actuation setpoints).

Response (c) See response to RAI 4 below

RAI 4
Please provide a qualitative discussion of the expected outcome of events where fuel damage occurs.

Duke Response to RAI 4

The methods applied to evaluate the D3 transients are generally the same methods used to perform the Chapter 15 analyses. These methods have been extended to consider the common mode failure of the RPS and ESPS actuations and model the actions of the active plant control systems.

The D3 LOCA and non-LOCA analyses use initial conditions selected based on the same conservative considerations as the UFSAR Chapter 15 analyses. The boundary conditions are a combination of those used in the existing UFSAR Chapter 15 analyses, and new boundary conditions involving control systems not credited in the UFSAR Chapter 15 analyses. An attempt is made to obtain best-estimate results through the usage of boundary conditions that do not reflect single failures and through modification in the acceptance criteria.

During a May 20, 2008 meeting where Duke described the D3 analysis to NRC staff, Duke indicated that the methodology used produced conservative results. This statement was made based on the fact that standard core departure from nucleate boiling (DNB) methods had been used for the D3 analysis. The standard method uses the statistical DNBR limit as the DNB limit, and increases that limit by some amount of conservatism to arrive at the design DNBR limit. The design DNBR limit used is higher than realistic DNB values, increasing the number of rods predicted to undergo DNB (if any). Any rod predicted to experience DNB was considered to be failed. In addition, the initial core power used for the simulations was 102% of the current rated thermal power. This power level was selected to cover a potential measurement uncertainty recovery power uprate.

The D3 evaluation uses a core-cooling criterion for LOCA related events. The methods used are not capable of simulating the transient response to this criterion, and therefore use criteria that are within the individual methodology's capability. For example, the Appendix K methods employed for the small break LOCA analysis are qualified up to a clad temperature slightly above 2200°F, but the mass and energy release methods are limited to lower cladding temperatures by the available material properties. The methods used for the LOCA related D3 analyses are exercised within their respective range of applicability. This ensures that conservative results are obtained, as the transient results obtained do not approach the core-cooling criterion.

During the May 20, 2008 meeting, when discussing the conservatism in the containment response, the containment pressure response curve presented was for a double-ended cold leg break with minimum safeguards type assumptions without actuation of the containment spray or cooling units. The NRC asked what the expected containment pressure response would be with maximum safeguards. In response to this question Duke offers the following explanation.

When the additional ECCS flow resulting from maximum safeguards conditions is considered, the containment pressure response is not expected to be significantly different. This is due to the steaming rate to containment not being dependent on the ECCS flow. The ECCS to the core is limited to the boil-off rate for a cold leg break. The injected ECCS above this rate spills from the broken cold leg. In the Oconee containment response methodology, injecting low pressure injection below the cold leg nozzle in the reactor vessel downcomer minimizes the condensation of steam on injected ECCS. This limits the steam condensation to the interface of the liquid and steam in the downcomer and the cold legs. The change in condensation due to the increase in ECCS flow is not expected to be significant. Since the containment pressure response is tightly coupled to the steaming rate, the containment pressure would not be expected to be significantly different from that already published.

RAIs associated with Communications

RAI 5
Please provide data verifying the one-way communication link of the Port Tap with the external plant data systems.

Duke Response to RAI 5:

The vendor (Net Optics) has formally confirmed that the physical disconnection of the RX pins on the printed circuit board for the communication port of the Port Aggregator Tap only allows one-way communication. Duke also requested Net Optics to provide a copy of a schematic that demonstrates the one-way communication capabilities of the Port Aggregator Tap. Net Optics has agreed to make a schematic of the device available for review by Duke and/or the NRC at the Net Optics offices in Santa Clara, California. Duke is currently working on a proprietary agreement with Net Optics to enable Duke to submit the schematic to the NRC.

RAI 6
Please provide documentation to demonstrate that the isolation communication processor is on the SVE2 board.

Duke Response to RAI 6:

The TELEPERM XS (TXS) design uses separate communication and safety-processors. The devices operate asynchronously through Dual Port Random Access Memory (DPRAM). The safety-processors operate autonomously, so that the safety-related function processing is not compromised by communication activities. The isolation communication processor is located on the SL21 communication module. The communication processor is indicated by the V25 block on Figure 6-1. The interface to the SVE2 safety processor module is through the Interface X6 connection.

Data is exchanged between the SVE2 and SL21 over MicroNET and MicroNET-L2. MicroNET-L2 forms the link between MicroNET and the firmware on the SL21. The principle of data transfer between MicroNET-L2 and the firmware of the SL21 is described below.

The SL21 module (including the firmware) is designed and qualified using the configuration management process for safety-related components described in the TELEPERM XS topical report. Changes to the SL 21 module since the TELEPERM XS Topical Report was issued are described in the response to RAI 52.

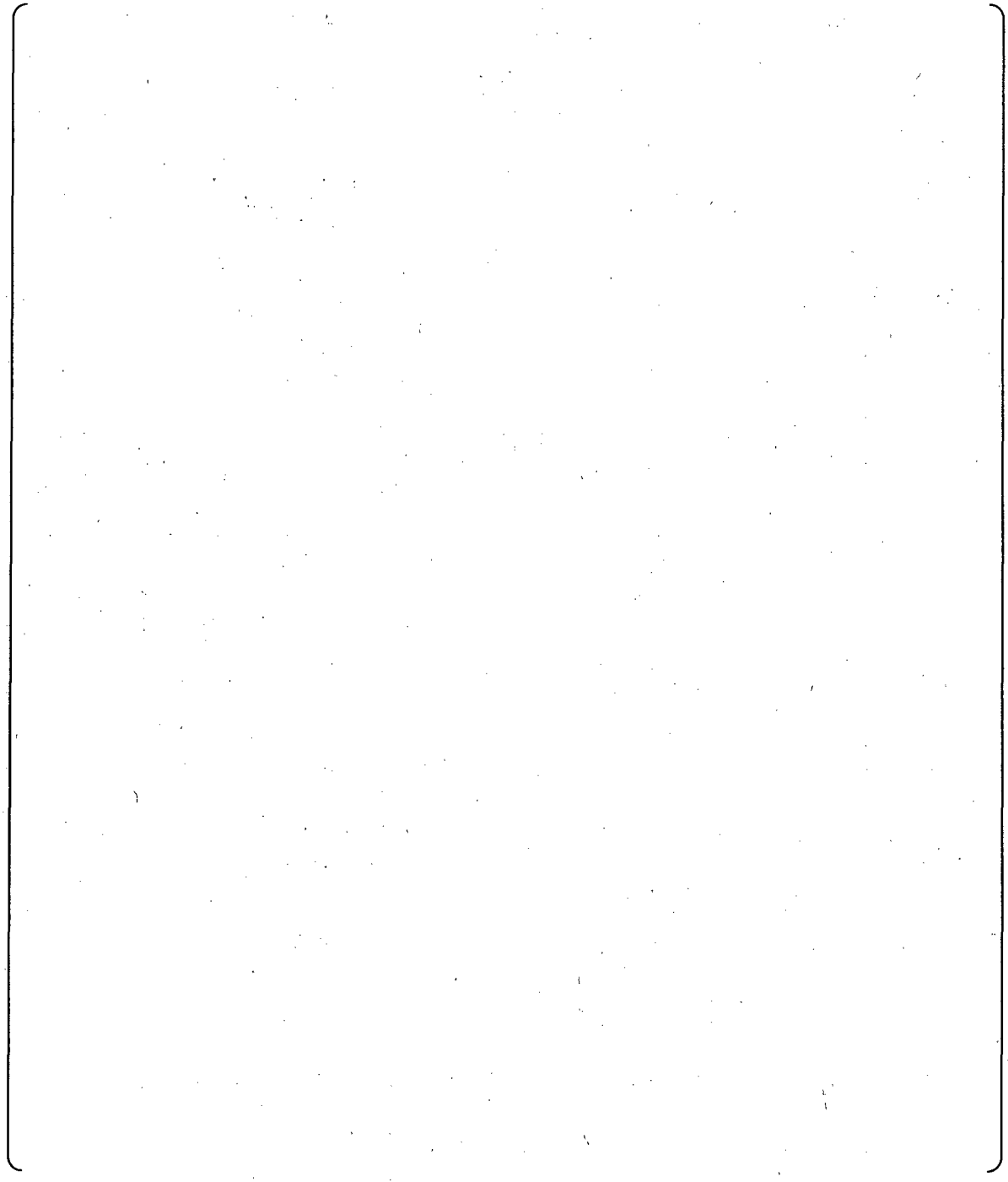


Figure 6-1, Block Diagram of the SL21 Communication Module

Figure 6-2: Basic Structure of the PROFIBUS Interface

RAIs associated with December 13, 2006, AREVA Slides

The NRC was provided a copy of the December 13, 2006 (ML070080325), briefing slides on the digital replacement project that, that in part, addressed safety-related (SR) inter-channel and SR channel to non-SR systems data communications. Please provide an explanation for the following questions to facilitate the staff's understanding of the Oconee Teleperm XS (TXS) platform design features.

RAI 7

Slide 5 - The 3rd bullet says that "only static memory allocation is used." Please explain when this allocation is done, and how it is controlled. Is either static or dynamic memory re-allocation performed at any time after the original compiling from the "C" code?

Duke Response to RAI 7

The physical memory allocation to data and programs is static. That means that data and programs that are required to implement I&C functions are permanently assigned to defined memory areas in advance. The allocation of memory occurs during the code generation and compiling. The allocation of the communication dual port random access memory (DPRAM) is done during system start-up and not changed afterwards.

Data exchange with the communication processor passes through the DPRAMs. Input data for a function processor are directly written from the communication processor into the DPRAM of the receiving function processor. In the opposite direction, results from the

function processor are written into the DPRAM of the interface module concerned (part of the communication means) via the backplane bus. Physically different areas of the DPRAM are dedicated to receiving and sending.

RAI 8

Slide 23 - This slide shows the communications method used to demonstrate independence. The slide shows the safety function processors, DPRAM, SL21 boards, and the SLLM. The SL21 is labeled as the buffer circuit. Is there an interposing communications processor, and if so, where is it located? Please provide a circuit diagram or schematic showing the interposing communications processor, and its connections to other circuits.

Duke Response to RAI 8

See response to RAI 6.

RAI 9

Slide 24 - This slide shows a figure from Annex G of Institute of Electrical and Electronic Engineers (IEEE) Std 7-4.3.2. This annex was not endorsed by the staff, because use of a buffer circuit without an interposing communications processor was considered insufficient isolation. Is this method of isolation the one used for the Oconee digital safety system?

Duke Response to RAI 9

The method of isolation used for safety to safety communication isolation for the Oconee digital RPS/ESPS is based on Figure E2 of IEEE Std 7-4.3.2-2003 (same as figure G2 of IEEE Std 7-4.3.2-1993). The communication isolation scheme is supplemented with the use of separate input and output message buffers on the safety function processors (SVE2), separate communication modules (SL21) using dual port random access memory (DPRAM), and physically different areas of the DPRAM dedicated to receiving and sending, as shown in Figure 9-1.

Also see responses to RAIs 6 and 7.

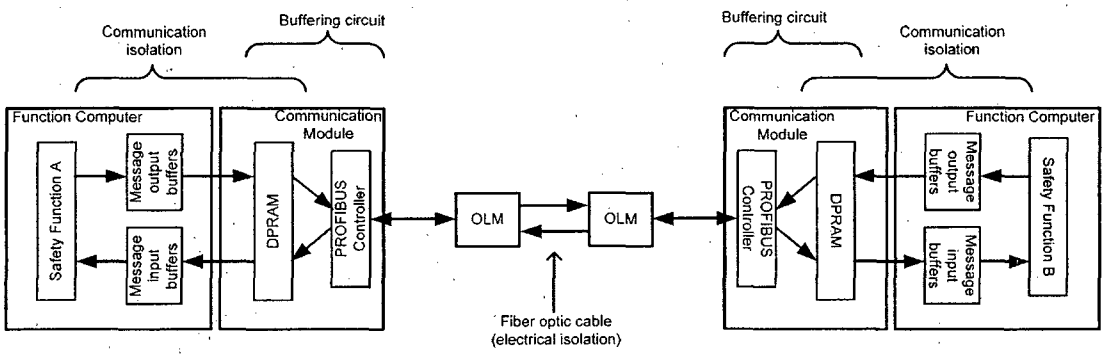


Figure 9-1: Oconee RPS/ESPS Communication between Safety Channels (Two-way Communication)

RAI 10

Slide 27 - The 3rd bullet says the cyclic data transfer has a predefined package size, constant bus load and age monitoring.

(a) Please define the package size and show the bit allocation for the message. Is this a standard bus protocol, and if so, which is it?

(b) Please define the bus load, show what it is, and how often a message is sent. Define what units are on the bus, and under what conditions each is the bus master.

(c) How is the checksum generated, and how is the message age monitoring accomplished?

(d) How does usage of a bus meet the Interim Staff Guideline (ISG) 4 requirement that all communications be point-to-point?

Duke Response to RAI 10

Response (a): The analog and binary application data (Function Diagram data) to be transferred are prepared in an individual, static Function Diagram Group (FDG) message buffer during the current cycle of processing the application functions (i.e., the function diagram module FDG_n). This message, called FDG message, is supplemented with a short FDG-specific message header (H_{FDG}).

The TELEPERM XS (TXS) system uses a proprietary message frame for communication. The proprietary TXS messages are comprised of a standard message header used for all messages and a fixed data section that is specified for each type of message. All messages are constructed to these specifications every time messages are assembled.

Response (b): Bus load refers to the amount of data that is available on a network connection (bandwidth) and actual amount of data being transferred on the network connection at any given time.

Bus load = data transferred/bandwidth

The Oconee RPS/ESPS application uses only point-to-point communications (i.e., two stations using token ring-like technology). Separate communication links are used for each communication channel.

TXS PROFIBUS uses the PROFIBUS FDL protocol, which is a layer 2 master-master protocol. As such, there is no specific master on the bus; instead, all stations handle the protocol in the same way.

[

]

Response (d): The Oconee RPS/ESPS application uses only point-to-point communications (i.e., two stations using token ring-like technology). Separate communication links are used for each communication channel.

Separate SL21 communication channels and ports are assigned to each communication link. The SL21 communication module works independently of the SVE2 safety processor.

[

]

RAI 11
Slide 27 - The 4th bullet says there is no dynamic allocation of resources. Is there static allocations of resources?

Duke Response to RAI 11

The physical memory allocation to data and programs is static. That means that data and programs that are required to implement I&C functions are permanently assigned to defined memory areas in advance. The allocation of memory occurs during the code generation and compiling. The allocation of the communication Dual Port Random Access Memory (DPRAM) is done during system start-up and not changed afterwards.

RAI 12
Slide 27 - The 7th bullet mentions a simple type of multi-tasking. Please define the multi-tasking, and show how it is done without using interrupts. The bullet also mentions the service commands. What commands are considered service commands, how are they sent to the safety processor, and under what conditions.

Duke Response to RAI 12

[

]

RAI 13

Slide 28 - The 7th step of the cyclic operations is shown as "write output data." Is this considered inter-channel or safety to non-safety communications. Please show all output data possible, and where it is written to. If this data can go to more than one place, show how the routing is accomplished.

Duke Response to RAI 13

[ ]

RAI 14

Slide 29 - This slide shows the cyclic signal processing. Please provide a detailed description of each of the elements, including bit size and allocation, time for each portion of the processing, and a description of how each portion is generated and used.

Duke Response to RAI 14

This slide does not show cyclic signal processing in the sense of bits and bytes. It is showing the different processing task steps and their sequences. The overall time shown on the slide is 25 milliseconds (Oconee safety processor cycle time) and the time needed for each step depends on the processors and functions run on that processor.

The various sequential tasks shown on the referenced slide are correlated to the various TELEPERM XS (TXS) Runtime Environment (RTE) communication and processing cycle tasks. Three color coordinated figures are included in this response to help integrate the information.

The task identified as 'IN' in Figure 14-1 corresponds to the RTE and MicroNET tasks performed during Phases 1 and 2 of the processing cycle, as shown in Figure 14-2. The central control unit of the RTE triggers MicroNET to transfer the messages from the receiving dual-port random access memory (DPRAM) locations of all linked SL21 modules into the corresponding message input buffers in Phase 1. The RTE then checks the integrity of the message transfer from the sending SVE2 processor to the receiving SVE2 processor. The data messages are checked for correct message header and age. In addition, cyclic redundancy checksum and not-a-number (i.e., invalid floating point data) checks are performed.

The task identified as 'RCV' in Figure 14-1 corresponds to the Application Software tasks performed during Phase 3 of the processing cycle, as shown in Figure 14-2. The Function Diagram Group Input Function starts the processing on the application software level. The individual signals inside the message are identified and allocated to the signal memories.

The task identified as 'COMPUTE' in Figure 14-1 corresponds to the Application Software tasks performed during Phase 4 of the processing cycle, as shown in Figure 14-2. The function diagram modules belonging to the individual functions are processed during Phase 4.

The task identified as 'OUT' in Figure 14-1 corresponds to the Application Software tasks performed during Phase 5 of the processing cycle, as shown in Figure 14-2. As last step of application software processing, The Function Diagram Group Output Function is triggered by the central control unit to collect the results of the processing and assemble new data messages to the standard data structure.

The task identified as 'SND' in Figure 14-1 corresponds to the RTE and MicroNET tasks performed during Phases 6 and 7 of the processing cycle, as shown in Figure 14-2. The RTE then adds the message header to the message data (including cyclic redundancy checksum and the cycle counter information) and stores the messages in the message output buffers in Phase 6. The RTE the triggers MicroNET to transfer the output messages from the output buffers to the sending DPRAMs of the respective SL21 module in Phase 7.

The task identified as 'TEST' in Figure 14-1 corresponds to the remaining cycle time used to process the self-monitoring tasks and any service requests performed during Phase 8, as shown in Figure 14-2. The RTE service task acts as a background activity during phase 8 of the RTE cycle (i.e., occupying the remaining processing time at the end of the RTE cycle). The service task is handled sequentially, after the completion of the seven-step process used to execute the function diagrams. The TXS design does not use a multi-tasking scheme controlled by process interrupts. The execution priority of the service task is lower than the priority of the RTE cycle task (e.g., implementing cycle phases 1-7). The execution of a request may therefore last several cycles. Execution of service requests by the RTE is shown in Figure 14-3.

The self-monitoring task is controlled by the self monitoring software, which continuously performs tests of all relevant hardware components of the processing module (e.g., RAM-test,

ROM-checksums, and watchdog-test).

Service requests are sent by the TXS Service Unit in service messages and are addressed to a particular safety function processor. When a service message is received, it is checked by the RTE and only valid requests are accepted. At the end of the request execution, the response data structure is put into the data section of the next signaling message and is sent by the RTE cycle activities

The responses to RAIs 13, 15, 16, and 17 provide more details on the tasks performed in Phases 1, 2, 6, and 7.

The responses to RAIs 12 and 35 provide more details on the tasks performed in Phase 8.

Figure 14-1: TXS Cyclic Signal Processing

Figure 14-2: Organization of the RTE Communication and Processing Cycle

Figure 14-3: Execution of Service Requests by the RTE

RAI 15

Slide 30:

(a) *The 1st bullet says that a fiber optic medium is used. Is this two fibers, each with one-way transmission, or a single fiber with two-way transmission?*

(b) *The 3rd bullet speaks of avoidance and independent control. How is this done? If channel A and channel B are communicating, where is the data stored? Is the communications processor synchronized with the safety processor, and if so, how?*

(c) *The 5th bullet mentions "not-a-number checking." What is this, and how is this done?*

(d) *The 6th bullet states that on-line validation limits the propagation of faulty data. How does this on-line validation differentiate between faulty data and data rapidly changing from a rapidly changing plant condition?*

Duke Response to RAI 15

Response (a): Two fibers are used for each communication pair. One fiber connection is used for each direction of data transmission.

Response (b): Communication between different safety function processors (SVE2) is done by messages. These messages can contain the following information:

- Signals from TELEPERM (TXS) Application Software (i.e., data messages from Function Diagram Group (FDG) modules)
- Service requests from the TXS Service Unit (service messages), or
- System error messages, trace data, or request responses to the TXS Service Unit (signaling messages)

[redacted]

See response to RAI 81 for additional information on loss of a token.

RAI 16

Slide 32:

(a) The 1st bullet states there is a "separate logical MicroNET communications channel for each message." Is the separate channel a physical point-to-point transfer, or is this a logical point-to-point transfer?

(b) The 1st bullet also mentions a "unique MicroNET communications interface." Please define this interface in detail.

(c) The 3rd bullet mentions the standard header. Please provide the size, bit definition and coding for each of these portions of the header. Where and how is each of these generated?

(d) The 4th bullet states that the "message size determined individually for each message. Please list the different types of messages, what the message size is, how this message size was determined, and what the content of each message is, by bit definition.

Duke Response to RAI 16

[ ]

The Oconee RPS/ESPS application uses only point-to-point communications (i.e., two stations using token ring-like technology). Separate communication links are used for each communication channel. Separate SL21 communication channels and ports are assigned to each communication link.

[ ]

See responses to RAIs 6, 13, 15, 16, and 31 for detailed information on MicroNET.

Response (c): See response to RAI question 10 (a)

Response (d): Message communication between TXS computers (in general and also via the MSI computer with gateways) and the TXS Service Unit takes place for two different and strictly separate purposes:

RAI 17

Slide 37 - This slide discusses the received message checking.

(a) Is this checking done by the interposing communications processor or by the safety processor?

(b) The 3rd check shown is for sequence number. What occurs if a sequence number is skipped?

(c) How many numbers must be skipped to trigger a communications fault?

(d) Is there a memory of missed messages, that is, what would happen if every other message was missed?

Duke Response to RAI 17

Response (a): The integrity of all messages received from other safety function processor is checked in phase 2 of the RTE cycle by the receiving safety function processor.

⌈ ⌉

Response (c): See response to RAI 17 (b).

⌈ ⌉

[ ]

RAI 18
Slide 38 - This slide discusses message age monitoring. When ONE_MISS status is present, how long will the previous message be used? This seems to indicate only one cycle, but the staff had previously been told the previous message could be used for 200 ms.

Duke Response to RAI 18

See response to RAI 17 (b).

RAI 19
Slide 39 - This slide on message age monitoring says an error situation will exist if a data message is not received by the RTE for two or more cycles.

(a) Is this two or more cycles of the interposing communications processor or of the safety processor?

(b) How are the two processors synchronized?

Duke Response to RAI 19

Response (a): The slide statement refers to two or more cycles of the receiving TXS safety function processor.

Response (b): The TXS safety function processors are not synchronized.

RAI 20
Slide 42 - This slide has a green box which says "Use of inter-channel communications does not create new interfaces, it simply changes the location of the interconnections."

(a) Does this mean that the inter-channel communications and safety to non-safety communications use the same buffers, fiber optic lines, etc.? If this is true, would this also mean that there is one bus or LAN for both types of communications, and therefore there are non-safety devices on the bus or LAN used for inter-channel communications?

(b) Please justify this, and show how point-to-point communications is used.

Duke Response to RAI 20

The statement in the green box was meant to address IEEE Std 603-1991, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, compliance and separation of channels. The Oconee RPS/ESPS application uses only point-to-point

PROFIBUS L2 communications (i.e., two stations using token ring-like technology). Separate communication links are used for each communication channel. This communication type is used for all communications between safety channels and between the safety channels and the Monitoring and Service Interface (MSI).

The communication between the MSI and the TELEPERM XS (TXS) Service Unit and the TXS Gateway are via SINEC H1 communication links. These three stations are on the same network connection as shown on slide 9.

At no time are non-safety and safety related communications on the same link.

RAI 21
Slide 44 - The 3rd bullet of this slide states that an alarm indication is initiated by the on-line signal validation.

(a) Will this alarm trigger a limited condition of operation (LCO)? If not, why?

(b) What will be done by the operators or technicians in response to this alarm?

Duke Response to RAI 21

Response 21 (a)

An alarm does not trigger immediate entry into a Technical Specification (TS) Condition. (Note: A "limiting" condition for operation (LCO) specifies the minimum equipment required to be operable. Failure to meet the LCO would result in entry into a TS Condition.)

The online monitoring capabilities of the TELEPERM XS are designed to provide early indication of discrepancies between redundant input signals or failures within the system. The alarm indication is the equivalent of the channel check surveillance that is performed on the currently installed analog RPS/ESPS. The receipt of the online signal validation alarm indication can represent several potential problems. The potential problems can include an input instrument has deviated from the other redundant sensors, an input instrument has failed, the online signal validation function has failed or a channel communication link has failed. Of the potential problems listed above, only the failed input instrument will impact the operability of a RPS or ESPS channel. The deviation of an input sensor from the redundant sensors does not impact the operability of the channel since the alarm indication is provided for early detection of potential drift problems. The statalarm would require an evaluation to determine the cause of the alarm and potential operability concerns. The signal validation function failure or channel communication failure will not impact the operability of an RPS/ESPS channel since the TXS is designed to operate in the silo mode with no communications or signal validation.

TS 3.3.1 LCO requires three RPS channels to be operable. During normal plant operations four RPS channels are operable. Therefore, entry into a TS Condition is not required when one channel of RPS is out of service. However, if the plant is operating with only three RPS channels operable as allowed by the TS 3.3.1 LCO, the inoperability of another RPS channel requires entry into TS 3.3.1 Condition A for one required RPS channel inoperable.

TS 3.3.5 LCO requires three channels of one ESPS set to be operable. During normal plant operations, with all three channels of both ESPS sets operable, entry into an ESPS TS Condition will not be required when one channel of one set of ESPS is out of service since a complete set of ESPS is available with three channels operable. However, the failure of an input sensor to the ESPS system will impact a channel on both ESPS sets. Thus, entry into TS 3.3.5 Condition A for one ESPS channel inoperable will be required.

If the functionality of the signal validation is lost, entry into a TS Condition is not required. However, the channel check surveillance requirement will need to be performed manually by Operations personnel for the inputs that have lost the online signal validation function.

Response 21 (b)

As part of the RPS/ESPS project, Alarm Response Guides (ARGs) are being developed for statalarms and computer alarms. These ARGs will provide the direction for Operation personnel to respond correctly to the system alarms. The RPS/ESPS project schedule has the ARGs being developed approximately three months prior to implementation. It is expected that the content of the ARG for the online signal validation alarm will direct Operations personnel to review redundant indicators, if available, to determine if the alarm is due to a failed instrument which can impact channel operability. If channel operability is impacted, a Technical Specification Action Item Log (TSAIL) entry will be made to track the channel status. For situations where fewer channels than required by TS LCO are operable, entry into the appropriate TS Condition will be made by Operations personnel. Following the determination of the impact on the RPS and/or ESPS operability, Operations personnel will contact Maintenance and/or Engineering to troubleshoot the problem.

RAI 22

Slide 45 - This slide shows error information from the TXS being transferred to the service unit and alarms. Please describe in detail how this is done, and what equipment is involved.

Duke Response to RAI 22

The Oconee RPS/ESPS application software is design to generate alarms when failures are detected either by system software (e.g., physical input channel failure) or engineered functions (e.g., channel check deviation alarms). Application level alarms are alarmed to the operator by two methods: alarms sent to the TELEPERM XS (TXS) Gateway as computer points (i.e., data messages from the safety function processor to the TXS Gateway via the

Monitoring and Service Interface (MSI)) and alarms sent to the plant annunciator system as physical outputs from the safety channel.

Additionally, Runtime Environment (RTE) error messages are generated to indicate failures detected at the system level. The types of errors included in RTE message are communication faults, input/output driver detected errors, and processor errors. System level messages are sent to the TXS Service Unit by the RTE. These messages are sent via the signaling message from the safety function processor via the MSI to the TXS Service Unit.

RAI 23
Slide 46 - This slide shows a wide black line extending horizontally from each SAA1. What is it?

Duke Response to RAI 23

This line indicates the boundary between field and TXS equipment. It was not meant to convey any other special meaning.

RAI 24
Slide 48 - The 2nd bullet of this slides states that the 2nd min/ 2nd max logic will prevent an "overly conservative spurious trip."

(a) Can this feature mask a sensor failure?

(b) Will a sensor failure still result in an LCO for the respective channel?

Duke Response to RAI 24

Response 24(a)

A sensor failure will not be masked by the 2nd min/2nd max logic. The online monitoring capabilities of the TXS are designed to provide an alarm when a sensor input fails. The 2nd min/2nd max logic feature of the RPS/ESPS is designed to actuate a channel when the 2nd signal exceeds the actuation setpoint, therefore, a sensor failure would not result in the actuation of a channel.

Detailed information pertaining to the error flagging of the signals is outlined in the response to NRC RAI 15.

Response to 24(b)

The failure of an input sensor for a respective ESPS input channel will result in entry into a TS 3.3.5 Condition A for ESPS and may result in entry into TS 3.3.1 Condition A for RPS as explained in the following paragraph. (Note: A "limiting" condition for operation (LCO) specifies the minimum equipment required to be operable. Failure to meet the LCO would result in entry into a TS Condition.)

TS 3.3.1 LCO requires three RPS channels to be operable. During normal plant operations four RPS channels are operable. Therefore, entry into a TS Condition is not required when one input sensor for one channel of RPS is inoperable. However, if the plant is operating with only three RPS channels operable, as allowed by the TS 3.3.1 LCO, the inoperability of another RPS channel requires entry into TS 3.3.1 Condition A for one required RPS channel inoperable.

TS 3.3.5 LCO requires three input channels of one ESPS set to be operable. During normal plant operations, with all three input channels of both ESPS sets operable, entry into an ESPS TS Condition will not be required when one input channel of one set of ESPS is out of service since a complete set of ESPS is available with three channels operable. However, the failure of an input sensor to the ESPS system will impact an input channel on both ESPS sets. Thus, entry into TS 3.3.5 Condition A for one ESPS input channel inoperable will be required.

RAI 25
Slide 51 - This slide discusses the automated channel check logic.

(a) Please list all equipment and logic checked during the current (analog system) channel checks, and compare this to the equipment and logic which would be checked by an automated channel check.

(b) Does the current channel check test the sensor wires to the trip system, and will this still be checked by the automated channel check?

Duke Response to RAI 25

Response 25(a)

As defined in the current ONS Technical Specifications, a Channel Check shall be the qualitative assessment, by observation, of channel behavior during operation. This determination shall include, where possible, comparison of the channel indication and status to other indications or status derived from independent instrument channels measuring the same parameter.

In order to satisfy the Channel Check surveillance requirement of a qualitative assessment using observation of the existing RPS and ESPS, Operations personnel perform specific steps

in the Periodic Instrument Surveillance procedure every 12 hours. During the performance of this procedure, the RPS/ESPS instruments outlined in the following table are assessed by the observation methods listed in the required conditions column in the table. The table is for operation in Modes 1 and 2.

	Component	Required Conditions
SR 3.3.1.1 12 Hours	RPS Instrumentation NI Power Range NI-5, 6, 7, 8, 9	Verify computer readouts agree within 2%. (If OAC unavailable, 4% in RPS Cab) **NOTE: IF** the channels are off scale, the channel check will only verify that they are off scale in the same direction. (TS Bases SR 3.3.1.1)
SR 3.3.5.1 12 Hours	ESPS Analog Instrumentation RB Pressure Narrow Range	Verify computer readouts agree within 0.6 psi (2 psi in ES Cab). **IF** readouts differ by > 0.4 psi, issue a Priority "E" Work Request.
SR 3.3.1.1 12 Hours	RPS Instrumentation RC Pressure Narrow Range	Verify computer readouts agree within 26 psi (If OAC unavailable, 48 psi in RPS Cab).
SR 3.3.1.1 12 Hours	RPS Instrumentation RC Temperature TH (A Loop)	Verify computer readouts agree within 3□F (If OAC unavailable, 5□F in RPS Cab).
SR 3.3.1.1 12 Hours	RPS Instrumentation RC Temperature TH (B Loop)	Verify computer readouts agree within 3□F (If OAC unavailable, 5□F in RPS Cab).
SR 3.3.1.1 12 Hours	RPS Instrumentation RC Flow	Verify total flow agrees within 4800 klbm/hr **AND** no computer alarms for high flow present.
SR 3.3.5.1 12 Hours	ESPS Analog Instrumentation RC Pressure Wide Range	Verify computer readouts agree within 75 psi (100 psi in ES Cab).
SR 3.3.5.1 12 Hours	ESPS Analog Instrumentation ES Channels 7 & 8 RB 10 psig	Verify no trips present. Verify status annunciators operable (lamp test).
SR 3.3.1.1 12 Hours	RPS Instrumentation RP RCP/Flux Trip	Verify no Dummy Bistable installed. Verify no trips present. Verify status annunciators operable (lamp test).
SR 3.3.1.1 12 Hours	RPS Instrumentation RB High Press Trip	Verify no Dummy Bistable installed. Verify no trips present. Verify status annunciators operable (lamp test).

Since the Channel Check is an observation of the instrumentation to perform a qualitative assessment, no logic or functional checks are performed for the existing RPS and ESPS as part of the Channel Checks.

Following the installation of the digital RPS and ESPS, the definition of a Channel Check remains the same in the Oconee Technical Specifications. In order to satisfy the Channel Check requirement, the same RPS and ESPS instrumentation will be qualitatively assessed by observation utilizing online signal monitoring. The online signal monitoring is performed multiple times per second instead of once per 12 hours. If the online signal monitoring is out of service, then manual observation will be performed to satisfy the Channel Check surveillance requirements. As is the case with the analog RPS and ESPS, logic or functional testing of the digital RPS and ESPS will not be performed to address the Channel Check surveillance requirements in the Technical Specifications.

In summary, there is no difference between the instrumentation that is qualitatively assessed as part of the Channel Check surveillance for the analog or digital RPS and ESPS.

Response 25(b)

As noted in the response to Part (a) of this RAI, the Channel Check as defined in the Oconee Technical Specifications is a qualitative assessment by observation of the channel behavior. If there is a problem with the sensor wires that results in the deviation of signal indication in the analog RPS and ESPS, the problem will be identified as part of the instrument indication comparisons by Operations.

The Oconee Technical Specification, following the installation of the digital RPS and ESPS, will contain the same Channel Check definition. If there is a problem with the sensor wires that results in the deviation of signal indication to the digital RPS and ESPS, the problem will be identified as part of the digital system online monitoring.

Additional information related to the performance of the Channel Checks using the online signal monitoring is available in Section 3.3.7.2, 3.3.16.5.1 and 3.4.5.3 of Enclosure 1 of the Oconee RPS/ESPS LAR submittal. In addition, Section 8 of Enclosure 2 of the Oconee RPS/ESPS LAR submittal and the proposed Technical Specification Bases for the associated surveillance requirements in the Oconee RPS/ESPS LAR submittal provide justification for online monitoring to satisfy the Channel Check surveillance requirements.

RAI 26
Slide 54:

(a) The drawing seems to indicate that communications between the various TXS RPS/ESF channels and the voters is via the MSI. Is this correct?

(b) The drawing shows an ethernet switch between the Netoptics unit and the service unit. What is the function of this switch? What other devices are attached to this switch?

(c) Please define the boundary of the safety to non-safety border.

Duke Response to RAI 26

Response (a): No. Slide 54 shows the connections between the safety function processors and the Monitoring and Service (MSI) for purposes of transferring service and signaling messages. Slides 10 and 42 show the connections between safety function processors that transfer interchannel data messages.

Response (b): The Ethernet Switch is used to keep the NetOptics communications active if the Service Unit is offline or disconnected. If this switch is not present, then data messages will not continue to be sent to the TXS Gateway. The NetOptics device will detect a dead link on Port B and will stop transferring data to Port C (to the TXS Gateway). No other devices are attached to the Ethernet Switch.

Response (c): MSI is the safety to non-safety isolation point, as shown in Figure 26-1.

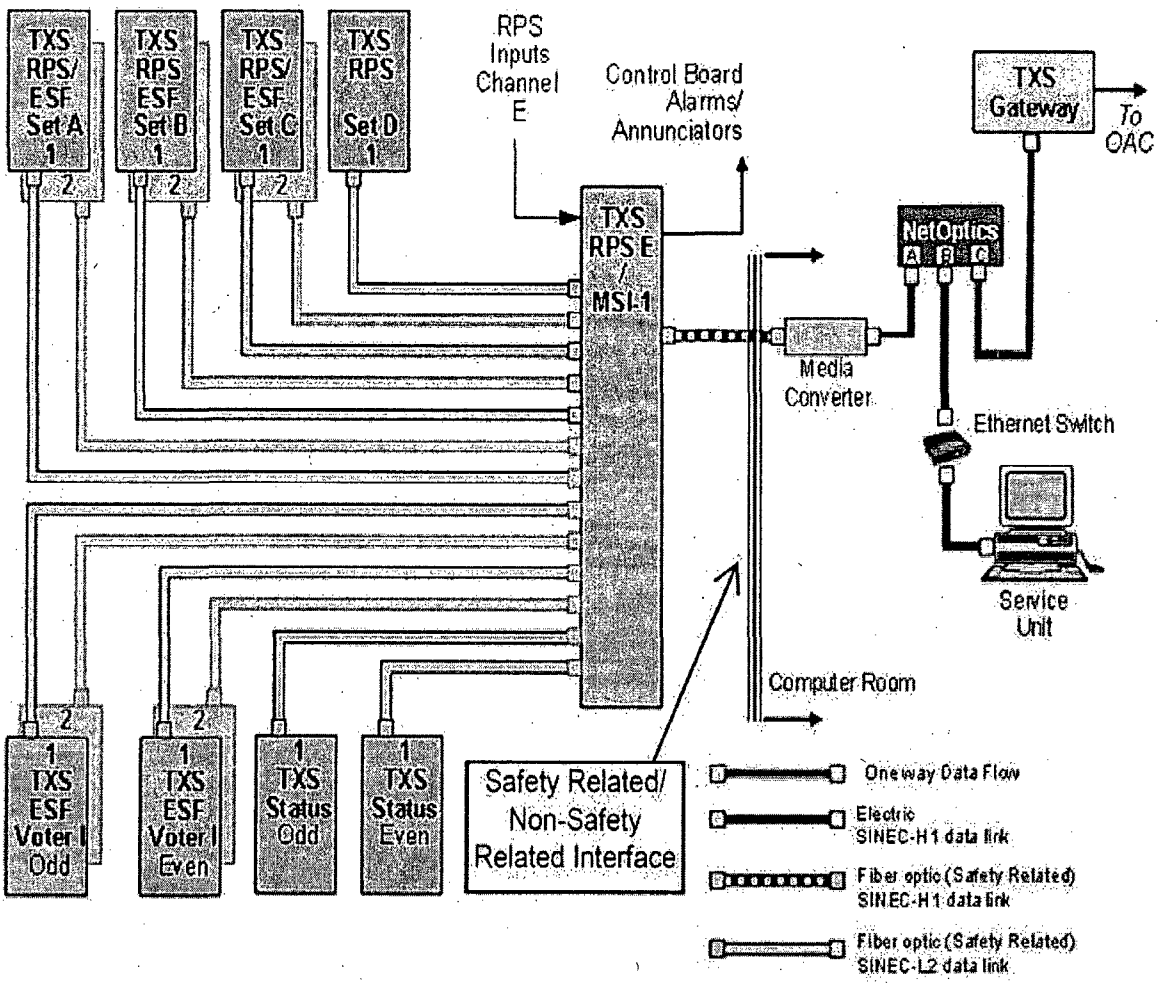


Figure 26-1: Oconee RPS/ESPS Safety-Related/Non-Safety Related Interface

Electrical isolation between the safety-related/non-safety related interface is provided by the use of fiber optics. The MSI is powered from a non-1E poser source; however, the loss of powered has no adverse impact on the safety functions processors performing the RPS and ESPS functions.

The method of isolation used for safety to non-safety communication isolation for the Oconee digital is based on Figure E4 of IEEE Std 7-4.3.2-2003 (same as figure G4 of IEEE Std 7-4.3.2-1993). The communication isolation scheme is supplemented with the use of separate input and output message buffers on the safety function processors (SVE2), separate communication modules (SL21 for L2 and SCP2 for H1) using dual port random access memory (DPRAM), physically different areas of the DPRAM dedicated to receiving and sending, and an additional MSI communication barrier, as shown in Figure 26-2.

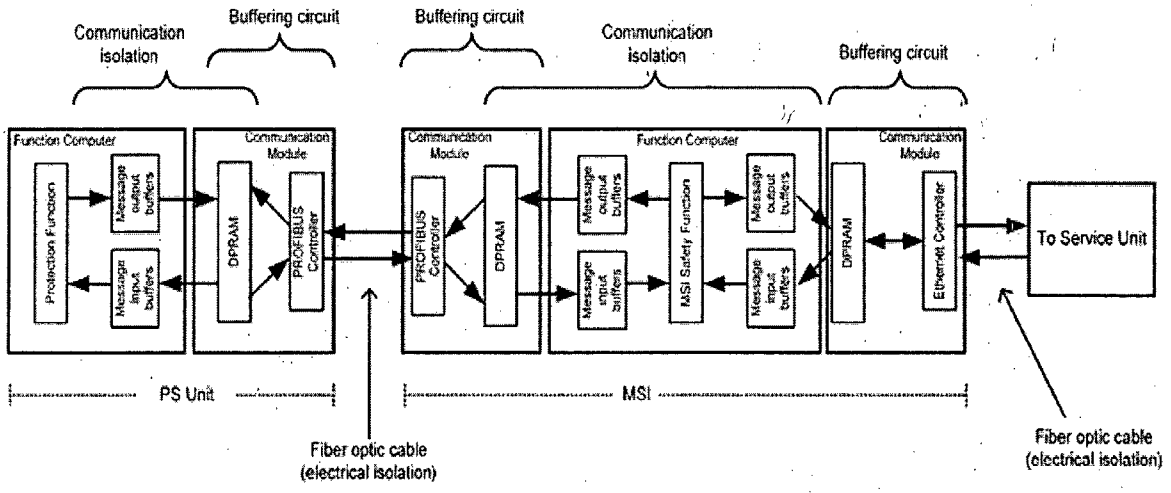


Figure 26-2: Oconee RPS/ESPS Communication between Safety and Non-Safety Systems (Two-way Communication)

RAI 27
Slide 58:

(a) The staff believes this is a logic view, and not a physical representation of the logic. Please confirm this understanding.

(b) If this is correct, the failure of an input line would also be a failure of that line wherever it is physically used. What are the other uses of this line, and how are the additional subsequent failures taken into account?

Duke Response to RAI 27

Response (a): This slide is a standard training slide and does not show actual Oconee screens or logic. It give a representation on how the application software would be displayed using the Dynamic Function Diagram Editor. The software is "programmed" and displayed by the Function Diagram Editor in a logical view. All software on a Function Diagram physically runs on a single defined safety function processor (i.e., logic on a Function Diagram is not split between safety function processors). Multiple Function diagrams are run on each safety function processors.

Response (b): The failure of an input line is recognized as a failure of that line wherever it is physically used. For inputs signals with detected failures, the faults status is set for the signal. The Oconee RPS/ESPS application software contains logic to take action to alarm, and handle these input failures. The fault status is applied to the signal throughout the software until it is handled via one of the function block with active fault status functionality.

RAI 28

Slide 60 - This slide shows that the parameter change enable key switch does not, as required by ISG #4, create a "physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic", but rather sets a bit in a register. Why is this permissible, and why is this type of logic used in a safety-related system.

Duke Response to RAI 28

The design and use of the Service Unit was extensively described in the TXS Topical Report. The following sections from the report describe relevant aspects of the Service Unit, its use, and its isolation from the safety-related portions of the system:

2.4.3.4.1	Operating System
2.4.3.4.4	Function Block Modules
2.5.1	Introduction (to Testability)
2.5.2	Tasks of the Service Unit
2.5.3.4	Online Display of Hardware Structure
2.5.4	Connection to the I&C System
2.5.5	Architecture of the Service Unit
2.5.6	Handling and Use of the Service Unit
2.5.7	Testing and Maintenance
2.6	Control of System Access (in particular, 2.6.2 Technical Measures)
2.9	Interference-Free Communication (in particular, 2.9.3 Ethernet Communication)
3.1.1.1	System Overview
3.1.1.4	Requirements and Architectural Challenges
3.1.3.4	Runtime Environment (RTE)
3.2.2.2	Goals of the Integration and System Tests
3.2.2.3	Qualification Process
3.2.2.4	Submitted Documents and Results
4.1	Typical Architecture of Safety I&C Systems
4.2	Design Principles
4.3	Signal Transmission from Class 1E to non 1E Equipment and Circuits
4.4	Single Wire Signal Transmission
4.5	Digital Data Transmission via Serial Busses (in particular, 4.5.1 Communication with the Service Unit)
7.6	Independence

7.9	Control of Access
7.20	Maintenance Bypass
8.1.1	Overall System (in Qualification Documents)

The NRC Safety Evaluation Report (SER) for the TXS Topical Report discusses the Service Unit, its use, and its isolation from the safety-related portions of the system:

Section 2.0	SYSTEM DESCRIPTION (at pages 5 and 6)
Section 2.2	Software Description (at pages 15 and 16)
Section 2.2.1.1	Operating System Software (at pages 19 and 20)
Section 2.2.1.2	Platform Software (at pages 21, 22, and 27)
Section 5.0	SUMMARY OF REGULATORY COMPLIANCE EVALUATION (at pages 47, 51, and 52)

NRC document DI&C-ISG-04, Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc) Interim Staff Guidance, Revision 0, states in the IMPLEMENTATION section that:

> "Except in those cases in which a licensee proposes or has previously established an acceptable alternative method for complying with specified portions of the NRC's regulations, the NRC staff will use the methods described in this Interim Staff Guidance (ISG) to evaluate licensee compliance with NRC requirements as presented in submittals in connection with applications for standard plant design certifications and combined licenses."

Duke Energy notes that earlier drafts of DI&C-ISG-04 contained additional language that reflected the understanding of this implementation statement that was communicated by NRC at various stakeholder meetings. The specific statement was:

> "Systems accepted by the staff in the past that are not fully in accordance with this guidance were accepted on the basis of detailed case-by-case review: that prior acceptance is not rescinded or diminished by this guidance, nor does it serve as precedent for waiving the guidance provided herein."

Duke Energy is not aware of any communication from NRC that indicates that's the earlier understanding of the implementation has been fundamentally changed.

The relevant aspects of the Oconee RPS/ESPS Service Unit design, its use, and its isolation from the safety-related portions of the system were extensively described in the TXS Topical Report and approved by NRC in the associated SER.

RAI 29

Slide 63 - This slide shows data flow for various types of messages. Does the notation →CPU)"or "(CPU→)" refer to the MSI, and if so, why was this not shown in that manner?

Duke Response to RAI 29

The notations (CPU ⇒) and (⇐ CPU) were used to represent the TXS safety processor performing the Monitoring & Service Interface (MSI) function. The notation was chosen to represent both the intermediate MSI role and the fact that a TXS safety processor was handling the message.

RAI 30
Slide 64:

(a) Are the yellow lines Profibus between the various RPS channels and the MSI/RPS E?

(b) There is a vertical black line connecting the service unit, the TXS gateway and the line from the MSI / RPS E. This line extends beyond those units. Please define this line, and list all devices attached to this line, or which could be attached to this line in other applications.

Duke Response to RAI 30

Response (a): Slide 64 describes how service and signaling messages are transferred on the networks. Slides 9 and 10 describe the various data links as to protocols (i.e., L2 PROFIBUS or H1 Ethernet) and the transmission media (i.e., fiber optic or copper wire).

Response (b): The black line on slide 64 is meant to represent a simplified communication path. The line extensions are not meant to imply any other connections. Slide 9 shows this data network in more detail. Document 1 listed in Table 1-2 of the Oconee RPS/ESPS LAR shows the detailed system architecture.

RAI 31
Slide 65 - This slide states that signaling messages are assembled in phase 6 of every cycle (see slide 35, 1st sub-bullet). Does this mean all messages to all devices are assembled in phase 6, and sent in phase 7? Please provide an exact description of what occurs in every part of phases 6 and 7, in what order, and how this order is controlled.

Duke Response to RAI 31

Yes, all messages are assembled in phase 6 and sent in phase 7. The Runtime Environment (RTE) for each safety processor (SVE2) assembles the pre-defined individual data message each cycle. Each data message is separate and individual. Each data message is assembled separately and transferred to a separate and specific dual port random access memory (DPRAM) location. After transfer of the messages to the DPRAM, the safety processor is not involved with and further communication tasks for the messages; instead, the communication module (SL21) handles all network communication activities. A failure of the SL21 module has no affect on the operation of the SVE2 module.

-
-
-
-
-

RAI 32
Slide 66:

(a) *The 1st bullet discusses information commands allowed during normal operations. The read back and request for repeated transmission would indicate there is two-way communications between the non-safety service unit and the safety system during normal operation, even when the key switch is not released. Please confirm this.*

(b) *The 5th sub-bullet mentions "trace data for Oconee." What is this and how is it used?*

Duke Response to RAI 32

Response (a)

The Oconee safety processors are set to allow requests of trace information during online operation. This setting gives the operating staff the ability to view internal data and status of the safety function processor. The trace request simply requests the trace data; the request does not allow of any changes on the safety function processors. For further information of when this information transmission is processed, see response to RAI 12.

RAI 33

Slide 68 - The 5th sub-bullet on this slide states that service commands are accepted for execution if the "Service command is permitted for execution in the current RTE operation mode" Please list each service command, and under what conditions could it be executed. Of particular interest are those service commands which could be executed with the TXS on-line and performing its safety function.

Duke Response to RAI 33

The data format for each type of service request is predefined, consisting of the request code and a set of required request parameters that are request-specific. One or more service requests are sent in the data section of the service message frame. Each individual service message sent by the TELEPERM XS Service Unit is addressed to an individual safety function processor.

Table 33-1 provides an overview of the service requests of the Runtime Environment (RTE) and indicates by an "x" the respective operation modes in which they are permitted (I=**I**nitialization during start-up, O=**O**peration, P=**P**arameterization, T=Function **T**est, D=**D**iagnosis). The TXS is on-line and capable of performing its safety function in the Operation and Parameterization (when not in bypass) modes.

RAI 34
Slide 69:

(a) *This slide mentioned protocols for communications independence for two-way communications. Please provide the definition of those protocols.*
(b) *The 4th sub-bullet states that there is no "strong" response time requirement. What is the response time requirement?*
(c) *Please define, in detail, the signaling messages mentioned in the 5th sub-bullet.*

Duke Response to RAI 34

Response (a): The interference free communications protocols for PROFIBUS and Ethernet communication links are:

- Use of a fiber optic transmission medium to ensure that effects caused by electromagnetic interference can not propagate,
- Individual memories for each message ensuring the separation of the data flow for sending and receiving,
- Cyclic processing of all tasks (message transmission included) without any possibilities of influencing the linked communication systems (independent control flow of communication module SL21 and safety function processor SVE2),
- Check on the received messages for whether the transmission has been performed with valid message data as a matter of principle, and
- Input data voting on principle to generally ensure correct input data for function diagram module processing.

The following additional features are ensured for TELEPERM XS (TXS) communication via SINEC H1:

- Communication to other digital systems (outside TXS) is engineered to be unidirectional in the application software of the Monitoring and Service Interface.
- The change of the operating mode of a dedicated SVE2 processor required the transmission of two different messages coordinated in time: a request message initiated by the service staff from the service unit and a signal message containing the enable signal. An unintended change of the operating mode by faulty or erroneous messages can be excluded.
- The enable signal is processed such that:
  - the required system fault tolerance conditions are ensured (which is considered as the basis for the system architecture) and
  - an intended change of the operating mode of a dedicated SVE2 processor is compatible to the being plant operating conditions.
- If during test performance the initial release conditions which allowed the start of a test are violated (either by plant operating conditions, decided by the reactor operator, or by a fault in the TXS system) the test is automatically finished by a reset and the system returns to normal cyclic operating in some seconds.

See responses to RAIs 12, 15, 16, 28, 32, 34, 40, and 80 for detailed information on the safety-to-safety and the safety-to-nonsafety communication protocols.

Response (b): The intent of the statement is that there is no numeric response time limit specified for the processing of service requests. There is no safety-related response time requirement for the service requests. As discussed in the response to RAI 12, service messages can be transmitted over several cycles as Priority 2 tasks.

Also see response to RAI 16 (d).

RAI 35
Slide 71:

(a) Please redraw this slide to show exactly where and how each task is entered and exited. What triggers the departure from each task?

(b) How is the time available for the self-test task determined, and by what?

Duke Response to RAI 35

Response (a): The TELEPERM XS (TXS) operating system is a static multitasking real-time operating system. Static in this context means that all the operating systems resources used are specified on system startup and are not variable during runtime. The kernel of the operating system includes a small scheduler that can manage up to 16 tasks. The scheduler is activated cyclically by a millisecond hardware timer and is responsible for coordinating the task. During normal operation of the TXS system, up to three tasks are active: the Runtime Environment (RTE), the service task, and the automatic self-monitoring. The RTE is the actual platform for the application function. It is activated cyclically by the operating system and calculates the specified application functions. The service task is activated by the RTE if

it identifies a permissible request from the Service Unit. After the request has been processed the service task deactivates itself. The automatic self-monitoring operates as a continuous background task which cyclically checks the hardware equipment of the function processor for correct functioning. See the response to RAI 12 for more information on these tasks.

In addition to the three tasks that are used during normal operation, two other tasks are included in the operating system, which are only activated during startup or under fault conditions.

In addition to task coordination, the operating system also provides services for accessing the hardware, setting, and resetting hardware timers and for communication between the various function processors. The communication is implemented in such a way that it is always transparent to the application software whether the function processors are plugged into the same subrack or whether they are addressed via a serial bus.

The RTE is the most important task of the function processor because it calls the actual application functions. It is activated cyclically by the operating system and then processes the following functions:

- resetting of a hardware timer as a watchdog,
- incrementing the cycle counter,
- reading in the process data from the input/output modules,
- reading the messages from the dual-port random access memory (DPRAM),
- transfer of the data to the function diagram group modules,
- processing the function diagram group modules,
- checking the fault messages from processing the function diagram group modules and setting the fault status signals,
- output of the results via input/output modules,
- transmission of messages to other function processors,
- activation of the service tasks, if permissible manual service requests have been identified, and
- deactivation of own task until the next cycle.

The functions processed cyclically by the RTE are described below.

At the beginning of the processing cycle, on the one hand, the local cycle counter is incremented and the watchdog timer is set to a value that is larger than the activation cycle for the RTEs set in the operating system. If the RTE does not terminate correctly due to a fault in the signal flow, the watchdog timer times out and generates a hardware interrupt. This interrupt then activates a special interrupt service (exception handler) that saves the state of the computer for subsequent analysis and puts the computer into a defined fault state. In this fault state, all output signals are set to predetermined states and the processor is kept in a waiting loop. The signal outputs are disabled in several different ways by explicit driver calls and by a hardware signal (BASP) via which the load power supply for the input/output modules is disconnected.

The 16-bit cycle counter forms the internal relative short-time base. It is used as the sign of life clock for communication and for time-sequencing of fault signals. The cycle count of the RTE at the time of transmission is appended to every message. This information is used by the receiving function processor to monitor the validity of the message and correct functioning of the transmitter.

Data are input and output via the input/output modules directly through driver programs which access the buffers of the input/output modules either writing or reading data. A separate driver program exists for each input/output module and is also responsible for module-specific conversion of the data. Fault alarms that are detected on the input/output module (wire break, overflow, and underflow) are used to mark the signals concerned with the signal status "ERROR." Each configured signal in TELEPERM XS contains not only the signal value but also a signal attribute with the status flags "Fault" and "Test." These flags are used for fault masking. Missing front connectors or a missing load power supply can result in the enable signal for addressing input/output modules not being formed. The missing enable is detected and signaled by the time-out monitoring. At the same time, the status flags are set to "ERROR" for all signals concerned so that these signals do not have any effect on further function processing.

Messages are read by direct access to the local DPRAM. In applications with high safety relevance, all messages contain additional data for integrity monitoring on the application layer. This includes the cycle count of the RTE which has transmitted the message, the message identification number, the message length, and a checksum with which the integrity of the data from the RAM of the transmitting function processor to the RAM of the receiving function processor is monitored. If the RTE detects that the cycle count has not been incremented properly in a message received, this means, on the one hand, that all data contained in the message are too old and must be considered faulted and, on the other hand, that the information must be stored in the cyclically transmitted signaling messages indicating that an upcircuit function processor is no longer functioning properly. An incorrect checksum also indicates that the signals of the message are inconsistent and must be excluded from all further processing. If the data received are up-to-date and consistent they are passed on to the actual application functions (function diagram group modules).

The function diagram group modules are activated by the RTE in the form of function calls. Function diagram modules and function diagram group modules are generated by code generators from the formal specification (hardware and software specification). All safety functions are specified as function diagrams. Each function diagram is implemented in software by one and no more than one software module (i.e., the function diagram module). Because several function diagram modules are typically implemented on one function processor, all function diagram modules that are to be processed with the same cycle time are grouped together to form function diagram group modules. A function diagram group module therefore consists of a sequence of calls to function diagram modules and copy functions by which signal transfers between the function diagram modules are implemented. A function diagram module consists of a sequence of calls to function block modules that are interconnected by data structures.

After processing of the function diagram group modules, the results are passed on by the RTE either to the input/output modules via drivers or to other function processors in messages. The cyclic signaling messages are also transmitted to the monitoring and service interface and on to the Service Unit. These messages provide information on the current state of the RTE. If faults occur during the processing of the function diagram group modules, all the signals affected are marked with status "FAULT" before being passed on.

After processing of the actual application software, the request messages cyclically transmitted from the monitoring and service interface to the function processor is evaluated. If this request message contains a permissible request from the Service Unit, the service task that interprets this request is activated and executed. Requests from the Service Unit include requests to output specific data such as the contents of the fault buffers or parameters, etc., but also requests for changing the operating mode of the RTE. All requests for changing the operating mode of a function processor are only executed if a second, independent enable signal is set for the RTE of the dedicated function processor. The path via which this second, independent enable signal is issued is configured application-specifically on function diagrams. After a request from the Service Unit has processed, the request task deactivates itself.

When the RTE and the service task are inactive, cyclic self-monitoring is executed as a low-priority background task by the operating system. This task checks the hardware functions of the function processor in a recurring cycle. During runtime, three tasks are defined:

- Monitoring task: The monitoring task is automatically started by the operating system after each reset. Control starts in the RTE initialization (module INIT), which controls the complete initialization phase of the RTE. After successful initialization, control is permanently passed to the RTE monitoring (module MONIT). The RTE monitoring controls the processing of service requests received via service messages from the external Service Unit. When no more service requests need to be processed, the monitoring task is suspended. It is activated by the cycle task each time a new service message is received.
- Cycle task: The cycle task is activated by the RTE initialization after successful completion of the initialization phase. The cycle task is controlled by module CYC, and operates with a predefined, constant cycle time, which equals the cycle time of the fastest of its function diagram group modules. The cycle task handles all communication via messages, the input/output modules, and the cyclic processing of the function diagram group modules. It has the highest priority of all three tasks, thus ensuring that the cyclic operation of the function diagram group modules always happens with the specified cycle time. If a new service message from the Service Unit has been received, the cycle task activates the monitoring task to process the service requests. This takes place asynchronously with the cycle task and may last several cycles. After the service requests have been processed, the cycle task takes over the results and sends the request responses to the Service Unit with the next signaling message.

- Self-monitoring task: The self-monitoring task is automatically started by the operating system after each reset. It has the lowest priority of all tasks, and is only scheduled when the monitoring and cycle tasks are not active. The self-monitoring task is controlled by the self monitoring software, which continuously performs tests of all relevant hardware components of the processing module (RAM-test, ROM-checksums, watchdog-test, etc.).

The design decision to separate the RTE cycle and the RTE monitoring into two separate tasks was made for the following reasons.

- The RTE monitoring processes the service requests received via service messages from the Service Unit. Processing of these requests requires additional computing time, depending on the request and its parameters. For example, programming the EEPROM might take up to 2 milliseconds per byte. By separating the RTE monitoring and RTE cycle in two tasks, the computing time for the cyclic operation is decoupled from the computing time needed for request processing. Thus deterministic behavior, i.e., nearly constant computing time, can be achieved for the function diagram group module processing, and maintaining the required cycle time is guaranteed.
- The scheduling sequence of the three tasks is shown in Figure 12-1 in the response to RAI 12. The cycle task and the monitoring task share a set of common functions to access commonly used data, for example in the modules ERRORMSG, MODE, FDGIFC, and TRACE. The coordination between the two tasks is done by protecting critical regions of control-flow with a mutual-exclusion semaphore. The cycle task holds the semaphore from the start of its operating cycle until its end. Thus the monitoring task cannot access (nor change) common data as long as the cycle task is active. The monitoring task holds the semaphore only for short time intervals (< 1 millisecond), for example for writing a new parameter value, and then immediately releases it. This guarantees that the start of the cycle task can not be delayed inadmissibly by the monitoring task.

See responses to RAIs 12, 13, 31, and 35 for additional information on the runtime tasks.

Response (b): The time available for self test tasks is the time remaining in a cycle (e.g., 25 ms) after the safety function process (cycle task) and the service task have been executed. The remaining time is used to execute the self-test tasks until it is time to start the cycle task again. A 1 ms Interrupt Timer is used to schedule and control the execution of the cycle task, service task, and the self-test task.

The safety I&C system is designed such that the actual safety functions (the application software) does not require more than approximately 50% of the CPU time (the runtime of the RTE only amounts to a few milliseconds). This permits the self-monitoring to also make use of approximately 50% of the CPU time. A complete check of the hardware of a function processor takes approximately 10 minutes.

The amount of time available for each safety processor (SVE2) is based on the time it takes to process the function diagram groups assigned to that processor. The time available for the self-monitoring tasks can be different for each safety processor; however, the time available for self-monitoring tasks is the same for each cycle of a safety processor because of the deterministic nature of the processing cycle.

Also see response to RAI 12 for additional discussion.

RAI 36

Slide 75 - This slide discusses communication with the service unit. Please describe the isolation of the service unit from other non-safety plant equipment, and how that isolation will be maintained.

Duke Response to RAI 36

The only connection from the TELEPERM XS (TXS) Service Unit to other plant equipment is through the TXS Gateway. The NetOptics port tap (one way communication device) prevents any data communication from the Gateway to the TXS Service Unit or the Monitoring and Service Interface. The TXS Service Unit is not connected to any other equipment. This configuration is shown in LAR Figure 2.1-1. This same information is shown on Slide 9.

RAI 37

Slide 78:

(a) The 1st bullet and sub-bullet says the RTE is "similar" to the RTE of function computers. Please explain what "similar" means, and specifically point out any differences.

(b) Please provide an exact definition, format, bit assignment, and method of formatting for each type of data, service and signaling message, and when each is used.

(c) The 4th bullet mentions the one-way communications device. Please describe this device in detail, and in particular, provide sufficient information so the staff can confirm the one-way nature of this device.

Duke Response to RAI 37

Response (a): The Runtime Environment (RTE) on the TXS Gateway provides the same functionality as RTE the SVE2 safety processors. The differences are as follows:

- RTE for the TXS Gateway runs in a different software environment compiled for a personal computer rather than a SVE2,
- Operating system services based on Windows instead of MICROS,
- MicroNET send/receive interface for messages based on the local area network interface of the TXS Gateway computer rather than a SCP2, and

- No self-monitoring tasks are performed on TXS Gateway.

The RTE of the TXS Gateway provides capabilities to receive service messages and respond to service requests; however, this capability is not used for the Oconee RPS/ESPS design because signaling messages from the TXS Gateway are blocked by the NetOptics device.

The TXS Gateway software is developed using the TXS SPACE tool. It is subject to the verification and validation activities outlined for Software Integrity Level-2 software in accordance with Oconee Software Verification and Validation Plan.

Response (b): Data messages from the TXS channels (routed through MSI) to the TXS Gateway contain information for display on the plant computer. Service message are messages from the TXS Service Unit to the TXS Gateway. Signaling messages are responses to Service Requests (contained in service messages) from the TXS Gateway to the TXS Service Unit. In the Oconee RPS/ESFAS design, signaling messages are blocked by the NetOptics port tap (one way communication device).

See response to RAI question 10 (a) for information on data message size, how Data message size is determined, and what is the content of each data message. See response to RAI 16 (d) for information of service and signaling messages.

Response (c): See the response to RAI 5.

RAIs associated with Interim Staff Guidance #4

ISG #4), staff positions # 3, 9, 10, 11,12, 14, 18, 19 and 20 in Enclosure 3 of Supplement 2, "Position Paper on Alignment of Oconee RPS/ESPS with ISG#4 (AREVA Document No. 51-9076647)" need additional information to sufficiently address the ISG Staff positions as follows:

RAI 38

Staff position #3 states: "A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system."

Since the staff has not received the previously requested detailed message formats and bit assignments, please provide this information along with an explanation of how each of these messages enhances the performance of the safety function. Particular care should be given to the reason why this enhancement is necessary, and why this method was chosen, and how it is necessary and related to the safety function.

Duke Response to RAI 38

Detailed information concerning the message formats and bit assignments is provided in response to NRC RAIs 10 and 12. In regards to the necessity of data transfer between the channels and the enhancements provided by the data transfer, the following information provides the details on the purpose of the system functions which utilize interchannel communications.

As noted in ISG 4 Staff position #3, unnecessary complexity within the safety processor functions must be avoided. The Oconee RPS/ESPS design utilizes specific design features that enhance the performance of the safety system.

One requirement of the RPS/ESPS is to provide online function monitoring and channel check capabilities. These functions are performed using data transfer between the safety channels using interchannel communications. By incorporating the online channel function monitoring and channel check capabilities, the safety processors are able to detect sensor faults and equipment malfunctions in a continuous manner which exceeds the Technical Specification Surveillance Requirements for Channel Functional Testing and Channel Checks of the RPS/ESPS equipment. These functions provide an enhancement to support the safety function of the system.

In addition to the Channel Functional Testing and Channel Checks, the interchannel communications provide for the use of the 2nd Min/2nd Max feature. The 2nd Min/2nd Max feature provides an enhancement by reducing the potential cause for spurious actuation. Once the first signal passes the threshold for channel actuation, notification to the operator is provided without placing the system in a half trip/actuation condition. Thus, the issue can be investigated without risking an inadvertent plant trip or transient. The 2nd Min/2nd Max function provides a safety benefit to reactivity management and fault tolerance.

Another form of communication to the safety processor is from the TXS Service Unit. The TXS Service Unit provides for online data logging, trends, and maintenance support. The information from the TXS Service Unit is only available when the Service Unit is connected to the RPS/ESPS. The response to NRC RAIs 10 and 12 outline how data communication to the TXS Service Unit does not impact the performance of the safety functions. Thus, the enhancement to the RPS/ESPS data collection is performed without impacting the safety function processor. This is a case where the data collection function is being performed outside of the safety processor which meets the intent of the NRC Staff's position.

RAI 39

Staff position # 9 states: "Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device."

Please describe how the memory locations within the shared memory are allocated and fixed. The staff has been told this occurs when the software is compiled, but does not understand how this is done, how the memory allocation is fixed, what would occur if more memory is allocated than is physically present, and how the transmitting and receiving units know what the allocation is, and how to used that data.

Duke Response to RAI 39

See responses to RAIs 6 and 7 for information on memory allocation.

RAI 40

Staff position # 10 states: "Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment." This section goes on to state: "A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual processor / shared memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic."

The staff understands that the Areva TXS system proposed for use at Oconee uses key switches which sets a bit within memory, and does not use a physical disconnect. This would appear to conflict with staff guidance. Please explain why the TXS system should be approved. Include in the discussion any additional protection which may exist, or what additional protection will be provided by Oconee, beyond the normal key protection, sign-out requirements, and administrative activities which would also be used for a physical disconnect key switch.

Duke Response to RAI 40

The NRC RAI points to several protection activities that are typically performed as part of the control of a physical disconnect keyswitch. The ONS TXS system uses a combination of personnel access controls, administrative controls, and design features (including hardware and software elements with appropriate alarms) to protect the safety-related software from unauthorized alteration.

RAI 41

Staff position # 11 states: "Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety function processor unless all safety functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence."

Please provide a detailed description of how interdivisional communication explicitly precludes the ability to send software instructions to a safety function processor, and how receipt of a message about the unavailability of a sensor will not direct the processor to branch to a new instruction sequence.

Duke Response to RAI 41

The TXS system only sends data messages in interchannel communication. Data messages do not affect or alter the safety function processor. There are no software instructions or commands that are sent via interdivisional communications.

The validity of the sensor data and message status information is processed within the application software in the same manner every cycle. The application software acts on the data in the same manner every cycle; no branching occurs based on the receipt of a sensor error message. Detailed information pertaining to the methods that interchannel communications and message handling occurs is provided in the response to RAIs 10 and 12.

RAI 42

Staff position # 12 states: "Communication faults should not adversely affect the performance of required safety functions in any way."

Please provide the detailed message formats and bit assignments, with an analysis of how an error in each part of the message would be detected. This information is similar to that requested for Staff Position # 3.

Duke Response to RAI 42

Communication faults will not adversely impact the performance of the required safety functions. A worst case fault condition (total loss of interchannel communications) will result in the safety channels functioning in the "silo" mode where they react to their specific input devices without considering the inputs from the other channels.

The TXS SER approves the system response to the worst case hypothetical failure mode of total loss of inter-channel communications. The TXS design is able to detect any

communication faults and respond in an acceptable manner. For RPS functions, the 2.MAX/2.MIN blocks respond to loss of communication with the "silo" mode which is similar to one-out-of-one hardwired logic. For ESPS functions, the voters fail in the desired state of not actuated. Any loss of communications results in control room alarms. Therefore, the Oconee TXS design is consistent with the design concepts approved in the SER.

The response to, or detection of, specific communication hazards are described below:

A discussion of the message formats and bit assignments is provided in the response to NRC RAIs 10 and 15.

RAI 43

Staff position # 14 states: "Vital communications should be point to point by means of a dedicated medium (copper or optical cable). In this context, "point to point" means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified."

The TXS system proposed for use at Oconee does not appear to use point to point communications, please provide a detailed description of the communications methods used. In particular, please show any instances where more than one communications link used the same wires or fiber, any instance where the same communications port or hardware is used, or where more than one communications link used the same software to process the data.

Duke Response to RAI 43

The Oconee RPS/ESPS application uses only point to point communication with separate communication links for each communication channel. Detailed information related to the point to point communication is provided in the responses to NRC RAIs 10 and 16.

RAI 44

Staff position # 18 states: "Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication."

Please provide this analysis.

Duke Response to RAI 44

A discussion of the various communications and the enhancements provided by the communications is provided in the response to NRC RAI 38.

RAI 45

Staff position # 19 states: "If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety functions. Communications throughput thresholds and safety system sensitivity to communications throughput issues should be confirmed by testing."

Please show how Oconee identified the true data rate, including overhead, to ensure that communication bandwidth was sufficient to ensure proper performance of all safety functions.

Please provide the information on the true data rate and overhead. In addition, please show how this was tested.

Duke Response to RAI 45

The TXS communication loads are constant and occur in a deterministic manner as described in the response to RAI 10. The results of the design analysis using the *netload* tool indicate that the worst case constant communication loading between safety channels is less than the rated capacity of the data links. Proper operation of the communication links are validated during the pre-FAT hardware integration tests.

RAI 46

Staff position # 20 states: "The safety system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing."

Please provide these calculations and design basis data error rate, and how this was tested.

Duke Response to RAI 46

For the Oconee RPS/ES project, AREVA NP produced a calculation for the RPS/ES Controls Upgrade response time. The calculation documents the response time of the TELEPERM XS platform, application software, and peripheral modules associated with the upgrade of the Oconee RPS/ES. The scope of the response time calculation covers the portions of the safety circuits that are being replaced with the TELEPERM XS platform and have response time requirements. It does not include response times of field sensors, or response times of actuation equipment (i.e., valve and damper stroke times, spin-up times of pumps and fans, etc.) which are note being replaced by the RPS/ES modification.

The response time for each process function was determined by algebraically combining:

- The time constants of the input hardware peripheral modules
- Time delays due to the Application Software Function Blocks included in Functional Diagrams Group (FDG) modules (e.g., software filters, B-Delays, pulse generators, software timers, etc.)
- The response time due to signal propagation of the TELEPERM XS digital signal and network communications
- The time constants of the output hardware peripheral modules

The response time of the distributed TXS I&C system is determined in accordance with the approach described in EPRI TR-114017 Final Report, July 2002 – "Qualification of the Framatome ANP TXS Digital Safety I&C System – Revision to EPRI TR-114017". EPRI TR-114017, Section 9.1.2 describes a general approach for determining response times and illustrates that process with a generic evaluation. For an application specific analysis, input

parameters (i.e., CPU cycle time) used in the generic analysis are replaced with site-specific values.

The effect of the loss of a message, which is considered data error, due to age is bounded by the loss of the affected, single communication link within the Oconee RPS/ESPS System Architecture. A lost message has the same effect for the monitored parameter as a loss of communications on that link. The bounding effect of a single communication link failure has been analyzed in Failure Modes and Effect Analysis performed for the Oconee RSP/ESPS design. That analysis concluded that the failure of a single communication link does not prevent the performance of the safety system function because either valid signals from other redundant channels are received or the redundant channels would provide the safety actuation within the required response time. AREVA NP Document 51-5023886-03, Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Failure Modes and Effects Analysis, was submitted to NRC in LAR Supplement 1.

The response time requirements are obtained from Revision 5 of Oconee calculation OSC-8623, "RPS and ESFAS System Functional Description." The response time calculated results are contained in AREVA document 32-9009296 -004 "Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Response Time Calculation." A copy of AREVA NP document 32-9009296-004 is provided in Enclosure 3. The response time analysis reflects the message age monitoring behavior described in response to RAIs 17 and 19.

The calculated response time meets the required response time of the RPS and ESPS.

Thee non-safety Diverse Actuation equipment is not included in this calculation. The response time of the Diverse Actuation equipment will be verified by test only.

The response times calculated for the RPS and ESPS will be tested during the Factory Acceptance Test. The FAT procedures are still under development and will be provided once the procedures are approved. The schedule for providing the FAT procedures has been discussed with the NRC during previous meetings and conference calls.

RAIs associated with Software Program Manual

RAI 47
Please provide the copy of Office Instruction, OI-1457, "TELEPERM XS Software Quality Assurance Plan," that is applicable to the Oconee RPS/ESPS project.

Duke Response to RAI 47

The current version of AREVA NP Operating Instruction, OI-1457, *TELEPERM XS Software Quality Assurance Plan*, is provided in Enclosure 2.

RAI 48
Please provide the latest applicable copy of AREVA NP Inc. Document No. 51-9001942-004, "Oconee Nuclear Station, Unit 1 RPS/ESPS Controls Upgrade Software Generation and Download."

Duke Response to RAI 48

AREVA NP document 51-9001942-004, Unit 1 RPS/ESFAS Controls Upgrade Software Generation and Download, is provided in Enclosure 2.

RAIs associated with Verification and Validation (V&V)

RAI 49
Please provide a detailed description of the Duke review and oversight activities of the Oconee safety system V&V efforts, which were performed by its vendor.

Duke Response to RAI 49

In Supplement 4 of the Oconee RPS/ESPSLAR dated May 28, 2008, Duke addressed the NRC issue associated with V&V. This included addressing NRC concerns associated with AREVA independent V&V activities. Supplement 4 asserted that the V&V group is technically, managerially, and financially independent from the design organizations. Duke confirmed this by sending personnel from the Oconee Reactor and Electrical Systems engineering group and from the Oconee Major Projects engineering group to AREVA Alpharetta to review their V&V processes. These reviews were focused on ensuring that adequate independence existed between the V&V group and the design group. During the reviews, personnel from the V&V group were interviewed and the business organization structure was evaluated. Based on these reviews, Duke concluded that the AREVA V&V group is technically, managerially, and financially independent from the design organizations.

Supplement 4 states that the V&V group has technical competence equivalent to the Software Design group and that V&V personnel are trained on the TXS System Software and Hardware as well as the provisions of the software development process. Duke confirmed this by reviewing V&V personnel training records and interviewing V&V personnel to evaluate their understanding of their roles and obtain their perception of the qualifications required to perform V&V activities. As a result, Duke concluded that the AREVA V&V group personnel are as qualified as the Design group personnel.

Also, during oversight reviews, Duke focused on V&V document development and approval. As noted in Supplement 4, the V&V documents include but are not limited to Factory Acceptance Test (FAT) plans, Requirements Traceability Matrix, specifications, procedures, and reports.

Duke performed a detailed review of the FAT plan to ensure that adequate functional testing was being factored into the FAT. Duke provided comments that included operating experience from a previous project for the Digital Control Rod Drive Control System replacement testing. As a result, the FAT includes additional testing of the RPS/ESPS power system voltage and current information to validate breaker and cable sizing. During review of the FAT plan, Duke commented that Lead/Lag testing needed to be performed during the FAT. Independently, the AREVA V&V group provided the same feedback on the FAT test scope. As a result, the FAT includes Lead/Lag testing. The FAT Plan was one of the documents subjected to a Quality Management Plan review and was approved by the Licensing and Quality Steering Team (LQST) after resolution of all FAT plan comments.

Duke reviewed the Requirements Traceability Matrix (RTM) to verify the accuracy of the tracing of the design requirements into the design. Revision 1 of the RTM was reviewed since it covered the V&V review of the design phase. Duke's review identified errors where design requirements were traced to an incorrect design document. The Duke review team determined that Revision 1 of the RTM was not accurate and needed to be corrected prior to being accepted by Duke. Revision 2 of the RTM was developed by AREVA to address Duke's comments and to validate the entire RTM. As part of the RTM review, Duke observed preparation of revision 2 at AREVA's office in Alpharetta, Georgia. This observation confirmed that AREVA V&V personnel had the correct focus on developing an accurate RTM. Following receipt of RTM revision 2, Duke performed another review to ensure all comments were addressed and a thread audit of additional requirements to ensure that no new problems were introduced by revision 2. Duke's reviews resulted in a determination that all identified issues with the RTM were corrected.

Additional reviews of documents such as the Software V&V Plan, Software Design Description, Software Requirements Specification, Software Configuration Management Plan, and Software Safety Plan were performed by Duke as part of the Quality Management Plan for the RPS/ESPS project. All of these documents had extensive comments that required revision of the document prior to acceptance by the LQST.

Duke made copies of LQST Completion files available to the NRC for review during the NRC's Oconee site visit the week of May 15 – 19, 2008. The LQST Completion files provide a record of comments and how they were resolved, meeting minutes, and completed forms indicating LQST approval. These files were created for all of the documents reviewed under the Quality Management Plan. Additional details on the Quality Management Plan are provided in the response to NRC RAI #53.

Another attribute of V&V reviewed by Duke was the authority and resources of the AREVA V&V group to ensure V&V activities are not adversely affected by commercial and schedule pressures. Meetings with the V&V personnel demonstrated that adequate resources are available within the V&V team to perform the V&V activities for the Oconee RPS/ESPS project. Interviews with the V&V personnel, hardware design personnel, and software design personnel confirmed that the V&V group has overall authority for the V&V activities that included FAT. An example of this authority was demonstrated when the V&V group required Lead/Lag testing be added to the FAT procedures (as described above).

RAIs associated with Factory Acceptance Test (FAT)

RAI 50
Please provide an explanation of what documentation is impacted by the change in the testing strategy, summarizing the impact, and providing a schedule for the submittal of the revision to these documents.

Duke Response to RAI 50

Duke Energy provided a response to acceptance review issue 5 by letter from David Baxter dated May 28, 2008. In that response Duke Energy committed to revise the Software Verification and Validation Plan and the Factory Acceptance Test Plan to reflect the modified approach outlined for validation testing. These two documents are the only documents affected by the change in testing strategy. The following AREVA NP documents are provided in Enclosure 2:

- AREVA NP document 51-9052960-003, Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade Factory Acceptance Test Plan
- AREVA NP document 51-9010419-007, Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Software Verification and Validation Plan

RAIs associated with Exceptions

RAI 51
Please provide the documentation identifying all standards used by the supplier and any deviations from these standards, including any associated acceptability determination.

Duke Response to RAI 51

The Oconee RPS/ESPS LAR identifies all standards used by the supplier (AREVA). During an April 2, 2008, Duke/NRC Conference Call, the NRC Staff asked Duke whether the Oconee RPS/ESPS digital upgrade complies with all the standards referenced in the LAR. Duke's initial response was that if the words comply or conform were used then the digital upgrade complied, however, such words indicating IEEE Standards were used or followed did not necessarily indicate compliance with a standard. Because of these wording differences, Duke agreed to evaluate the wording of the RPS/ESPS LAR and determine whether any exceptions to IEEE standards and other guidance were taken other than those already noted.

Duke has concluded based on this review that the RPS/ESPS digital upgrade complies with IEEE Standards, regardless of verb usage, except where specifically noted. The only exceptions taken were to IEEE Std. 828-1990 and IEEE Std. 1012-1998. The exception to

IEEE Std. 828-1990 is addressed in LAR Enclosure 1 Section 3.4.3.2.6. Exceptions to IEEE Std. 1012-1998 are addressed in LAR Enclosure 1 Sections 3.4.3.2.4 and 3.4.3.2.6.

Additional information is provided in responses RAI 68 (configuration management) and Acceptance Review Issue 5 (verification and validation).

RAIs associated with Changes

RAI 52
Please provide an explanation of the changes to the TXS system since the TXS Topical Report that includes a fact based explanation of changes, and an explanation of how these facts can be combined to arrive at an acceptability determination.

Duke Response to RAI 52

See Attachment 3 to this Enclosure

RAIs associated with Quality Management Plan

RAI 53
Please provide an explanation of the Duke review of documentation produced by its vendor, and of Duke's vendor audit activities: (a) a detailed explanation of the activities requested, (b) providing examples of the issues identified by Duke, and (c) how issues were resolved.

Duke Response to RAI 53

In Supplement 4 of the Oconee RPS/ESPSPS LAR, Duke provided a brief overview of the Quality Management Plan (QMP) initiated by Duke. The QMP provided supplemental guidance and instructions where needed to ensure that the RPS/ESPS Upgrade Project deliverables, associated with licensing the new TXS system, met quality requirements. The following explanation provides detailed information about the QMP, the project activities that were reviewed under the QMP, examples of issues identified by Duke using the QMP, and the resolution of the identified issues listed as examples.

In September 2006, AREVA NP concluded, and Duke agreed, that the RPS/ESPS Project could not produce technically acceptable, high quality work products in a predictable manner. AREVA NP formally issued a restraint order. Work was stopped on the RPS/ESPS project until appropriate corrective actions were taken to ensure proper personnel qualifications and operating instructions existed to restart work on the RPS/ESPS project. Following the completion of the required training and revision/development of the necessary operating instructions, AREVA NP QA allowed the commencement of work on the RPS/ESPS project with restrictions (i.e., AREVA NP QA surveillance of all design activities). At the same time as

AREVA NP's restraint order, Duke QA entered restrictions on the Duke Approved Vendors List to prohibit receipt of any products or deliverables unless Duke QA concurred with AREVA NP QA on implementation of required corrective actions on each deliverable. As part of the RPS/ESPS project team, the Duke QA group assigned dedicated resources to the AREVA NP Alpharetta, Georgia offices to ensure that the QA processes used for the development of AREVA NP documents supporting the RPS/ESPSPS LAR, in addition to the development of application software, were followed.

During this period (from October 2006 until May 2008) Duke QA spent a significant amount of time at the AREVA NP Alpharetta offices. Oversight activities included a review of the document development process, qualification and training of project personnel, and an evaluation of the AREVA NP corrective action program. Also, during this time period Duke QA conducted surveillance activities at supporting AREVA NP locations in Lynchburg, Virginia and Erlangen, Germany. A Duke QA triennial qualification audit performed in April 2008, determined that AREVA NP had implemented significant improvements to the structure of the engineering and QA functions and that the restrictions on the Duke Approved Vendors list associated with AREVA NP could be lifted. Duke QA will continue to perform oversight at the Alpharetta offices including supporting locations throughout AREVA NP. This oversight effort will include monitoring the corrective action process, conducting surveillance of the hardware and software manufacturing, Basic Hardware Testing, and FAT.

For deliverables that supported the development of the Oconee RPS/ESPS LAR submittal, supplemental oversight was implemented using the RPS/ESPS Project QMP. The QMP focused on the following principles to ensure quality Oconee RPS/ESPS LAR supporting documentation.

- Technical and regulatory issues for this kind of project are significantly complex and significant such that no single project management structure alone can effectively implement quality assurance requirements. Therefore, the QMP will be used to supplement underlying programs, skills and leadership.
- Quality is not "inspected into" the system. Quality is achieved by people possessing the competence, skills, knowledge, experience, training, resources, work ethic and motivation to do the job right.
- The QMP is a jointly developed and approved plan by Duke and AREVA NP.
- The QMP is a focused effort to use Human Performance tools and mechanisms to ensure appropriate application of already established programs, policies and procedures.
- People involved in quality activities are properly led by competent managers and leaders so they can do the job right the first time.
- Quality documentation is readily available to provide sufficient objective evidence and a defensible record that QA requirements and commitments have been met.
- The QMP is not constrained by cost or schedule issues.
- The QMP is a standalone document that can be credited and applied to any other project activity, including the project plan, LAR, and other contractual actions.
- The QMP employs a "Trust but Verify" approach with Duke providing oversight on all identified activities that affect project quality. The QMP considers the following questions:

- Is a given deliverable complete? Is it likely to change due to any known, planned or likely influences?
- Are competent resources, training, procedures and guidelines in place, and are they being followed, for all key identified activities from start to finish?
- Does the schedule provide adequate independent verification & validation (V&V) activities and resources?
- If any quality variations emerge on work in progress, are corrective actions being properly identified and resolved? Does the project schedule account for these corrective actions?
- Are appropriate controls in place, and are they being followed, to stop and correct activities that are resulting in inadequate quality?

For the RPS/ESPS project, a Licensing and Quality Steering Team (LQST), made up of appropriate leaders from the stakeholder organizations responsible for key project activities that can affect the quality of project deliverables, was named. Each stakeholder organization used a "Quality Core Team" made up of subject matter experts from their organization, to perform detailed quality verification reviews of project activities.

The LQST generated an initial list of approximately 30 documents requiring QMP application and transmitted this list to the RPS/ESPS Project Manager for inclusion in the overall project schedule. All the documents developed by AREVA NP listed in Table 1-2 of Enclosure 1 to the Oconee RPS/ESPS LAR, and noted as being available for NRC review, were subjected to an LQST review. Duke procedures and uncertainty calculations listed in the table were excluded since they were developed using Duke processes. The LQST also reviewed documents not listed in Table 1-2 that were used to support the RPS/ESPS LAR (e.g., Codes and Standards Matrix, RPS/ESPS TXS System Description, IEEE Std. 1012-1998 Position Paper on V&V, Surveillance Change Justification document, ISG-04 Position Paper).

The response to RAI #49 provides examples of issues identified during the review of the FAT Plan and Requirements Traceability Matrix, as well as the resolution of the issues. Additional examples of issues identified during the LQST review activities are provided below to further demonstrate the thoroughness of the reviews. These examples are only selective examples and additional detail is available for NRC in the LQST documentation files which were reviewed with the NRC during their May 2008 Oconee site visit.

The LQST review of the Codes and Standards Matrix identified that Regulatory Guide 1.97 was incorrectly marked as not applicable to the RPS/ESPS project. In addition, several of the AEC Design Criteria contained in the Oconee UFSAR were incorrectly marked as not applicable to the project despite the reference to the documents in the associated Equipment Specifications. Numerous comments were made concerning the reference of the wrong revision of a code or standard in the matrix. The LQST required AREVA NP to revise the Codes and Standards Matrix document to correct all of the identified issues prior to accepting the document.

The LQST review of the Dedication Procedure for the Absopulse AC/DC Power Supply identified that the Critical Characteristics verification did not include physical characteristics,

the dedication procedure did not contain a sequential listing of the acceptance criteria that coincided with the procedure steps, many procedure steps did not include sign-offs, there were multiple actions per step, and the procedure steps lacked clarity. AREVA NP modified the dedication procedure to address these issues prior to LQST approval. Following completion of the procedure revisions, AREVA NP decided to re-perform dedication testing on all of the power supplies even though the majority of the power supply dedication had already been completed using the initial version of the procedure.

In addition to the LQST review activities, the Duke engineering change process has oversight controls built in the modification process. The oversight controls require verification that all design requirements are designed into the system and tested to ensure proper operation. A verification matrix is developed for the project to list all of the design requirements, how each design requirement is tested in FAT and/or SAT, how each design requirement is tested during post-modification testing, and has sign-offs by plant engineering personnel. The plant engineering sign-offs demonstrate that all of the design requirements have been reviewed and verified prior to installation of the modification.

In order to perform the verification matrix review, the Duke personnel trace the FAT procedures against the Software Design Description drawings to ensure that adequate overlap exists in the FAT. Comment documentation sheets are generated for each comment that needs to be addressed by AREVA NP due to apparent discrepancies. These comment documentation sheets are utilized to obtain AREVA NP's response to Duke's comments. If a significant deviation or discrepancy is identified, then Duke generates a Corrective Action Process document in the Oconee database or has AREVA NP generate a Corrective Action Program document in their database. After the comments are provided to AREVA NP, comment resolution meetings or conference calls are held to discuss the comments to ensure that the comments are understood by the AREVA NP test preparers. During these discussions, Duke and AREVA NP agree on how to resolve these comments. Satisfactory resolution of the comments is required before Duke provides formal approval of the FAT procedures.

Another design oversight mechanism in the engineering change process consists of the pre-implementation matrix. The pre-implementation matrix contains all of the items identified during the FMEA, Integrated Design Review, and Testing Open Items. All of the items in the pre-implementation matrix are evaluated to determine the impact on the RPS/ESPS. Each item must be satisfactorily addressed by the project team and approved by plant engineering prior to implementation of the modification. The verification matrix and pre-implementation matrix are under development at this time by the project team.

LAR Review Items- Questions on Software

General Questions

RAI 54

(a) What conventions are followed to identify requirements within:
(1) AREVA NP Inc. Office Instructions (OIs)
(2) Project-Specific Plans
(3) Software Requirements Specifications (SRSs)
(b) Where are these conventions documented?

These questions have been misunderstood in the past, and therefore clarification is provided in the form of a definition and examples.

Convention: *a: usage or custom*
b: a rule of conduct or behavior
c: an established technique, practice, or device

Examples: *ANSI/IEEE Std 829-1983: "The words shall, must and the imperative form identify the mandatory material within this standard. The words should and may identify optional material."*

IEEE Std 1219-1998: "The words shall and must identify the mandatory (essential) material within this standard. The words should and may identify optional (conditional) material."

ANSI/IEEE Std 1008-1987: "The word must and imperative verb forms identify the mandatory material within this standard. The words should and may identify optional material."

Duke Response to RAI 54

Response (a): AREVA NP identifies requirements by words that are imperative such as *shall* or *must* as cited in the question. The usage of shall is: "Used to indicate a requirement to be followed in order to conform to the standard and from which no deviation is permitted." The usage of *should* is: "A suggested practice that is not mandatory in programs intended to comply with a standard." These definitions and intended usage are provided in the standard AREVA NP PoPS (Policies and Procedures System) Dictionary, which is located on the AREVA NP Website. The source document which requires the word usage is the AREVA NP Administrative Procedure 1303-07, Control of Corporate Policies and Implementing Documents.

AREVA NP states conformance to specific IEEE Standards in the Oconee project documents. The AREVA NP conformance statements are, at times, qualified by documented deviation, nevertheless conformance is based on each standard's imperative requirements denoted by

the convention defined by the Standard for conformance such as in the examples provided in the question. For example, the statements in ANSI/IEEE Std 829-1983, *IEEE Standard for Software Test Documentation*:

> The words *shall*, *must* and the imperative form identify the mandatory material within this standard. The words *should* and *may* identify optional material.

Many later IEEE Standards define what conformance or compliance means with respect to the Standard such as this statement from IEEE 1012-1998, *IEEE Standard for Software Verification and Validation*:

> The word *shall* identifies mandatory requirements to claim conformance with this standard. The words *should* or *may* indicate optional tasks that are not required to claim conformance to this standard."

Therefore when AREVA NP claims conformance to a standard it is understood that the standard defines the applicable convention by use of specific words and the requirements associated with the words to claim conformance to the standard. This approach is appropriate to the use of Industry Standards applied to software development.

The identification of requirements for the purposes of tracking and tracing for the software life cycle process is not based solely on whether it is denoted by the imperative *shall* or *must*. There are times when a customer may identify a technical requirement using other terms but with the intention that it be applied equivalent to a *shall* or *must* statement. In addition there are several types of requirements that are not, by nature, technical that are commonly imposed by the customer. Therefore when identifying technical requirements for traceability in software development, whether they are from Operating Instructions (OIs), Project Specific Plans, or Software Requirements Specifications, AREVA NP follows a convention documented in the Operating Instruction OI-1591, *TXS System – Requirements Traceability Matrix*, which defines different requirement types as follows:

> Commercial Requirement: Requirements other than technical or quality assurance; such as cost, schedule, terms and conditions, number of copies, etc.
> Functional Requirement: A requirement that specifies a function that a system or system component must be able to perform.
> Process Requirements: Required tasks that when followed, produce a desired output.
> Quality Requirements: Required processes of evaluating overall project performance to provide confidence that the project will satisfy the relevant quality standards.
> Technical Requirements: The requirements that specify the desired functional or physical characteristics or capabilities of the product including, but not limited to, architecture, inputs, outputs, algorithms, logic, compliance with Codes and Standards, required tests, qualification and analyses.

For purposes of requirements traceability, the convention for identification of technical requirements is defined in OI-1591 as follows:

> Several different requirement types may exist in a document including commercial, quality, process and technical requirements. The RTM should trace technical requirements unless specified otherwise by the client."

Therefore AREVA does not use a word convention in requirements traceability but rather a functional convention as defined in the operating instruction. The functional convention includes Technical requirements in traceability but does not require that commercial, process, or quality requirements be included.

In an earlier version of OI-1591, which was in effect when the Oconee Unit 1 RTM was prepared, the following definition was provided for Requirement:

> A Requirement is the physical and functional capabilities that a system or component must provide. Requirements are derived directly from user needs and are stated in a contract, standard, specification, or other formally imposed document.
>
> The requirement may have specific attributes such as software, hardware, priority, qualification method, risk or others as assigned in the database. Requirements are listed individually under the associated package in ReqPro.

This version was applicable for the Oconee Unit 1 RTM development.

Response (b): The AREVA NP convention for identification of requirements is defined in documents noted in the response to part (a) above.

RAI 55
In defining the inputs for the software development effort, Duke produced:

1 *OSC-8623, "RPS & ESPS System Functional Description," also identified by AREVA NP Inc., Doc. No. 32-5061401-006.*

2 *OSC-8695, "Unit 1 Software Parameters for TXS Plant Protection System," also identified by AREVA NP Inc., Doc. No. 32-507267-002*

OSC-8623 requires that "Actual in-plant setpoints are listed in OSC-8695..." The RTM shows OSC-8695 as input to the SRS, which is an input to the Software Design Description (SDD); however, OSC-8695 could not have been created without using the SDD as an input; the SDD is listed as an input to OSC-8695.

Please describe the role and use of OSC-8695 in the software development process.

Duke Response to RAI 55

The original issue of Duke Energy calculation OSC-8695, *Unit 1 Software Parameters for TXS Plant Protection System*, was developed by Duke Energy based on revision 2 of the Software Design Description (AREVA NP document 51-5065423-002, *ONS Unit 1 RPS/ESFAS Controls Upgrade Software Design Description*). It is clear from the content of OSC-8695 that the specific software function blocks used in the Software Detailed Design were necessary for the calculation of the software parameters for the function blocks. OSC-8695 provides the calculated software parameters for the function blocks of the Software Design Description. OSC-8695 also utilizes data from other Duke Energy calculations as input data and basis for any assumed values.

The Requirements Traceability Matrix shows that OSC-8695 is linked to the Software Requirements Specification, not because it is an input to the SRS, but because some setpoints or other values provided in the Software Requirements Specification are also provided in OSC-8695. This link was added to alert the user to duplicative information by showing a relationship between the documents. As stated in OSC-8623, *RPS & ESPS System Functional Description*, the actual plant setpoints are provided in OSC-8695.

The Independent Verification and Validation group verified that the Software Detailed Design correctly implemented the software parameters specified in OSC-8695. This verification activity was documented in the verification and validation design phase summary report.

RAIs associated with Supplement 2

The following questions were identified during the review of Supplement 2 (ML081260167).

RAI 56
NUREG-0800 (SRP), Chapter 7, Branch Technical Position 7-14, Section B.3.1.1 contains acceptance criteria for Software Management Plans. Supplement 2 does not describe the documentation of the plan for software management.

Please provide a description of how the SRP acceptance criteria associated with the Software Management Plan (SMP) are addressed in the LAR and its supplements.

Duke Response to RAI 56

A review of the Standard Review Plan acceptance criteria associated with the Software Management Plan in SRP BTP 7-14 Section 3.1.1 indicates that the acceptance criteria include the following Management Characteristics - purpose, organization, oversight, responsibilities, and security. In addition, the acceptance criteria include the following Implementation Characteristics - measurements and procedures. The last portion of the

acceptance criteria includes the following Resource Characteristics - budget, methods/tools and personnel.

In order to ensure that the acceptance criteria for SRP BTP 7-14 Section 3.1.1 were satisfied, AREVA developed a suite of Operating Instructions that as a whole completely address the various characteristics of the acceptance criteria. The following information discusses the role of each Operating Instruction (OI).

AREVA OI-1456 "TELEPERM XS Project Phase" outlines the phases for a TELEPERM XS project. Each Phase is described including typical phase input, tasks, processes, and outputs and results.

AREVA OI-1457 "TELEPERM XS Software Quality Assurance Plan" provides the necessary measures to make sure that the developed Application Software conforms to established technical requirements, rules, and standards. This Plan describes the tools to be used and methodology to be followed in developing and maintaining software to be used for the design of TELEPERM XS Application Software.

AREVA OI-1578 "TELEPERM XS Software Safety Plan" outlines that the goal and objective of the Software Safety Plan is for achieving high functional reliability and design quality for the safety-critical Application Software. Planned and documented software safety analysis activities are to be used as factors to determine achievement of safety objectives to ensure that safety system software development is consistent with the defined system safety analyses. Software safety analysis activities are conducted during the Basic Design and Detailed Design Phases of the software development life cycle.

AREVA OI-1460, TELEPERM XS Software Configuration Management Plan, establishes the methods and tools used to identify and control the TXS Application Software developed for TELEPERM XS (TXS) projects. The content and structure of OI-1460 conforms with the guidance of Regulatory Guide 1.169 and IEEE Std 828-1990 and IEEE Std 1042-1987. OI-1460 applies to all software and related documentation for the design, modification, or testing of TXS Application Software developed for projects. In addition, OI-1460 applies to the Graphical Service Monitor Screen development. The plan is applicable from the Basic Design Phase to the completion of the Final Documentation Phase in the TXS Project Phases. At the completion of the Final Documentation Phase, Software Configuration Management is controlled by the Duke Energy software quality assurance plan. Also see the response to RAI 68 regarding configuration control boards.

AREVA OI-1577 "Processing Open Items" is a process for documenting potential discrepancies, improvements or anomalies that deviate from the required status or condition discovered during the phases of a TELEPERM XS Project as defined in OI-1456 TELEPERM XS Project Phase or during other ICS projects. The process for using the Open Items List applies at the beginning of the Project Startup Phase and continues through completion of the Final Documentation Phase. Each individual Open Item documents the discrepancy, improvement or anomaly from initial identification of the issue through final resolution and becomes a permanent record upon closure.

AREVA OI-1459 "TELEPERM XS Software Verification and Validation Plan" specifies activities to be performed during the software management and development processes that will demonstrate high levels of quality and confidence in the software being developed. The V&V activities are the reviews, inspections, analyses, and tests conducted by competent individual(s) or group(s) to provide the traceable documented evidence that a high level of quality and a low level of risk have been achieved. In addition to the OI, additional information on the Software V&V efforts has been included in Supplement 4 of the Oconee LAR.

AREVA OI-1591 "TXS System Requirements Traceability Matrix" provides guidance on the development of a project specific Requirements Traceability Matrix. A Requirements Traceability Matrix (RTM) provides a method for documenting and tracing project requirements throughout the life of a design project. Requirements tracing is performed to ensure that all requirements from the system requirements documents, including but not limited to the Functional Requirements Specification (FRS), are incorporated in the Software Requirements Specification (SRS), and the optional Hardware Requirements Specification (HRS), and implemented throughout the design, implementation, and testing activities. Use of a RTM provides documentation that the design addresses the software requirements in both forward and backward directions. It also can assist in the development of testing documentation by clearly defining areas requiring validation testing.

AREVA OI-1589 "TELEPERM XS Cyber Security" provides administrative controls and design feature requirements for maintaining cyber-security on all TELEPERM XS (TXS) projects in accordance with RG 1.152. Specifically, the methods described in this OI are aimed at maintaining access control (both physical and logical), developing security requirements with the customer, preventing undocumented code (e.g. back door coding), malicious code (e.g. intrusions, viruses, and worms), and installing and maintaining the TXS safety system. Additional information related to Cyber Security is contained in the Duke submittal dated January 30, 2008 related to the Oconee RPS/ESPS project.

Cyber Security is addressed in Duke submittal dated January 30, 2008 associated with the Oconee RPS/ESPS LAR.

RAI 57

NUREG-0800 (SRP), Chapter 7, Branch Technical Position 7-14, Section B.3.1.2 contains acceptance criteria for Software Development Plans. Supplement 2 does not describe the documentation of the plan for software development.

Please provide a description of how the SRP acceptance criteria associated with the Software Development Plan (SDP) are addressed in the LAR and its supplements.

Duke Response to RAI 57

A review of the Standard Review Plan acceptance criteria associated with the Software Development Plan in section 3.1.2 indicates that the acceptance criteria are addressed by

AREVA Operating Instruction OI-1456 "TELEPERM XS Project Phase". OI-1456 outlines the phases for a TELEPERM XS project. Each Phase is described including typical phase input, tasks, processes, and outputs and results.

For a TELEPERM XS project The Project Phases are:

- Elaboration of the Quotation
- Project Start-Up
- Basic Design
- Detailed Design
- Manufacturing
- Testing
- Installation
- Commissioning
- Final Documentation

The TXS Project Phases follow the life cycle planning guidance of IEEE Std. 1074, as endorsed by NRC Regulatory Guide 1.173.

RAIs associated with the Requirements Traceability Matrix (RTM)

A RTM is one effective way to assure that all requirements have been implemented. Oconee has used an RTM (AREVA NP Inc. Document No. 51-9062040-002) for this assurance. The following questions regarding the RTM were identified during the review process, and are based on the following three quotations from AREVA NP Inc. documents.

The Software Verification and Validation Plan (SVVP), AREVA NP Inc. Doc. No. 51-9010419-005, states:

Proprietary *[[(Section 5.2.1, page 28) "V&V shall trace software requirements between DUKE Energy ONS Project design documents and AREVA NP specification. The input data used for this V&V Task includes, but not limited to: ...Duke Energy's Software Parameters [OSC-8696] ..."]]*
(Section 5.2.1, page 29) "...each requirement shall be copied verbatim from its source into the SRM, when possible."]]

The Requirements Verification and Validation (V&V) Activity Summary Report, AREVA NP Inc. Doc. No. 51-9056720-001, states (Section 4.1.1.4, page 22):

Proprietary *[["3) Completeness: The SRM traces of the relationship between the SRSs and the System Requirements were found to be mostly complete. The trace teams resolved the incomplete traces discovered during the review process. Open items were issued if the correct traces could not be identified.*

The SRM ReqPro database was verified to be complete, except as identified by the Open Items delineated below."]]

RAI 58

Oconee Calculation OSC-8623, Rev. 5 (also called AREVA NP Inc., Doc. No 32-5061401-006), "RPS &ESFAS System Functional Description" states: "Actual in-plant setpoints are listed in OSC-8695..." The SVVP requires that the requirements from the software parameters document be traced in the software requirements traceability analysis, and that each requirement traced be cut and past into the RTM.

(a) The software parameters document (AREVA Doc No. 32-5072673-001) is referenced as a source of requirements in the Oconee RTM, but most of its requirements are not included in the RTM. Please explain why.

(b) Section 4.1.1.2 of Requirements Verification and Validation (V&V) Activity Summary Report, AREVA NP Inc. Doc. No. 51-9056720-001, does not identify that the software parameters document was used in the software requirements traceability analysis. Please explain why.

SDD Section 3.4 states: "The ONS Parameter Calculation OSC-8695 ... defines the necessary values for those parameters associated with plant specific design basis information."

(c) Please describe how it was verified, and documented, that these "actual in-plant setpoints" have been implemented in the RPS/ESPS system.

(d) Please identify the location in the LAR and associated documentation that demonstrates that these "actual in-plant setpoints" have been verified as being implemented in the design, or provide such documentation.

Duke Response to RAI 58

Response (a): The Oconee Software Parameters calculation OSC-8695, *Unit 1 Software Parameters for TXS Plant Protection System*, is incorporated into the AREVA NP record management system as AREVA NP document 32-5072673, *Oconee Nuclear Station Unit 1 Software Parameters for TXS Plant Protection System*. The observation is correct that Attachment 1 from OSC-8695 was not copied and pasted into the Requirements Traceability Matrix (RTM). The tool used for the RTM is Requisite Pro (an IBM product), which requires that a document be in Word[1] format to automatically load into the database. Duke Energy documents, such as OSC-8695, were provided by Duke Energy in pdf[2] file format and then converted into Word by AREVA NP using optical character recognition technology. Attachment 1 of OSC-8605 also contained numerous equations, calculations, and characters which did not convert intelligibly into a Word file. Therefore OSC-8695 is traced as a

---

1 Microsoft Office Word is a document authoring program included in the Microsoft Office system.

2 A file format used by Adobe Acrobat.

document but the individual parameters from Attachment 1 were not individually listed, as permitted by the Oconee Software Verification and Validation Plan Section 5.2.1, which states that:

> ...each requirement shall be copied verbatim from its source into the SRM, when possible.

The "when possible" qualifier was interpreted as allowing a place holder trace to the document as a reminder in the RTM tool of the link between OSC-8695 and other design documents.

Response (b): The original issue of Duke Energy calculation OSC-8695, *Unit 1 Software Parameters for TXS Plant Protection System*,[3] was developed by Duke Energy based on revision 2 of the Software Design Description (AREVA NP document 51-5065423-002, *ONS Unit 1 RPS/ESFAS Controls Upgrade Software Design Description*). It is clear from the content of OSC-8695 that the specific software function blocks used in the Software Detailed Design were necessary for the calculation of the software parameters for the function blocks. Therefore the development of the parameters in OSC-8695 occurred during the detailed design phase of the project, which followed the requirements phase activities. As a consequence, Section 4.1.1.2 of AREVA NP document 51-9056720-001, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Project Requirements V&V Activity Summary Report*, does not identify that the software parameters document was used in the software requirements traceability analysis.

Response (c): All setpoints in the Software Design Description (AREVA NP document 51-5065423-007, *ONS Unit 1 RPS/ESFAS Controls Upgrade Software Design Description*) were verified against revision 2 of Duke Energy calculation OSC-8695, *Unit 1 Software Parameters for TXS Plant Protection System*,[4] as described in AREVA NP document 51-5072680-004, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Project Design Phase V& V Activity Summary Report*.

The implementation of application code based on the design elements of the Software Design Description ensures that the actual in-plant setpoints have been implemented in the RPS/ESPS system application code. These requirements have been traced as a verification task as part of the implementation phase verification and validation activity, as documented in AREVA document 136-9086711-000, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Project Implementation Phase V&V Activity Summary Report*.

---

[3] The original issue of Duke Energy calculation OSC-8695 is available in the AREVA NP records management system as AREVA NP document 32-5072673-000, *Oconee Nuclear Station Unit 1 Software Parameters for TXS Plant Protection System*.

[4] Revision 2 of Duke Energy calculation OSC-8695 is available in the AREVA NP records management system as AREVA NP document 32-5072673-003, *Oconee Nuclear Station Unit 1 Software Parameters for TXS Plant Protection System*.

Response (d): Setpoints are discussed in Section 3.3.16.8 of the LAR. The associated setpoint documentation is referenced in that section. See the response to RAI 58 (c) for how the setpoints were verified in the design.

RAI 59
The Requirements V&V Activity Summary Report does not identify, as an open item, that "actual in-plant setpoints," identified in OSC-8695, are not incorporated into the Software Requirements Matrix (SRM); please explain why.

Duke Response to RAI 59

The original issue of Duke Energy calculation OSC-8695, *Unit 1 Software Parameters for TXS Plant Protection System*,[5] was developed by Duke Energy based on revision 2 of the Software Design Description (AREVA NP document 51-5065423-002, *ONS Unit 1 RPS/ESFAS Controls Upgrade Software Design Description*). The development of the parameters in OSC-8695 occurred during the detailed design phase of the project, which followed the requirements phase activities. As a consequence, Section 4.1.1.2 of AREVA NP document 51-9056720-001, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Project Requirements V&V Activity Summary Report*, does not identify that the software parameters document was used in the software requirements traceability analysis and, consequently, there was no open item issue for the requirements phase activity.

RAI 60
Many individual requirements (e.g., setpoint and parameter values from OSC-8695) are not copied verbatim into the RTM; please explain why.

Duke Response to RAI 60

The tool used for the Requirements Traceability Matrix (RTM) is Requisite Pro (an IBM product), which requires that a document be in Word[6] format to automatically load into the database. Duke Energy documents, such as OSC-8695, *Unit 1 Software Parameters for TXS Plant Protection System*, were provided by Duke Energy in pdf[7] file format and then converted into Word by AREVA NP using optical character recognition technology. Attachment 1 of OSC-8695 contained numerous equations, calculations, and characters which did not convert intelligibly into a Word file. Therefore OSC-8695 is traced as a document but the individual parameters from Attachment 1 were not individually listed, as permitted by the Oconee

---

5 The original issue of Duke Energy calculation OSC-8695 is available in the AREVA NP records management system as AREVA NP document 32-5072673-000, *Oconee Nuclear Station Unit 1 Software Parameters for TXS Plant Protection System*.

6 Microsoft Office Word is a document authoring program included in the Microsoft Office system.

7 A file format used by Adobe Acrobat.

Software Verification and Validation Plan Section 5.2.1, which states that:

> ...each requirement shall be copied verbatim from its source into the SRM, when possible.

The "when possible" qualifier was interpreted as allowing a place holder trace to the document as a reminder in the RTM tool of the link between OSC-8695 and other design documents.

RAI 61
Tracing of the Availability Requirement.

(a) The RTM contains one entry for the requirement in SRS Section 3.2.2, "Availability." The text of this requirement in the RTM is just the title of the section. The RTM traces this entry to SDD Section 5.0, "DESCRIPTION OF THE ATTACHMENTS;" however, SDD Section 5.0 does not contain information specific to the implementation of this requirement. Please explain why.

(b) Please provide an explanation of the traces to inappropriate sections and how this was addressed by V&V.

Duke Response to RAI 61

Response (a): As a point of clarification, there is not a trace in the Requirements Traceability Matrix (RTM) from Software Requirement Specification (SRS) item 3.23.2 to the Software Design Description (SDD) Section 5.0, *Description of the Attachments*. The SDD is a combination of inputs from Word[8] and FunBase.[9] The Word portions of the SDD are text descriptions and can be imported into the RTM. The information in FunBase cannot be imported. Consequently, the SDD has been entered into the RTM by listing sections; however the RTM reference does not correlate to SDD paragraph numbers. RTM SDD5.0 should not be interpreted as SDD paragraph 5.0; it is a reference number that is assigned by Requisite Pro. There are no traces from SRS 3.23.2 to the SDD, since this is a general requirement of the system's availability to perform its function. The availability requirement will be demonstrated by a system availability test that has not been issued.

Response (b): As noted in the response to part (a) above, RTM SDD5.0 should not be interpreted as SDD paragraph 5.0. It is assumed that the question about inappropriate traces is based on an assumption that SDD5.0 meant SDD paragraph 5.0.

---

[8] Microsoft Office Word is a document authoring program included in the Microsoft Office system.

[9] FunBase is a TELEPERM XS tool used to administrate the naming of software modules, parameters, signals, data tables and other entities in the specification or design so that each entity is uniquely and consistently named and properly connected in the application software.

RAI 62

The RTM contains one entry for all of the requirements in SRS Section 3.2.3, "Security and Access Control." The text of this requirement in the RTM is just the title of the section. The RTM traces this entry to SDD Section 4.2, "RPS Trip #2;" however, SDD Section 4.2 is empty (i.e., "reserved for future use").

Please explain how the Security and Access Control requirements are documented in and traced to the SDD?

Duke Response to RAI 62

An important context for the answer to this question is that the original Requirements Traceability Matrix (RTM) for the Oconee RPS/ESFAS replacement project was developed using an Access database tool.[10] As revisions to specification and design documents were made, the links in the Access database had to be reestablished. It was decided in 2007 to migrate the RTM to the Requisite Pro tool (an IBM product). Therefore, the revised RTM was developed at a time when the input and output documents existed and had been incorporated into the Requisite Pro tool.

The Software Design Description (SDD) document is a combination from Word[11] and FunBase.[12] The Word portions of the SDD are text descriptions and can be imported into the RTM but the FunBase, the actual code description details, cannot be imported. Consequently, the SDD has been entered into the RTM by listing sections; however the RTM reference does not correlate to SDD paragraph numbers. This affected the level at which the tracing from the Software Requirements Specification (SRS) to SDD was accomplished. The tracing from SRS 3.23.3 was performed at the section level which traces to SDD4.2. The SRS subsections were not individually traced since the subsection information in SRS 3.23.3.1 through 3.23.18 all trace to SDD4.2 and other documents. The RTM trace to SDD4.2 points to SDD module SM-0902 (Attachment 4-2) which is the SDD module for the TELEPERM XS Runtime Environment (RTE) Parameter Change Enable function. Note that all requirements in the SRS subsections 3.23.3.1 through 2.23.3.18 pertain to the RTE Parameter Change Enable function for software or the hardware related keyswitch which is not a software requirement.

---

10 Microsoft Office Access is a database management program included in the Microsoft Office system.

11 Microsoft Office Word is a document authoring program included in the Microsoft Office system.

12 FunBase is a TELEPERM XS tool used to administrate the naming of software modules, parameters, signals, data tables and other entities in the specification or design so that each entity is uniquely and consistently named and properly connected in the application software.

RAIs associated with the Software Requirements Specification (SRS)

The following questions are a result of reviewing the Software Requirements Specification (SRS) -- "Oconee Nuclear Station, Unit 1 RPS ESFAS Controls Upgrade Software Requirements Specification," AREVA NP Inc. Doc. No. 51-9054435-002.

RAI 63

The SRS states (Section 2.6, page 46):

Proprietary *[["All setpoint and parameter values are considered preliminary. Setpoint and parameter values will be established by the unit specific software parameter calculation. COLR values will be established by the COLR calculation every cycle and will not be necessary for the design of the Application Software."]]*

(a) What document (i.e., what Title & Document No.) will contain the final setpoint and parameter values?

(b) How will it be verified and validated that the final setpoint and parameter values are properly implemented in the RPS/ESPS system installed at site?

(c) When will the final setpoint and parameter values be input into the deliverable system and associated documentation?

(d) Please describe the relationship between the core operating limits report (COLR) calculations, COLR values, and the software parameters document.

Duke Response to RAI 63

Response (a): Duke Energy calculation OSC-8695, *Unit 1 Software Parameters for TXS Plant Protection System*, will contain the final setpoint and parameter values for the installed system. Additionally, the final Software Design Document (AREVA NP document 51-5065423, *ONS Unit 1 RPS/ESFAS Controls Upgrade Software Design Description*) delivered to the plant will reflect the parameter values in the Duke calculation. These parameters have been designed as changeable parameters in the application software to allow Duke to modify the setpoints, Core Operating Limits Report values, and other parameters, as needed. This flexibility meets the requirements set forth in the Duke System Functional Description OSC-8623, *RPS & ESPS System Functional Description.*

Response (b) and (c)

As noted in the Software Parameters Calculation, some software parameters are cycle specific and will be controlled by station procedures. The Oconee RPS/ESPS has been designed based on the current version of the SDD, which is based on Revision 2 of the Software Parameters Calculation. The setpoints and parameters in Revision 2 of the parameters calculation have been input into the Oconee RPS/ESPS system that is undergoing Factory Acceptance Testing.

Once Factory Acceptance Testing is completed and the equipment is sent to Oconee, the equipment will be setup at Oconee and the draft station procedures will be validated on the system. As part of this validation, the installation of up to date software parameters and setpoints will occur. The station procedures that will control the setpoints and parameters are in the development phase and are not scheduled for completion until the summer of 2009.

The final verification of the correct installation of the final setpoints and parameter values will occur during installation and functional testing of the RPS/ESPS at Oconee. The installation and functional testing procedures are being developed at this time. It is expected that the installation and functional testing will consist of a mixture of the station maintenance procedures and functional test procedures in order to ensure proper setpoint and parameters installation.

Response (d)

The Core Operating Limits Report (COLR) is developed in accordance with the program contained in Technical Specification 5.6.5. The COLR establishes the following operating cycle values:

1. Shutdown Margin limit for Specification 3.1.1;
2. Moderator Temperature Coefficient limit for Specification 3.1.3;
3. Physical Position, Sequence and Overlap limits for Specification 3.2.1 Rod Insertion Limits;
4. AXIAL POWER IMBALANCE operating limits for Specification 3.2.2;
5. QUADRANT POWER TILT (QPT) limits for Specification 3.2.3;
6. Nuclear Overpower Flux/Flow/Imbalance and RCS Variable Low Pressure allowable value limits for Specification 3.3.1;
7. RCS Pressure, Temperature, and Flow Departure from Nucleate Boiling (DNB) Limits for Specification 3.4.1
8. Core Flood Tanks Boron concentration limits for Specification 3.5.1;
9. Borated Water Storage Tank Boron concentration limits for Specification 3.5.4;
10. Spent Fuel Pool Boron concentration limits for Specification 3.7.12;
11. RCS and Transfer Canal boron concentration limits for Specification 3.9.1; and
12. AXIAL POWER IMBALANCE protective limits and RCS Variable Low Pressure protective limits for Specification 2.1.1.

Of the limits determined by the COLR, only the Nuclear Overpower Flux/Flow/Imbalance and RCS Variable Low Pressure allowable values, which are listed in Table 3.3.1-1 of the Oconee Technical Specifications, are impacted by the Software Parameters Calculation. The analytical methods used to determine the core operating limits have been previously reviewed and approved by the NRC. The specific methods are outlined in Oconee Technical Specification 5.6.5. The core operating limits are determined such that all applicable limits (e.g., fuel thermal mechanical limits, core thermal hydraulic limits, Emergency Core Cooling System (ECCS) limits, nuclear limits such as SDM, transient analysis limits, and accident analysis limits) of the safety analysis are met.

The Software Parameters Calculation identifies the software function block parameters utilized in the digital Reactor Protective System (RPS) and the Engineered Safeguards Feature Actuation System (ESFAS) that are associated with plant specific design based information. In order for the TXS software to operate correctly, function blocks are assigned specific numerical and alphanumerical values called parameters. The Software Parameters Calculation identifies the necessary parameters for the new ESPS and RPS software function blocks associated with plant specific design basis information. The Software Parameters Calculation does not provide an exhaustive list of ESPS and RPS function block parameters. A full list of RPS/ESFAS function blocks and their associated parameter settings is provided in the Software Design Description (SDD).

The values determined in the COLR for the Nuclear Overpower Flux/Flow/Imbalance and RCS Variable Low Pressure are included in the Software Parameters Calculation in the associated trip function sections. The Nuclear Overpower Flux/Flow/Imbalance trip is FU-0003 in the parameters calculation. The RCS Variable Low Pressure trip is FU-0006 in the parameters calculation.

The correct parameter values for the Nuclear Overpower Flux/Flow/Imbalance and RCS Variable Low Pressure trips are loaded into the TXS system each cycle by performance of a station procedure. The values in the Software Parameters Calculation are based on ONS 1 Cycle 24, which is the current ONS operating cycle. The Software Parameters Calculation specifies that it does not need to be updated with changed COLR values each cycle because the values are administratively controlled by station procedures. The utilization of station procedures to administratively control COLR values for Nuclear Overpower Flux/Flow/Imbalance and RCS Variable Low Pressure trips is consistent with the work processes for the existing analog RPS.

RAI 64

The SRS states (Section 1.2, page 20):

Proprietary *[["The TXS Gateway software, MSI and the RPS E functions Application Software…shall be developed and maintained at the same level as the safety related software."]]*

(a) Please explain what "developed and maintained at the same level" means. That is, does it mean that this software is developed and maintained by including the same design features, and following the same analytical techniques, and procedural measures as for safety related software?

(b) Does it mean that this software will be traced with the same RTM methodology?

The SVVP (AREVA Doc No. 51-9010419-005) states (Section 4.6.6.2, page 24):

Proprietary *[["the functionality of [TXS Gateway software] is verified via line-by-line code review"]]*

The NRC noted that it is not an accepted practice to credit "line-by-line code review" instead of software functional testing of safety–related software; therefore, TXS Gateway software does not seem to be treated as safety related as required by the SRS.

(c) Please explain the apparent conflict between these two proprietary quotations.

Duke Response to RAI 64

Response (a): TELEPERM XS (TXS) Gateway Application Software is classified as non-safety related. TXS Gateway Application Software is developed and generated with the SPACE tool. The TXS Gateway Application Software is installed onto non-safety related equipment and does not perform any safety related functions. The TXS Gateway Application Software does not have any ability to create an adverse affect on the safety related system, since the TXS Gateway is isolated from the TXS safety processors by the NetOptics device. The TXS Gateway Application Software is classified as SIL-2 because it does not perform safety function and it is isolated from the Oconee TXS RPS/ESPS system by the NetOptics device.

TXS Monitoring and Service Interface (MSI) computers are classified as safety-related. The TXS MSI computers perform the safety function of providing communication independence between the TXS safety function processors and non-safety computers. The Channel E software is classified as SIL-4 because it performs a safety function and runs on a TXS safety processor platform.

The functions on Reactor Protection System (RPS) Channel E are classified as non-safety related. This software runs on a TXS safety processor in a separate channel that is physically separate and electrically isolated, with full TELEPERM XS communication independence, from the other RPS and Engineered Safety Feature channels. The RPS Channel E data links are only connected to the MSI and the Channel E and no data are exchanged with the safety function processors. The Channel E application software is developed with the SPACE tools and is developed and maintained at the same level as the safety related (QA1) software. RPS Channel E, RPS and ESFAS Miscellaneous functions do not perform any safety-related functions; however, the Channel E software is classified as SIL-4 because it runs on a TXS safety processor platform. The Channel E software cannot have an adverse effect on other safety related functions because of the physical separation, electrical isolation, and communication independence features of the Oconee RPS/ESPS design.

Also see the response to RAI 65 (a).

Response (b): The MSI, RPS Channel E, and the TXS Gateway application software are all traced with the RTM.

Response (c): AREVA NP does not see any conflicts between two proprietary quotations. The line-by-line code review is a separate activity from the software functional testing. Code review is part of the software code verification task that is performed as part of the implementation phase verification and validation activity. Software functional testing is a validation task performed as part of the test phase verification and validation activity for the Oconee RPS/ESPS system. AREVA NP document 51-9010419-007, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Software Verification and Validation Plan*, does not state that the line-by-line code review can be credited for the software functional testing. Code review and software testing can be complementary to each other; however, one cannot replace the other.

RAI 65

The SRS contains the following two requirements (see statements containing the verb "shall") that do not appear to be in the Software Design Description (SDD); the SRS states (Section 1.2):

Proprietary *[["All Application Software defined within this document, except for the TXS Gateway, MSI, and RPS E functions Application Software, is considered Safety Related and shall be developed to satisfy the requirements contained in...The TXS Gateway software, MSI, and the RPS E functions are classified non-safety, but they shall be developed and maintained at the same level as the safety related software."]]*

The Software Verification and Validation Plan (SVVP), AREVA NP Inc., Doc. No. 51-9010419-005, states (Section 5.2.1, page 29):

Proprietary *[["each requirement shall be copied verbatim from its source into the SRM"]]*

(a) The text of the two requirements above are not included in the SRM portion of the RTM (51-9062040-002, "Oconee Nuclear Station, Unit 1 RPS ESFAS Controls Upgrade Requirements Traceability Matrix Report"); please explain why.

The RTM depicts (See attachment F, page 2) that the requirements of the SRS are traced to the SDD.

(b) How are the two SRS requirements, quoted above, implemented within the SDD?

Duke Response to RAI 65

Response (a): AREVA NP will revise the Software Requirements Specification to clarify the treatment of the software for the TELEPERM XS (TXS) Gateway software, Monitoring and Service Interface (MSI), and the Reactor Protection System (RPS) Channel E functions. The clarification will reflect the following facts summarized in the Table below:

	MSI	RPS-E	TXS Gateway
Classification	Safety-related (i.e., 1E communication independence); however, Duke Energy power feed to cabinet is non-1E. MSI can perform safety function (i.e., prevents adverse impacts) with loss of power.	Performs non-safety functions; however, functions are located on a safety processor. Software is classified as safety-related for everything but functionality.	Does not perform a safety-related function but code was generated using SPACE.
Design Process Controls and Documents	Is treated and classified as safety-related.	Is treated and classified as safety-related.	Is treated and classified as non-safety related.
V&V	Classified as SIL-4	Classified as SIL-4	Classified as SIL-2
RTM	No difference between SIL-4 and SIL-2 in Oconee SVVP for requirements tracing in the RTM.		

The text of the two cited requirements will be changed. The current text is not now included in the software requirements portion of the Requirements Traceability Matrix (RTM). However, the TXS Gateway software, MSI, and the RPS Channel E functions are addressed in the RTM. The two cited requirements were not included in the RTM because they are relevant to the design process and to the resulting design documents rather than to specific technical and functional requirements. The RTM traces technical requirements, as described in the response to RAI 54.

Response (b): See response to RAI 64 for information on the MSI, RPS Channel E, and the TXS Gateway application software.

As for the implementation in the SDD, Section 1 of the SDD states as follows:

> The Application Software, except for the Non-Safety Related TXS Gateway Application Software, is classified as SIL-4, Nuclear Safety Related, QA Condition 1.

The SDD is marked as safety related and the task descriptions in each attachment of the SDD indicate the safety related status of software logic contained in the attachment. Additionally, the SDD submodule SM-0100 "Gateway", Attachment 4-2 of the SDD, marks which parts of the submodule are non-safety related for the TXS Gateway application software.

RAIs associated with the Verification and Validation (V&V)

The following questions are a result of reviewing the Software Verification and Validation Plan (SVVP), AREVA NP Inc., Doc. No. 51-9010419-005, and the Requirements Verification and Validation (V&V) Activity Summary Report, AREVA NP Inc., Doc. No. 51-9056720-001

RAI 66
RG 1.172 requires that: "[An SRS must be Correct, Unambiguous, Complete, Consistent, Ranked for importance and/or stability, verifiable, modifiable, and traceable.]"

The SVVP does not require that the software requirements are evaluated against the RG 1.172 criteria; the SVVP states (Section 5.2.1, page 29, Task No. 2):

Proprietary *[["Independent V&V shall evaluate all AREVA NP SRSs for correctness, consistency, completeness, accuracy, readability, and testability."]]*

Please provide an evaluation of how the criteria used by V&V provides an acceptable method of complying with the regulations addressed by RG 1.172.

Duke Response to RAI 66

The AREVA NP independent Verification and Validation group used IEEE Std 1012-1998, *IEEE Standard for Software Verification and Validation*, as endorsed by NRC Regulatory Guide 1.168, *Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, Revision 1, as its guiding document. AREVA NP document 51-9010419-007, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Software Verification and Validation Plan*, specifies that the independent Verification and Validation group shall evaluate all Software Requirement Specifications (SRS) for correctness, consistency, completeness, accuracy, readability, and testability as these terms are defined in IEEE Std 1012-1998, Table 1, Section 5.4.2.

Table 66-1 shows that the requirements spelled out in IEEE Std 1012-1998 match the requirements for Regulatory Guide 1.172, *Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, except for: item 2.4, *Ranking for Importance or Stability*.

The table also shows that the SRS does clarify what parts of the TELEPERM XS (TXS) System that are included in the Software Requirements Specification are not safety related. AREVA NP will revise the SRS as described in the response to RAI 65(a) to clarify the treatment of non-safety software.

NRC Regulatory Guide 1.172	IEEE Std 1012-1998
2.1 Traceability and Accuracy When specification or representation tools are used for requirements, as described in sections 4.3.2.2 and 4.3.2.3 of IEEE Std 830-1993, traceability should be maintained between these representations and the natural language descriptions of the software requirements that are derived from system requirements and system safety analyses.	**5.4.2 Requirements V&V Activity (development process)** **(1) Traceability Analysis.** Trace the software requirements (SRS and IRS) to system requirements (Concept Documentation), and system requirements to the software requirements. Analyze identified relationships for correctness, consistency, completeness, and accuracy. The task criteria are as follows: (1.1) Correctness a. Validate that the relationships between each software requirement and its system requirement are correct. (1.2) Consistency a. Verify that the relationships between the software and system requirements are specified to a consistent level of detail. (1.3) Completeness a. Verify that every software requirement is traceable to a system requirement with sufficient detail to show compliance with the system requirement. b. Verify that all system requirements related to software are traceable to software requirements. **(1.4) Accuracy** a. Validate that the system performance and operating characteristics are accurately specified by the traced software requirements.

NRC Regulatory Guide 1.172	IEEE Std 1012-1998
2.2 Completeness For safety system software, the description of functional requirements should specify how functions are initiated and terminated as well as the system status at termination. Accuracy requirements, including units, error bounds, data type, and data size, should be provided for each input and output variable. Variables controlled or monitored in the physical environment should be fully described. Functions expressly prohibited should also be described. Timing information is particularly important in specifying software requirements for safety system software. Functions with timing constraints should be identified and criteria for each mode of operation should be provided. Timing requirements should be deterministic and specified for both normal and anticipated failure conditions.	**(2) Software Requirements Evaluation.** Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the SRS and IRS for correctness, consistency, completeness, accuracy, readability, and testability. **(2.3) Completeness** a. Verify that the following elements are in the SRS or IRS, within the assumptions and constraints of the system: 1. Functionality (e.g., algorithms, state/mode definitions, input/output validation, exception handling, reporting, and logging); 2. Process definition and scheduling; 3. Hardware, software, and user interface descriptions. 4. Performance criteria (e.g., timing sizing, speed, capacity, accuracy, precision, safety, and security); 5. Critical configuration data; and 6. System, device, and software control (e.g., initialization, transaction and state monitoring, and self-testing). b. Verify that the SRS and IRS satisfy specified configuration management procedures.

NRC Regulatory Guide 1.172	IEEE Std 1012-1998
2.3 Consistency IEEE Std 830-1993 restricts the term to mean internal consistency, noting that an external inconsistency is actually an incorrect specification of a requirement. The term is used in this regulatory guide to mean both internal and external consistency. External consistency implies that the SRS is consistent with associated software products and system products, such as safety system requirements and design. Internal consistency means that no requirement in the requirements specification conflicts with any other requirement in the specification.	**(2) Software Requirements Evaluation.** Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the SRS and IRS for correctness, consistency, completeness, accuracy, readability, and testability. **(2.2) Consistency** a. Verify that all terms and concepts are documented consistently. b. Verify that the function interactions and assumptions are consistent and satisfy system requirements and acquisition needs. c. Verify that there is **internal consistency** between the software requirements and **external consistency** with the system requirements.
2.4 **Ranking for Importance or Stability** For safety system software, this characteristic means that software requirements important to safety must be identified as such in the SRS. Criterion 20 of Appendix A, among others, describes the functions that reactor protection systems must perform. Section 4.3.5.2 of IEEE Std 830-1993 suggests three degrees of necessity of requirement: *essential, conditional,* and *optional.* As used in IEEE Std 830-1993, the terms conditional and optional refer to requirements that are not necessary for the software to be acceptable. For safety system software, unnecessary requirements should not be imposed. There may be documented variations in essential requirements, but the variations must be linked in the software requirements specifications either to site	There are no IEEE Std. 1012-1998 requirements for ranking for importance or stability. **However**, the revision 2 of the SRS states in its scope: *"This SRS does not define the requirements for the TXS System Software running on TXS processors or the TXS Service Unit software and utilities (e.g., Graphic Service Monitor (GSM)). All Application Software defined within this document, except for the TXS Gateway, MSI, and RPS E functions Application Software, is considered Safety Related and shall be developed to satisfy the requirements contained in References /22/ through /24/. The TXS Gateway software, MSI, and the RPS E functions are classified non-safety, but they shall be developed and maintained at the same*

NRC Regulatory Guide 1.172	IEEE Std 1012-1998
and equipment variations or to specific plant design bases and regulatory provisions.	*level as the safety related software."* *NOTE: AREVA is committed to a revision of the SRS to clarify the treatment of TXS Gateway, RPS Channel E and MSI software. This revision is described in Response to RAI 65 (a).* AND: This SRS follows IEEE 830 (Reference /17/) with the exceptions noted below: • Each requirement listed in this SRS does not reference its source document for traceability; requirements can be traced using the Software Requirements Matrix (SRM). Additionally, all source documents are listed in the Reference section • This SRS organized the requirements primarily by function.
2.5 Verifiability IEEE Std 830-1993 recommends the removal or revision of unverifiable requirements. This is clarified to mean that all requirements should be verifiable and should be modified or restated as necessary so that it is possible to verify each one.	**(2) Software Requirements Evaluation.** Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the SRS and IRS for correctness, consistency, completeness, accuracy, readability, and testability. (2.1) Correctness a. Verify and validate that the software requirements satisfy the system requirements allocated to software within the assumptions and constraints of the system.
2.6 Modifiability This term is closely related to the style (form, structure, and modularity), readability, and understandability of the SRS. With respect to these characteristics, it is important that precise definitions of technical terms be available, either in the	**(2) Software Requirements Evaluation.** Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the SRS and IRS for correctness, consistency, completeness,

NRC Regulatory Guide 1.172	IEEE Std 1012-1998
SRS or in a glossary.	accuracy, readability, and testability. (2.5) Readability a. Verify that the documentation is legible, understandable, and unambiguous to the intended audience. b. Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, and symbols.
2.7 Traceability Section 4.3.8 of IEEE Std 830-1993 describes two types of traceability, and both types are required. Each identifiable requirement in an SRS must be traceable backwards to the system requirements and the design bases or regulatory requirements that it satisfies. Each identifiable requirement should be written so that it is also "forward traceable" to subsequent design outputs, e.g., from SRS to software design and from software design to SRS. Forward traceability to all documents spawned by the SRS includes verification and validation materials. For example, a forward trace should exist from each requirement in the SRS to the specific inspections, analyses, or tests used to confirm that the requirement has been met.	**5.4.2 Requirements V&V Activity (development process)** **(1) Traceability Analysis.** Trace the software requirements (SRS and IRS) to system requirements (Concept Documentation), and system requirements to the software requirements. Analyze identified relationships for correctness, consistency, completeness, and accuracy. The task criteria are as follows: (1.1) Correctness a. Validate that the relationships between each software requirement and its system requirement are correct. (1.2) Consistency a. Verify that the relationships between the software and system requirements are specified to a consistent level of detail. (1.3) Completeness a. Verify that every software requirement is traceable to a system requirement with sufficient detail to show compliance with the system requirement. b. Verify that all system requirements related to software are traceable to software requirements.

RAI 67

The SVVP requires that the requirements in SRS (51-9054435-002) be evaluated for testability; the SVVP states (Section 5.2.1, Task 2, page 29):

Proprietary ***[[****"Independent V&V shall evaluate all AREVA NP SRSs for ... testability."****]]***

The Requirements V&V Activity Summary Report documents the testability evaluation performed by V&V and concludes that the requirements are testable, and does not include any open items for requirements that are not testable. The Requirements V&V Activity Summary Report states (Section 4.1.1.4, page 31):

Proprietary ***[[****"6) Testability: As appropriate to a requirements document, the SRS contains objective acceptance criteria required for testability. The SRS structure lends itself well to application of test procedures and expected results.****]]***

In contrast to the quotations above, the SRS (51-9054435-002) contains requirements that are not testable, as demonstrated by the three examples below:

Proprietary ***[[****(Section 1.2, page 20): "All Application Software defined within this document, except for the TXS Gateway, MSI, and RPS E functions Application Software, is considered Safety Related and shall be developed to satisfy the requirements contained in ... The TXS Gateway software, MSI, and the RPS E functions are classified non-safety, but they shall be developed and maintained at the same level as the safety related software."*

(Section 2.1.1, page 32): "For each TXS processor, an executable file shall be generated that implements the Application Software safety functions to be performed by that processor."

*(Section 2.3, page 44) "The primary users of the RPS/ESFAS TXS System shall be qualified Engineering, Operations, Maintenance, System Administrators, and Training personnel at the Oconee Nuclear Power Station. Users will interface with the Application Software indirectly such as through the GSM or OAC. All classes of users shall be trained and qualified to perform their duties without imposing additional constraints on the Application Software. A Human Factors review may identify user constraints, which will be incorporated into the detailed design of the Application Software."****]]***

Please explain the testability conclusion in the Requirements V&V Activity Summary Report in light of the fact that the SRS contains requirements that are not testable.

Duke Response to RAI 67

IEEE Std 830-1993, Recommended Practice for Software Requirements Specifications, defines the appropriate attributes of a software requirements specification:

> 4.3 Characteristics of a good SRS
>
> An SRS should be
>
> a) Correct;
> b) Unambiguous;
> c) Complete;
> d) Consistent;
> e) Ranked for importance and/or stability;
> f) Verifiable;
> g) Modifiable;
> h) Traceable.

The description of verifiable states:

> An SRS is verifiable if, and only if, every requirement stated therein is verifiable. A requirement is verifiable if, and only if, there exists some finite cost-effective process with which a person or machine can check that the software product meets the requirement. In general any ambiguous requirement is not verifiable.

It is clear that all requirements in the SRS need not be testable but shall be verifiable by test, inspection, checking, or by other cost-effective means by a machine or individual.

IEEE Std 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology, defines testability as follows:

> **testability.** (1) The degree to which a system or component facilitates the establishment of test criteria and the performance of tests to determine whether those criteria have been met.
> (2) The degree to which a requirement is stated in terms that permit establishment of test criteria and performance of tests to determine whether those criteria have been met.

The types of testing and test objectives for verification and validation purposes are defined in IEEE Std 1012-1998, IEEE Standard for Software Verification and Validation, as follows:

> **3.1.1 Acceptance testing**: Testing conducted in an operational environment to determine whether a system satisfies its acceptance criteria (i.e., initial

requirements and current needs of its user) and to enable the customer to determine whether to accept the system.

3.1.10 integration testing: An orderly progression of testing of incremental pieces of the software program in which software elements, hardware elements, or both are combined and tested until the entire system has been integrated to show compliance with the program design, and capabilities and requirements of the system.

3.1.26 system testing: The activities of testing an integrated hardware and software system to verify and validate whether the system meets its original objectives.

3.1.27 test case: Documentation that specifies inputs, predicted results, and a set of execution conditions for a test item.

Therefore it is recognized that it is acceptable that the SRS contains requirements that are not testable but are nevertheless consistent with the requirements of IEEE Std 830-1993 that they be verifiable. The term testability from IEEE Std 610.12-1990 means that requirements must be stated such that they permit testing and the establishment of criteria that prove requirements are met. The test types defined in IEEE Std 1012-1998 indicate that testing will be conducted to demonstrate and show that the functional requirements and specified performance characteristics are met. Therefore IEEE Standard 1012-1998 requires verification that there are sufficient requirements that can be tested to demonstrate that the system performs the expected functional requirements.

The conclusion in AREVA NP document 51-9056720-001, *Oconee Nuclear Station* Unit 1 *RPS/ESFAS Controls Upgrade Project Requirements V&V Activity Summary Report*, for testability was that there are sufficient performance and functional requirements to support testing that will confirm that the requirements are met. This conclusion was based on the content of the Software Requirements Specification (SRS) and the specificity of the requirements. The SRS contains documented testing and performance requirements for each safety function (i.e., reactor trip function and engineered safety feature actuation function). It also contains sections for general system performance requirements and regulatory performance requirements. These characteristics support the conclusion of the Requirements Phase V&V Activity Report.

RAIs associated with the Software Configuration Management Plan (SCMP) Questions

The following questions are a result of reviewing the Software Configuration Management Plan (SCMP) – AREVA NP Inc Document No. 51-90064444-005.

RAI 68

The SCMP states that the guidance of Regulatory Guide 1.169, "Configuration Management Plans for Digital Software Used in Safety Systems of Nuclear Power Plants," is followed (Section 1.1, page 15):

Proprietary *[["The SCMP follows the guidance of Regulatory Guide 1.169...IEEE Std 828-1990...and ANSI/IEEE Std 1042-1987..."]]*

In a conference call, Oconee stated that the phrase "follows the guidance of" should not be understood to mean that the actions in the guidance document were done, "[because there is no requirement to do the things described in a guidance document]"; therefore this quotation is ambiguous in that it is not clear what is done. Oconee also stated that the term "conforms to" is used when all guidance is done.

Does the SCMP conform to Regulatory Guide 1.169 (i.e., is all of the guidance done)? If not, please clarify what alternative actions have been taken and explain how this is equivalent to the applicable RG 1.169 criteria.

Duke Response to RAI 68

The Software Configuration Management Plan conforms to 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*, as endorsed in Regulatory Guide 1.169, *Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*, with the exception of the use of a configuration control board meetings.

AREVA NP does not use Configuration Control Board meetings for the development of TELEPERM XS (TXS) application software; however, the overall AREVA NP approach to configuration management of the TXS platform, TXS projects, and the project-specific application software meets the intent of IEEE Std 828-1990 and IEEE Std 1042-1987.

NRC Regulatory Guide 1.169 endorses IEEE Std 828-1990 and IEEE Std 1042-1987. The Regulatory Guide does not mention configuration control boards or elaborate or interpret the guidance in the endorsed IEEE standards.

AREVA NP interpreted IEEE Std 828-1990 to specify requirements for a configuration control board, if one is used. Specifically, clause 2.2.2 states that

> For any review board or special organization established for performing SCM activities on this project, the Plan shall describe its ... (responsibilities listed).

Similarly, clause 2.3.2.3 states that:

> The Plan shall identify each configuration control board (CCB) and its level of authority for approving proposed changes. A CCB may be an individual or a group. Multiple levels of CCBs may be specified, depending upon the degree of system or project complexity and upon the project baseline involved. When multiple CCBs are used, the Plan shall specify how the proper level is determined for a change request, including any variations during the project life cycle.
>
> For any CCB utilized, the Plan shall indicate its level of authority and its responsibilities as defined in 2.2.2.

And, finally, clause 2.3.5 states that:

> For any CCB established to control interfaces, the Plan shall identify its responsibilities and procedures as specified in 2.2.2.

IEEE Std 1042-1987 provides insight as to the underlying purpose of configuration control boards in clause 2.3.3.

> Another functional concept of SCM is the extended use of configuration control boards (CCB). This concept provides for implementing change controls at optimum levels of authority. Configuration control boards can exist in a hierarchical fashion (for example, at the program, system design. and program product level. or one such board may be constituted with authority over all levels of the change process. In most projects, the CCB is composed of senior level managers. They include representatives from the major software, hardware, test, engineering, and support organizations. The purpose of the CCB is to control major issues such as schedule, function, and configuration of the system as a whole.
>
> The more technical issues that do not relate to performance, cost, schedule, etc, are often assigned to a software configuration control board (SCCB). The SCCB discusses issues related to specific schedules for partial functions, interim delivery dates, common data structures, design changes, and the like. This is the place for decision-making concerning the items that must be coordinated across CI but which do not require the attention of high level management. The SCCB members should be technically well-versed in the details of their area; the CCB members are more concerned with broad management issues facing the project as a whole and with customer issues.

Based on the discussion in IEEE Std 1042-1987, the high-level Configuration Control Board is not directly applicable to TXS projects. Instead, the software-related decisions contemplated at this level are handled generically for the TXS platform. The TXS platform configuration management process utilizes a Configuration Control Board.

TXS projects are built using the qualified TXS platform, which is a fully integrated suite of hardware and software designed specifically for nuclear safety applications. Application software for TXS projects is developed using the SPACE tool using qualified hardware and software modules. This tool is used to develop Function Diagrams and Network Diagrams. Function Diagrams specify the signal processing requirements for the system. Network Diagrams define the hardware components of the system and their logical interconnections. Application software code is automatically generated from the Function Diagrams and Network Diagrams by the SPACE tool. The application software is a direct outcome of this design process; it is not developed separately.

The intent of the high-level project-related review is addressed the by the routine project management meetings established in the Project Plan. These project meetings include internal project meetings, customer interface meetings, and management oversight meetings and involve the project stakeholders.

Separate Configuration Control Board meetings to address changes to the application software for a TXS project would be redundant to the project meetings and Design Review Boards. Members of a separate Configuration Control Board would include the project team members that participate in the other forums and interact with each other on a daily basis. All changes to project application software are tracked via the Open Item process, which requires an evaluation of affected documents and software changes. Software errors that are conditions adverse to quality are also processed in the Corrective Action Program. Since all changes are tracked via the Open Item process, and that process requires an evaluation of document and software changes, separate Configuration Control Board meetings would be a duplication of other existing processes using the same personnel. The Open Item process and associated evaluation are used in place of Configuration Control Board meetings.

The Software Configuration Management Plan specifies the organizational responsibilities, configuration management controls, change management controls, and interface controls. The Technical Manager is responsible for the implementation of the Software Configuration Management Plan.

The overall AREVA NP approach to configuration management of the TXS platform, TXS projects, and the project-specific application software meets the intent of IEEE Std 828-1990 and IEEE Std 1042-1987.

RAI 69

There are different conventions that are at times followed in the documentation of requirements. One convention is that a requirement is stated only once. Another convention is to present information relevant to a particular concern in a particular document; this presentation can be called a view. With multiple views comes the possibility of presenting some of the same information in more than one place. The combination of these two conventions is sometimes accomplished by stating a requirement in one place (e.g., using "shall") and describing it in all other places (e.g., using "is").

The SCMP states (see Section 3.2.2, page 35):

Proprietary *[["The process of modification, storing, and identifying the function diagrams, the resulting source code, executable programs, GSM screens, and scripts is described in AREVA NP Inc. OI-1460."]]*

This statement does not contain the word "shall;" is this statement a requirement?

Duke Response to RAI 69

The referenced sentence in AREVA NP Document 51-9006444-005, Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade Software Configuration Management Plan, is meant to be a statement of fact. The applicable *shall* statements are located in OI-1460, TELEPERM XS Software Configuration Management Plan, specifically Section 3.2.4.

RAI 70

The SCMP contains two definitions regarding "configuration audits": "Function Configuration Audit", and "Physical Configuration Audit." The body of the SCMP uses a third term "Configuration Audit;" the SCMP states (Section 3.4.1, page 38):

Proprietary *[["When the Application Software is completed and issued for release, a Code Configuration Document shall be issued. This document reports, using the "scanmic" tool, the exact configuration of all software that is part of the safety-related software portion of the TXS System. Included in this document are the configurations of the Application Software, System Software, L2 Software, and H1 Software running on the system. This configuration is documented in accordance with the AREVA NP Inc. Quality Management Manual (Reference /12/). AREVA NP Inc. ICS credits this activity and report as a* ***Configuration Audit****. This is acceptable because the Code Configuration Document records the exact configuration of the system's safety-related software. This document and therefore the system's safety-related software configuration is reviewed and approved by independent personnel which equates to a Configuration Audit."]]*

*Regulatory Guide 1.169 Section C.1.4, "**Configuration Audit**," states: "IEEE Std 610.12-1990 refers the definition of configuration audit to two other audits without specifying whether one or both definitions are meant. In the context of an audit for delivery of a product, a configuration audit includes both a functional configuration audit and a physical configuration audit."*

(a) Does the term "configuration audit" on page 38 of the SCMP refer to: "Functional Configuration Audit", "Physical Configuration Audit", or both?

(b) Please describe how the review of the Code Configuration Document addresses the "Functional Configuration Audit" and "Physical Configuration Audit" as defined in the SCMP.

(c) What documentation describes the designed configuration of all software that is part of the safety related software portion of the TXS System?

Duke Response to RAI 70

Response (a): The process described in Section 3.4.1 of the Software Configuration Management Plan (SCMP) was intended to describe the method of configuration status accounting that keeps track of the status of the latest version of each software component. The physical configuration audit is a formal audit that compares the final code against the final documentation for that code to ensure that the documentation and code are in agreement before being released to the user or customer. Section 3.4.2 of AREVA NP Operating Instruction OI-1460, *TELEPERM XS Software Configuration Management Plan,* was revised to clarify the process of conducting Physical Configuration Audits.

Response (b): The Functional Configuration Audit is a formal audit that compares the acceptance test results with the currently approved software requirements to ensure that all requirements have been satisfied. Section 3.4.3 of OI-1460 was revised to clarify the process used for conducting Functional Configuration Audits.

Response (c): The Code Configuration Document reports the configuration for all of the delivered software. When the Application Software is completed and issued for release, a Code Configuration Document is issued. This document reports, using the *scanmic* tool, the exact configuration of all software that is part of the safety-related software portion of the TELEPERM XS System. The configurations of the Application Software, System Software, L2 Software, and H1 Software running on the system are included in this document. The configuration is documented in accordance with the AREVA NP Quality Management Manual. The Code Configuration Document is published upon each release of the software. Section 3.3 of OI-1460 was revised to clarify the purpose and use of the Code Configuration document.

A copy of OI-1460-07, *TELEPERM XS Software Configuration Management Plan*, is included in Enclosure 2. The Oconee SCMP will be reviewed to reflect the changes to OI-1460.

RAIs associated with Software Integration Plan (SIntP)

The Standard Review Plan (SRP) documents that a description of the contents of a Software Integration Plan (SIntP) is contained in NUREG/CR-6101. The SRP states (NUREG-0800 Chapter 7, Branch Technical Position No. 7-14 Section B.3.1.4, "Software Integration Plan"):

> "NUREG/CR-6101, Section 3.1.7, 'Software Integration Plan,' and Section 4.1.7, "Software Integration Plan," contain guidance on SIntPs."

NUREG/CR-6101 states (Section 3.1.7):

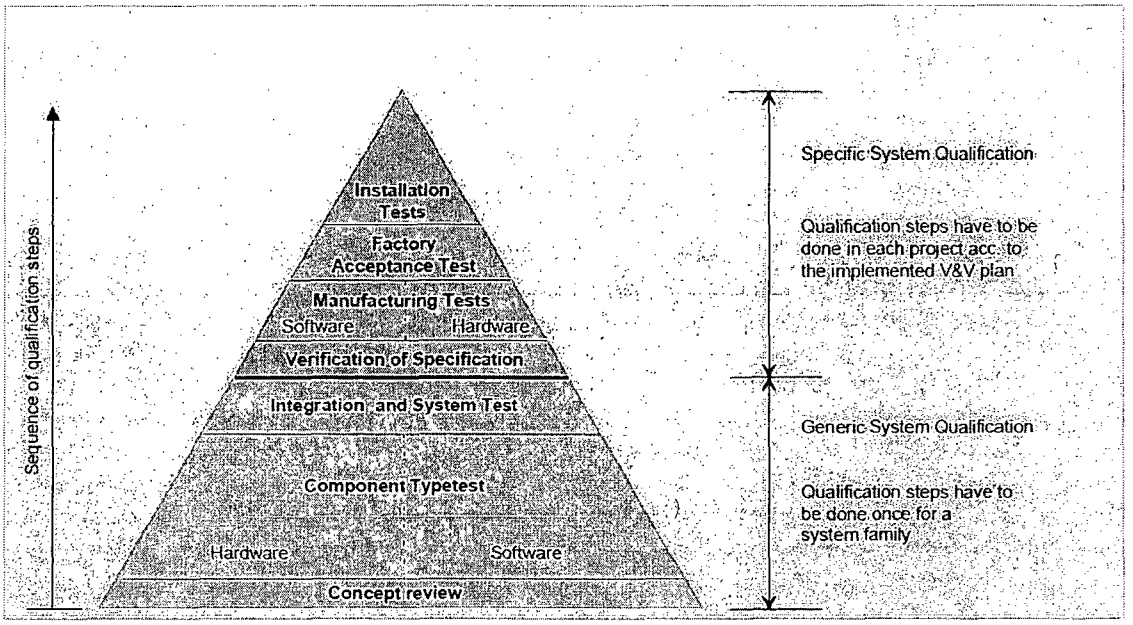
> "Software integration actually consists of three major phases: integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product. During the first phase, the various object modules are combined to produce executable programs. These programs are then loaded in the second phase into test systems that are constructed to be as nearly identical as possible to the ultimate target systems, including computers, communications systems and instrumentation. The final phase consists of testing the results, and is discussed in another report..."

RAI 71
Please provide an explanation of how the various RPS/ESPS integration activities address the SRP acceptance criteria for a SIntP. This explanation should include a cross reference that explains how RPS/ESPS project documentation addresses the full scope of integration as described by NUREG/CR-6101.

Duke Response to RAI 71

The TELEPERM XS (TXS) system is a fully integrated suite of hardware and software designed specifically for nuclear safety applications. The TXS system has significant nuclear operating experience. The TXS platform has been fully qualified as an integrated platform. The TXS system is described in TXS Topical Report. NRC approved the TXS Topical Report in a safety evaluation report (SER) issued in May 2000.

The overall qualification process for the TXS system is shown in Figure 2.2 of AREVA NP Topical Report EMF-2110(NP), *TELEPERM XS: A Digital Reactor Protection System*, Revision 1 (referred to as the TXS Topical Report). The qualification process is a two-part process: generic system qualification and specific system qualification. The qualification process for application software starts with the application-independent (generic) qualification process described in Section 2.1. The application-dependent (specific project) phase takes credit for all application-independent (generic) qualification activities, as noted on page 2-4 of the TXS Topical Report.



The generic qualification process included an integration and system test phase, which is described in detail in Section 3.2.2 of the TXS Topical Report. The system test documentation is listed in Section 8.1.1 of the TXS Topical Report.

Application software is developed using the TXS SPACE tool. This tool is used to develop Function Diagrams and Network Diagrams. Function Diagrams specify the signal processing requirements for the system. Network Diagrams define the hardware components of the system and their logical interconnections. Software code is automatically generated from the Function Diagrams and Network Diagrams by the SPACE tool. Logical 'software integration' occurs at this stage. The project-specific TXS system is developed from qualified hardware and software modules using the qualified development tools.

Physical software integration occurs during the FAT stage, when the application software is loaded on the TXS processors. The project-specific FAT Plan covers the approach and activities associated with the Software and Hardware Integration.

A project-specific Software Generation and Download Procedure is issued for each project to control and document the generation of each application software release. It is used to control and document the download of each approved software release to the target system. This project-specific Software Generation and Download Procedure is implemented under a work order (task-letter) for each Application Software Release. The Software Generation and Download Procedure is a configuration item that is governed by the Software Configuration Management Plan.

IEEE Std 1012-1998, *IEEE Standard for Software Verification and Validation*, describes four testing activities:

- Component Testing: Testing conducted to verify the correct implementation of the design and compliance with program requirements for one software element (e.g., unit, module) or a collection of software elements. (Clause 3.1.3)

- Integration Testing: An orderly progression of testing of incremental pieces of the software program in which software elements, hardware elements, or both are: combined and tested until the entire system has been integrated to show compliance with the program design, and capabilities and requirements of the system. (Clause 3.1.10)

- System Testing: The activities of testing an integrated hardware and software system to verify and validate whether the system meets its original objectives. (Clause 3.1.26)

- Acceptance Testing: Testing conducted in an operational environment to determine whether a system satisfies its acceptance criteria (i.e., initial requirements and current needs of its user) and to enable the customer to determine whether to accept the system. (Clause 3.1.1)

The combination of TXS generic qualification testing and project-specific testing addresses all of the testing activities in IEEE Std 1012-1998, as shown in Table 71-1.

The generic TXS platform integration and system testing generically satisfies aspects of IEEE Std 1012-1998 requirements for integration testing of the hardware modules, operating system software modules, and a typical application software package in a typical TXS system configuration. The Oconee Factory Acceptance Test (FAT) satisfies the project-specific aspects of IEEE Std 1012-1998 requirements for Oconee application software integration, system, and acceptance testing.

Table 71-1 - Alignment with IEEE Std 1012-1998 Testing Activities

IEEE Std 1012-1998 Testing Activity	Generic TXS Testing	Oconee Project Testing
Component Testing	Hardware and Software Type Tests, including Function Blocks)	Not Applicable (based on use of qualified hardware and software modules)
Integration Testing	Integration of TXS Hardware Modules, Operating System Software Modules, and a Typical Application Software Package in a Typical System Configuration	Integration Testing of System Hardware Components in Oconee Configuration: Pre-FAT prerequisites and procedure dry runs (manufacturing tests) Integration Testing of Oconee Application Software (Integration of Function Block and Function Diagrams): FAT Software Tests System and Acceptance Testing of Oconee System: Compete Set of FAT Tests
System Testing		
Acceptance Testing	Not Applicable	

The combination of TXS generic qualification testing and project-specific testing addresses all of the testing activities in IEEE Std 1012-1998.

The TXS Topical Report (Section 3.2.2) and AREVA NP Document 51-9052960-003, Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade Factory Acceptance Test Plan, address the relevant aspects of NUREG/CR-6101 Section 3.1.7.

RAI 72

Supplement 4 states that "FAT fulfills the requirements for system integration ... testing" and that "additional application software integration test cases are added to the scope of FAT to satisfy IEEE Std 1012-1998 validation requirements for application software integration testing." The "testing" aspects of FAT could be considered to address the testing the resulting integrated product; however the docketed FAT plan does not mention integration testing.

Please provide integration testing documentation.

Duke Response to RAI 72

The TXS Topical Report (Section 8.1.1) identifies the generic integration and system test documentation. The response to RAI 52 provides additional information on the integration testing performed for the SVE2 module.

AREVA NP Document 51-9052960-003, Oconee Nuclear Station, Units 1, 2, and 3 RPS/ESFAS Controls Upgrade Factory Acceptance Test Plan describes the general approach to the Oconee FAT, including the Pre-FAT activities (see Figure 1). An updated copy of the Oconee FAT Plan was submitted in response to RAI 50.

The Oconee FAT specifications and procedures are being submitted to NRC by separate correspondence. The documents will be annotated to address the test cases that address application software integration testing requirements.

RAIs associated with Software Installation Plan (SInstP)

The SInstP address the installation of the integrated system into the target environment (e.g., installation at the nuclear power plant); the SRP states (NUREG-0800, Chapter 7, Branch Technical Position No. 7-14, Section B.3.1.5, "Software Installation Plan"):

> *"NUREG/CR-6101, Section 3.1.8, 'Software Installation Plan,' and Section 4.1.8, "Software Installation Plan," contain guidance on SInstPs."*

NUREG/CR-6101 states (Section 4.1.8):

> *"The Software Installation Plan governs the process of installing the completed software product into the production environment. There may be a considerable delay between the time the software product is finished and the time it is delivered to the utility for installation.*
>
> *Without an Installation Plan, the installation may be performed incorrectly, which may remain undetected until an emergency is encountered. If there is a long delay between the completion of the development and the delivery of the software to the utility, the development people who know how to install the software may no longer be available."*

RAI 73

NUREG-0800 (SRP), Chapter 7, Branch Technical Position 7-14, Section B.3.1.5 contains acceptance criteria for Software Installation Plans.

Supplement 2 Table 2, "Disposition of References to the SPM from the ONS RPS/ESPS LAR," identifies that the Software Installation Plan is addressed by the Oconee "Software Generation and Download Procedure [AREVA NP Inc. Doc. No. 51-9001942-004]."

The Software Generation and Download Procedure does not contain site-specific installation instructions.

Please describe the planned site installation activities and associated documentation.

Duke Response to RAI 73

AREVA NP document 51-9001942-004, Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Generation and Download, is specifically written to cover all software installation activities up to and during the factory acceptance test for the Unit 1 software. This procedure contains sufficient detail such that Duke Energy will be able to write its own software download procedure. This Duke Energy procedure would be covered under the Duke Energy document NSD 800, Software and Data Quality Assurance (SDQA) Program.

LAR Review Items---- Question on TSs and Design

RAI 74
Section 9.3 in Enclosure 2 states that a quantitative availability analysis (32-5061241-00, not included in table 1-2) and a qualitative analysis (included in table 1-2) are utilized for calculating the probabilities of failure, and estimates of reliability and availability. The "operating history and reliability data is provided as the basis for the proposed test intervals." This section also states that the availability analysis did not include the TXS output relays and that it will be revised to include the output relays and the results of the FMEA.

Please submit the quantitative availability analysis, which includes the output relays and the results of the FMEA.

Duke Response to RAI 74

AREVA NP document 32-5061241-001, *Oconee Nuclear Station, Unit 1, RPS/ESFAS TXS Upgrade, Availability Analysis*, is provided in Enclosure 2 (Summary and Appendices 1-3 only). This document provides the quantitative availability analysis for the Oconee Nuclear Plant, Unit 1, RPS and ESPS TXS system. The analysis uses industry consensus standards as part of an overall approach to meeting the requirement of 10 CFR Part 50 for design safety systems of nuclear power plants. The form and content of this document complies with IEEE Standard 577-1976, *Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations.* The method for preparing, conducting, and evaluating the RPS/ESPS TXS system availability complies with the IEEE Standard 352-1987, *Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems.* The analysis demonstrates the high reliability that is built into the Oconee RPS and ESPS.

RAI 75

Section 9 in Enclosure 2 provides justification for changing the technical specifications (TSs) channel functional test interval from the current requirement of 45 days on a staggered test basis to an interval of 18 months plus 25%. In this section, Duke stated that this interval is consistent with the recommended surveillance testing provided in Topical Report EMF-2341(P) which was reviewed by the NRC as part of their review of TXS topical report. The document 51-9044432-003, "Oconee Nuclear Station RPS/ESPS Surveillance change justification" supports the proposed interval. In Section 1 of Enclosure 2, Duke referenced various sections of EMF-2341(P) for channel functional test and stated, "Logic System Functional Tests are accomplished by Continuous self monitoring."

However, the staff SER on the TXS topical report referenced EMF-2341(P) and stated in Section 4.2 as follows:

> *"The report describes measures to be implemented in safety I&C systems configured with a TXS architecture to comply with requirements for channel checks, functional tests, channel calibration verification tests, response time verification tests, and logic system functional tests.*
>
> *The measures include:*
>
> - *Periodic verification (during refueling outages) of accuracy and time constants of the analog input modules*
> - *Continuous self-monitoring and on-line diagnostics to verify proper functioning of digital systems and to ensure integrity of the installed application and system software*
> - *Periodic actuation of output channel interposing relays - The reactor trip function is tested at the same surveillance test interval as current technical specifications (typically quarterly) and the engineered safety features actuation system (ESFAS) function is tested consistent with the licensee's refueling outage (typically 15 to 24 months).*
>
> *As defined in the [Advanced Light Water Reactor (ALWR)] Standard Technical Specifications, a logic system functional test is a test of all required logic components (i.e., all required relays and contacts, trip functions, solid-state logic elements, etc.) of a logic path, from as close to the sensor as practicable up to, but not including, the actuated device, to verify operability. The logic system functional test may be performed by means of any series of sequential, overlapping, or total system steps so that the entire logic system is tested.*
>
> *For some applications, interposing relays may be used in the logic component. The licensee should test those relays in accordance with the existing TS requirements. It is prudent to verify the logic system functions at least every refueling outage. This is a plant-specific action item along with the plant-specific technical specification requirements."*

Please provide detail explanation how continuous self monitoring of the instrumentation channel, which ends at the target system hardware (TXS Processor), will perform periodic functional testing of logic system and interposing relays as identified in the above statements of the staff SER. Also please submit AREVA document 51-9044432-003,"Oconee Nuclear Station RPS/ESPS Surveillance Change Justification" referenced in Section 9.4.

Duke Response to RAI 75

Based on discussions between NRC, AREVA and Duke on September 19, 2008, Duke decided to retain the current Technical Specification (TS) Channel Functional Test (CFT) frequency of once every 92 days and revise the TS Bases to indicate that for Unit(s) with the digital upgrade complete, the CFT is fulfilled by automatic cyclic self monitoring, manual verification of the setpoints and manual actuation of the output channel interposing relays.

The TS markup and TS retype for TS 3.3.1, TS 3.3.5, and TS 3.3.7 have been revised appropriately to reflect these changes and are included in Attachments 1 and 2, respectively, of this enclosure.

The Cyclic Self-Monitoring Task is implemented as a continuous test process in each SVE (Function Computer) to provide the earliest possible detection of hardware faults. The Cyclic Self-Monitoring Task checks the functions of the SVE and the connected components, which are tested during operation without impeding the safety tasks. It operates as an independent task with lowest priority and can be interrupted by programs with a higher priority, e.g. the RTE executing the Function Diagram Group Modules.

The time remaining between the end of the processing of the functional tasks and the beginning of the next cycle is used for the processing of Cyclic Self-Monitoring Task. Since a complete self-test procedure requires more than a single computer cycle, the Cyclic Self-Monitoring Task is divided into smaller tasks that are not interrupted. The small size ensures that the deterministic cyclic operation of the system is not influenced by the Cyclic Self-Monitoring Task. A complete pass of these tests can last a few minutes, depending on the duty cycle of the SVE.

The Cyclic Self-Monitoring is monitored by the RTE using a cycle counter. If the Cyclic Self-Monitoring Task is not completed within one hour, a RTE error message is generated.

The following tests are implemented in the Cyclic Self-Monitoring Task ("functional" as used below refers to the functional test of device tasks during Cyclic Self-Monitoring):

- CPU Test (functional)
- FPU Test (Functional)
- RAM Test (read/write)
- Flash Erasable Programmable Read Only Memory (FEPROM) Test (read/write)
- SSC Interrupts (functional)
- Timer interrupts (functional)

- Watchdog (functional)
- Scratch pad (CRC)
- I/O Bus (functional)
- Module LEDs (functional)
- Module Ports (functional)
- Parameter Registers (functional, CRC)
- System Ports (functional)
- Jumpers (functional)

Additional details related to the Cyclic Self-Monitoring task are outlined in the response to RAI 14. Details concerning the self monitoring of communication signals are provided in the response to RAI 15. The Cyclic Self-Monitoring task performs a complete functional test of the RPS/ESPS channel logic every few minutes. An RTE error message is generated if the Cyclic Self-Monitoring task is not completed within one hour.

AREVA NP document 51-9044432-004, Oconee Nuclear Station RPS/ESPS Surveillance Change Justification, is provided in Enclosure 2.

RAI 76

Oconee current TSs definition of channel functional test requires OPERABILITY verification, including required alarms, interlocks, display, and trip functions. The LAR has proposed changing this definition as follows:

- *Analog and bistable channels - the injection of 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.*

- *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 of all devices in the channel required for channel OPERABILITY.*

The current TSs definition specifies the "functions to be tested for operability verification" whereas the proposed change does not specify what are "all devices in the channel required for channel operability." Please explain this discrepancy and revise the proposed definition. Please note that the LAR Enclosure 1, Figure 2.2-1 identifies boundaries of a channel.

Duke Response to RAI 76

As stated in description of the TS change on page 1 of RPS/ESPS LAR Enclosure 2, the proposed wording is consistent with the Combustion Engineering (CE) Standard Technical Specifications (STS). Duke used the CE STS as precedence since its CFT definition addresses analog and digital computer channels. The use of the words "of all devices in the channel required for channel OPERABILITY" in place of "including required alarms interlocks, display, and trip functions" is not only consistent with the CEOG STS (NUREG 1432) it is also consistent with Revision 3 to the Babcock and Wilcox STS (NUREG 1430), the Westinghouse STS (NUREG 1431), the General Electric BWR/4 STS (NUREG 1433), and General Electric BWR/6 STS (NUREG 1434). Revision 3 of the STS was published June 2004.

The wording of Revision 3 to the STS was based on TSTF-205-A, which was approved by the NRC on January 13, 1999. The TSTF indicates that the revised definitions eliminate an ambiguity and possible misinterpretation of Channel Calibration and Channel Functional Test. The previous definitions used the phrase "including required alarms interlocks, display, and trip functions." Due to an ambiguity in the application of the word "required" and whether the list is inclusive or representative the NRC proposed this revision to the STS. The new phrase clarifies the use of the word "required" and makes clear that the components that are required to be tested or calibrated are only those that are necessary for the channel to perform its safety function.

Duke has determined, based on further review of Revision 3 to the STS and TSTF-205-A that a similar change needs to be made to the definition of Channel Calibration. Therefore, Duke proposes to change the words "including required alarms interlocks, display, and trip functions" to "of all devices in the channel required for channel OPERABILITY" in the Channel Calibration definition consistent with the STS wording.

The TS markup and TS retype for this change is included in Attachments 1 and 2, respectively, of this enclosure.

RAI 77

LAR Enclosure 1 page 2-8 and AREVA NP Inc. Doc., No. 51-9029108-003 page 21 (item 3 of LAR Enclosure 6), show Reactor Trip Relay Logic with two S451 digital output modules in each of the four channels; whereas, AREVA NP inc., Doc. No. 51-5065423-07 page 33 (item 14 in Table 1-2 of LAR) shows four modules per channel. Please explain the difference and function of these modules. Are these modules operating in a Master/ checker configuration as the two SVE2 processing modules in each ESFAS voter subsystems?

Duke Response to RAI 77

The Oconee design uses two S451 digital output models in each of the four RPS channels. Each S451 digital output module is capable of providing up to 32 outputs; however, only two outputs in each S451 are used in Reactor Trip Relay logic for the Oconee design.

AREVA NP document 51-9029108-003, Oconee Nuclear Station, Units 1, 2 and 3 RPS/ESFAS Controls Upgrade TXS System Description for LAR Input, shows a physical (hardware) view of the four output signals coming from two S451 modules. The figure on page 33 of AREVA NP document 51-5065423-07, *Oconee Nuclear Station, Unit 1 RPS/ESFAS Controls Upgrade Software Design Description, shows* four outputs per channel dedicated for Reactor Trip Relay Logic, not four modules per channel. A more detailed view that shows the S451 modules can be seen on Attachment 3-1 of the same document.

These S451 digital output modules do not operate in a Master/Checker configuration.

RAI 78

LAR Section 2.7.2 references Table 2.7-2 for a summary and discussion of the changes to software and references Table 2-4 for a summary of software revisions, since TXS SER. Table 2-4 is included in the submittal while Table 2.7-2 is missing. Please provide Table 2.7-2.

Duke Response to RAI 78

There is no Table 2.7-2. The reference to Table 2.7-2 should have been to Table 2-4. During editing, the tables were renumbered to coincide with the Chapter (2) instead of the Section (2.7). The editor missed renumbering this particular reference.

RAI 79

DLPIAS manual actuation capability, as explained in LAR Section 2.4.2.1, includes an Emergency Override pushbutton to permit a redundant capability to prevent inadvertent operation of the LPI pumps. Please explain and justify why a similar capability is not provided in DHPIAS. Also, identify as to what administrative controls will be established for the use of these override push buttons, how long the DASs will be allowed to be over-ridden, and will the affected RPS/ESPS channels be operable during the period of the DAS override? How will the DAS operability status be indicated?

Duke Response to RAI 79

A similar capability is being provided for DHPIAS, however it was not listed in the RPS/ESPS LAR since a decision had not been made to include the DHPIAS override switch at the time of submittal.

Administrative Controls will be established to address the use of the override switches. The Diverse LPI and HPI BYPASS/ENABLE pushbuttons will be used to bypass the DLPIAS and DHPIAS during both maintenance and operation. Plant procedures will require the DLPIAS and DHPIAS to be bypassed during controlled shutdowns at the same time the LPI Bypass and HPI Bypass are initiated for the ESPS. As stated in Section 2.4.2 of Enclosure 1 to the

RPS/ESPS LAR, Duke will implement a Selected Licensee Commitment (SLC) to address functionality requirements for the DLPIAS and the DHPIAS. The SLC Manual is Chapter 16 of the Oconee UFSAR. Changes to SLCs are considered changes to NRC commitments and are made in accordance with approved directives and by use of the 10 CFR 50.59 process.

Duke plans to base the DLPIAS and the DHPIAS SLC requirements on the existing non-safety related ATWS systems. For ATWS, the system may be bypassed for seven days to make whatever repairs are needed to the system and to restore it to service. If the system in not restored within seven days, then a report must be sent to the NRC within 30 days outlining plans for repairing the system and restoring it to service. Normally the Bypass switch would be used to take DLPIAS out of service. However, if for some reason the Bypass switch was unavailable, the Override switch will be used to accomplish the same thing and the same administrative requirements will apply.

The affected RPS/ESPS channels will be operable during the period of the DLPIAS or DHPIAS override. The three reactor coolant pressure transmitters that provide input to the ESPS channels will also provide isolated analog signals to DLPIAS and DHPIAS. DLPIAS and DHPIAS hardware will provide the necessary bistables, relays for the needed two out of three logic, etc. to perform their function. The DLPIAS and DHPIAS Bypass and Override switches affect only the DLPIAS and DHPIAS hardware. There is no effect from these switches on the RPS/ESPS channels.

A statalarm is provided for the DHPIAS and DLPIAS Bypass/Enable switches. Therefore, if either diverse actuation system is placed in bypass, an alarm will be displayed on SA1 statalarm panel. The DLPIAS Bypass/Enable and Override pushbuttons are located on UB2. The DHPIAS Bypass/Enable and Override pushbuttons are located on UB1. Pushing either Bypass/Enable pushbutton lights the amber light on its unit board. Pushing either Override button lights the red light on its unit board. The presence of a statalarm or indicating light is indicative of an inoperable diverse actuation system. Therefore, entry into a SLC condition entry would be made to track the diverse actuation system inoperability.

RAI 80

LAR Section 4.2.2 lists RG 1.118, Revision 3 to provide the regulatory requirements for the proposed change. Revision 3 of RG 1.118 endorsed IEEE Std. 338-1987 which states in Section 5 (13), "where practical, means shall be included in the design to prevent the simultaneous application of any bypass condition to redundant channels or load groups during testing."

LAR Enclosure 6 item 3 (AREVA NP Inc. Doc., No. 51-9029108-003) in Section 4, lists various operational modes such as TXS parameter change enable mode, RPS shutdown bypass mode, RPS instrument input channel manual bypass mode, and ESPS voter manual bypass mode. The key-switches of these bypass modes are administratively controlled and there are no hardware or software interlocks between channels. Please identify the means to prevent the simultaneous application of any bypass condition to redundant channels or load group during testing, as required by IEEE-338.

Duke Response to RAI 80

A detailed document was developed to address the functional requirements of the keyswitches that are used for the various operational modes. A summary of the keyswitch document is provided for this RAI response and the detailed information is contained in AREVA document 51-5045379-10 "Oconee Nuclear Station, Units 1, 2 and 3 RPS/ESFAS Controls Upgrade Design Specification for Keyswitches." This document was provided to NRC as item 7 in Enclosure 1 to LAR Supplement 1.

The purpose of the keyswitch document is to summarize the functional design requirements for the key-operated electronic switches (keyswitches) internal to the Oconee RPS/ESPS Plant Protection System cabinets. The keyswitch document also provides an overview of the keyswitch functions and implementation methodology.

To address the various operational modes for RPS and ESPS, each individual keyswitch operational mode is discussed separately below.

RPS Shutdown Bypass

RAI 81

According to the network architecture described in LAR Enclosure 1 and slides 23, 31, and 34 in the December 13, 2006, presentation, SL21 data link is used for communication between

RPS/ESFAS channels and uses a token for giving authority to each channel to send data. For a lost token condition, which sometimes happens, it is not clear how response time, deterministic procedure and fail-safe criterion is met. The token re-making time would delay the response time used in accident analysis, and/or may affect the deterministic property and the accident analysis. Please explain how this token passing instead of a point-to-point communication meets the safety criteria and maintains the accident analysis results. Please explain how this is comparable to ISG #4 criteria regarding point-to-point communications between safety channels.

Duke Response to RAI 81

The effect of the loss of a single token is bounded by the loss of the affected, single communication link within the Oconee RPS/ESPS System Architecture. A lost token would lead to a loss of communications on that link until the token is regenerated. The bounding effect of a single communication link failure has been analyzed in Failure Modes and Effect Analysis performed for the Oconee RPS/ESPS design. That analysis concluded that the failure of a single communication link does not prevent the performance of the safety system function because valid signals from other redundant channels are received by even the channel affected by the lost token. Similarly, the recovery time for the loss of a single token has no effect on overall system response time, since the redundant channels (and even the channel affected by the lost token) would provide the safety actuation within the required response time. AREVA NP Document 51-5023886-03, *Oconee Nuclear Station Unit 1 RPS/ESFAS Controls Upgrade Failure Modes and Effects Analysis*, was submitted to NRC in LAR Supplement 1.

The assumed common mode failure of all PROFIBUS connections would result in a total loss of all data communications between redundant protection channels and cause the Oconee RPS/ESFAS System to operate in a 'silo' mode. It is called a silo mode because each channel would trip when its single valid process input reaches the trip value. The loss of communication from one channel to another causes the input to the receiving channel to be faulted. The function blocks react to exclude the faulted input data from processing and use only the valid available inputs. If the valid inputs are reduced to only one due to signal faults then the function will trip when the single valid input reaches the trip value. This assumed condition is also bounded by the Diversity and Defense-In-Depth analysis performed for the Oconee RPS/ESPS design.

The point-to-point network architecture of the Oconee RPS/ESPS design has been described in response to RAIs 10, 13, 16, 20, and 43.

RAI 82

According to LAR Enclosure 1 (fig.2.1-2/2.2-1) and AREVA NP Inc. Doc. No. 51-9029108-003, Profibus L2 data link is used in inter-channel communication when each safety channel sends their input signal to 2.MIN/2.MAX Function Block of redundant channels, and when each channel send its bi-stable output to the redundant channel trip relays.

Please explain if token passing process is also used in the case of transmission of the bi-stable output from one channel to the redundant channels trip relays and provide the following information:

(a) Whether the two Profibus L2 data links, used in 2.MIN/2.MAX Function Block and bi-stable output, use the same token or it is a different token.

(b) What is the recovery process when the token is lost?

Please provide documentation to confirm deterministic communication.

Duke Response to RAI 82

Response (a): The Oconee RPS/ESPS design uses only point-to-point communications (i.e., two stations using token ring-like technology). Separate communication links are used for each communication channel. Data for the 2.MIN/2.MAX functions are transferred asynchronously between each safety function processor. Each data link has its own token.

The bi-stable (i.e., comparator function block) outputs are sent from the software to the field via an S451 Digital Output card. The exchange of the signals from each channel to the channel trip relays (i.e., 2/4 undervoltage relay voter) is via hardwired connections. No interchannel communications are involved with these outputs.

The Fiber Optic connections coming from the bottom of the RPS/ESPS channels shown on LAR Enclosure 1 (Figures 2.1-2 and 2.2-1) are connecting the channels to the Voters not the Reactor Trip Breakers. Refer to LAR Figure 2.3-1 for more information (dotted lines – fiber optic data link, solid line – hardwired connections).

Response (b): The TELEPERM XS (TXS) PROFIBUS communication control accesses the PROFIBUS via the layer 2 protocol Field Data Link (according to EN 50170, Volume 2/3 (PROFIBUS), Dec. 1996). This PROFIBUS standard describes the lost token recovery process. Documentation describing the deterministic PROFIBUS communication is provided in the TXS Topical Report section 2.9.2.

RAI 83

LAR Section 2.2.1 states, "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 statement does not include isolated and independent signals to DLPIAS and DHPIAS. However, Figures 2.4-1 and 2.4-2, respectively for DLPIAS and DHPIAS show buffered IE to non-1E signals from TXS to DLPIAS/DHPIAS.

Please confirm that the initiation signal from the respective SNV1 to DLPIAS/ DHPIAS is isolated and independent of the TXS processor.

Duke Response to RAI 83

The initiation signals from the respective SNV1 to DLPIAS/DHPIAS are isolated and independent of the TXS processors. The isolated signal from the SNV1 to DLPIAS or DHPIAS is non-safety related. The signal from the SNV1 to the TXS processor is safety related.

The statement referenced from Section 2.2.1 of the license amendment request Enclosure 1 was not written to be all-inclusive. Additional information on the DLPIAS/DHPIAS design is provided in Section 2.4 of the license amendment request Enclosure 1.

The SNV1 module is designed to multiply one analog input signal to four output signals. The input signal could be a voltage or a current signal. The SNV1 provide a galvanic isolation between the input and the outputs and to the power supply. The SNV1 module has been qualified using the TXS type test program, which includes functional testing under design basis environmental stress, seismic, and EMI/RFI tests. A TÜV qualification certificate was issued for the SNV1 module.

RAI 84

LAR Section 2.5.3 states:

"TXS service unit serves the following functions:

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

Functions such as, modifying online parameters, performing period testing, and central reloading of software have potential to adversely affect the safety functions. For these functions, the data exchange between safety system and non-safety systems should be processed in a manner that does not adversely affect the safety function.

Please identify the design provided in the TXS for prevention of this potential adverse effect of performing these functions on the safety system. Are these functions performed automatically or manually in a bypass mode using a software or hard-wired switch?

Duke Response to RAI 84

The response to this RAI addresses the various areas that were noted in the NRC RAI as having potential to adversely affect the safety functions.

Duke Response to RAI 52

Duke Response to RAI 52

RAI 52

Please provide an explanation of the changes to the TXS system since the TXS Topical Report that includes a fact based explanation of changes, and an explanation of how these facts can be combined to arrive at an acceptability determination.

Duke Response to RAI 52

The response to RAI 52 is provided in three parts. First, the changes to the TELEPERM XS (TXS) engineering procedures used for platform development are described. Second, the TXS hardware changes made since the TXS Topical Report was submitted to NRC are described. And third, the TXS software changes made since the TXS Topical Report was submitted to NRC are described.

1. Engineering Procedure Changes

The high quality development process for the TELEPERM XS (TXS) hardware and software was described in the TXS Topical Report. Several Siemens procedures were previously submitted to NRC in support of their review of the TXS Topical Report.[13] The changes to these procedures are summarized below.

1.1 Engineering Procedure FAW 1.1, *Phase Model for the Development of Software Components for TELEPERM XS*

No changes. The current revisions level of FAW 1.1 is Revision 0.

1.2 Engineering Procedure FAW 1.4, *Hardware Quality Assurance Requirements*

[redacted]

[13] Siemens letter NRC:99:037 from James F. Mallay to NRC dated September 1, 1999, regarding *Supporting Documentation for Review of EMF-2110(NP) Revision 1, "TELEPERM XS: A Digital Reactor Protection System"*

1.3 Engineering Procedure FAW 1.5, *Configuration Management Plan for the TELEPERM XS System Platform*

The current revisions level of FAW 1.5 is Revision B.

1.4 Engineering Procedure FAW 1.6, *Software Verification and Validation Plan*

No change. The current revisions level of FAW 1.6 is Revision 0.

1.5 Engineering Procedure FAW-1.7, *Information Security*

NRC conducted an inspection of the TXS information security program in Erlangen, Germany on March 10-14, 2008. The following excerpt is taken from NRC Inspection Report for AREVA NP GmbH 99901371/2008-201, dated May 7, 2008:

> The inspectors requested engineering procedure FAW-TXS 1.7, "Information Security," dated August 23, 2004, to review the security aspects during the development of the TXS operating system software and function block library

software to determine whether AREVA has a secure software development infrastructure. The vendor indicated that a corporate-wide procedure for information technology security incorporating all of the FAW 1.7 requirements had superseded this procedure. The inspectors reviewed the new procedure, AREVA NP GmbH "Informationssicherheit," dated November 25, 2005, with support from the vendor's technical staff. The inspectors also conducted detailed interviews with AREVA personnel to ensure that this new replacement procedure covered the necessary security aspects and requirements of a secure software development infrastructure. The inspectors requested information regarding, but not limited to, isolation of the development computers/network from the corporate network, access control and access rights to particular development computers, process for using purchased software, and physical access restrictions to the development lab. Additionally, the inspectors verified implementation of security measures during the tour of the TXS platform development lab. The inspectors found no issues associated with the security controls used for the development of TXS software.

1.6 Engineering Procedure FAW 2.1, *Programming Guidelines*

Minor enhancements were made to the procedure:

- Based were made to on experience with the programming of TXS software,
- Enhancements in the C++ programming guidelines (for tool development), and
- Adaptation to AREVA NP's corporate documentation guidelines.

The current revisions level of FAW 2.1 is Revision C.

1.7 Engineering Procedure FAW 2.2, *Documentation Guidelines*

Minor enhancements were made to the procedure:

- Improve practical guidance based on experience and
- Extension of guidelines to better define formal content of documents and version control.

The current revisions level of FAW 2.2 is Revision B.

1.8 Engineering Procedure FAW 3.3, *Contents of the Requirements Specifications for Software Components*

The new version of FAW-3.3 only concentrates on software requirements specifications. A separate engineering procedure specific to hardware requirements specifications was developed recently, providing more detailed guidance for hardware requirements engineering. (NOTE: This procedure change was not applicable for components used for

Oconee.) Economic data are no longer required to be contained in a requirements specification document for a TXS component.

Minor enhancements were made to the procedure:

- Consideration of the evolution of C++ and
- Adaptation to AREVA NP's corporate documentation guidelines.

The current revisions level of FAW 3.3 is Revision A.

1.9 Engineering Procedure FAW 3.4, *Contents of the Technical Specifications for Software Components*

The description of interfaces of a software component is concentrated in one section of the design specification. Aspects of user documentation are now described in an additional Engineering Procedure FAW NLL-053, *Generation, Approval and Archiving of TELEPERM XS System Documentation.*

Minor enhancements were made to the procedure:

- Consideration of the evolution of C++ and
- Adaptation to AREVA NP's corporate documentation guidelines.

The current revisions level of FAW 3.4 is Revision B.

1.10 Engineering Procedure FAW 3.5, *Contents of the Design Descriptions for Software Components*

Minor enhancements were made to the procedure:

- Consideration of the evolution of C++ and
- Adaptation to AREVA NP's corporate documentation guidelines.

The current revisions level of FAW 3.5 is Revision A.

1.11 Engineering Procedure FAW 3.6, *Contents of the Implementation Descriptions for Software Components*

Minor enhancements were made to the procedure:

- Consideration of the evolution of C++ and
- Editorial changes and adaptation to AREVA NP's corporate documentation guidelines.

The current revisions level of FAW 3.6 is Revision B.

1.12 Engineering Procedure FAW 4.1, *Software Tests*

No changes. The current revisions level of FAW 4.1 is Revision 0.

1.13 Engineering Procedure FAW 4.2, *Reviews*

Minor enhancements were made to the procedure:

- Improved practical guidance for review activities and better technical focus of review activities,
- Improved method of documenting review activities and results in the review protocol was established,
- Formal adaptation to the current organization of the development department,
- Consideration of the evolution of C++, and
- Adaptation to AREVA NP's corporate documentation guidelines.

The current revisions level of FAW 4.2 is Revision B.

2. Hardware Changes

The TXS hardware changes made since the TXS Topical Report was submitted to NRC are outlined below. The information is organized by hardware component. The discussion includes a summary of the qualification activities associated with each hardware change. In addition, a discussion of any associated software change is included for completeness.

Each TXS hardware change (and associated software or firmware changes) was made in accordance with the high quality development process described in part a above. This development process includes the use of a third party reviewer Technischer Überwachungs-Verein (German Technical Inspection Agency known as TÜV). A TÜV qualification certificate was issued for each qualified hardware module developed by AREVA NP.

2.1 New SVE2 Processing Module

The design function of the SVE2 module is to process the software which implements the engineered I&C functions of the TXS systems.

Original Development

The SVE2 was developed as a successor for the SVE1 processing module. The unavailability of components due to obsolescence (e.g., bus drivers, processor, system controller, etc.) has resulted in the need to development of a successor to the SVE1

processing module. The SVE2 module is also used as a basis for the SCP2 communication processors.

The type test program included function testing (worst case scenario), environmental, seismic, and EMC testing as specified by:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*
- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The hardware test program included:

- Start up tests - The start up tests include a complete functional and operability test under the worst case conditions of the temperature and power supply.
- Environmental tests - Two different environmental tests were performed: one in accordance with the KTA 3503 requirements the other in accordance with the guidance of EPRI TR-107330.
- Seismic tests - Two different seismic tests were performed: one in accordance with the KTA 3503 requirements the other in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility and power surge withstand capability) tests - The EMC tests were designed to qualify the SVE2 module in accordance with EPRI TR-102323, Revision 1.
- Final tests - The final tests include a complete functional and operability test under the worst case conditions of the temperature and power supply.

The SVE2 test program for KTA 3503 testing was performed by the independent experts of the TÜV Rheinland/Berlin-Brandenburg. The SVE2 test program addressed both the

qualification regimen described in the TXS Topical Report and the additional qualification requirements of plant-specific action item 1 in the SER for the TXS Topical Report.

[ ]

TÜV Qualification Certificate No. 968/K 109.08/08 was issued for SVE2 module revision 5 demonstrating that the module was qualified by analysis to the specified requirements.

Associated Software Changes

Release 3.0.2 of the TXS Software included the necessary adaptations to the online software and tools for the SVE2. The specific changes are listed below for the corresponding software components. Additional changes to address minor errors or enhancements were included with the release. The summary of the software changes was taken from the product information summary document prepared for each software release.

Note: Releases 3.0.0 and 3.0.1 were developmental releases.

Each TXS software change associated with the SVE2 hardware change was made in accordance with the high quality development process described in part a above. The development process for the qualified components of the TXS system platform included comprehensive verification and validation activities by AREVA NP GmbH, as well as by an external appraisal of the development and test results by independent test institutes: Gesellschaft für Anlagen- und Reaktorsicherheit (German Society for Plant Safety and Reactor Safety known as GRS), Institut für Sicherheitstechnologie (Institute for Safety

Technology known as ISTec), and Technischer Überwachungs-Verein (German Technical Inspection Agency known as TÜV).

The development process for the qualified components of the TXS system platform included comprehensive verification and validation (V&V) activities by the manufacturer, as well as by an external appraisal of the development and test results by test institutes (GRS, ISTec, and TÜV). The V&V activities which are performed during development comprise:

- Reviews of the development documentation and test specifications
- Module tests of the vital software components – Testing included a regression test and a test of the implemented modifications. All possible branches within the function to be tested are executed in this process. The major part of the functionality of the software can be verified with this test. Exceptions to this include direct hardware accesses as well as interactions between the individual software components.
- Code inspections - A code inspection of the complete source code was performed for the runtime environment (the central software component) to ensure that the modifications which were integrated into RTE were implemented correctly. For other software components, which had minor changes, a code inspection of the modified sections was performed.
- Functional tests of the software components - A component test was performed for all modified software components on the target system. The main emphasis of these tests was to check the adaptation for the SVE2 as well as the modified functionality. These tests also included checks of direct hardware accesses. For the software components which were not modified, selected regression tests were performed which proved compatibility with SVE2.
- Integration tests - This test included all software components used in a configuration typical for applications. In this way, the interactions between the individual software components were tested. Fundamental system characteristics of the TXS system such as input and output via I/O modules, communication between SVEs over different buses, and processing of function diagrams were also checked in the test cases. The test was performed on a test system which represents a small I&C system.

The modified software modules were subjected to an external qualification test by the Institute for Safety Technology (ISTec) and the Technical Inspection Agency (TÜV) Nord. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety Systems in Nuclear Power Stations*

A qualification certificate was issued by the test institute for each qualified software module demonstrating that the module was qualified by test to the specified requirements.

Qualified (Safety-Related) Software Modules

Runtime Environment (RTE)

The GRS-ISTec Qualification Certificate No. TXS-AUCG-0999-05 was issued for RTE version 2.30 issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

MICROS

The ISTec Qualification Certificate No. TXS-MIC-1201-05 was issued for Operating System MICROS version 1.04 issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

Hardware Organization Tool (HOT)

The ISTec Qualification Certificate No. TXS-HOT-02020-06 was issued for Hardware Organization Tool version 11.00 issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

HOT Wrapper

The ISTec Qualification Certificate No. TXS-HOT-Wrapper-1101-03 was issued for HOT Wrapper version 1.01 issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

Self-Monitoring

The ISTec -TÜV Qualification Certificate No. TXS-SUE-0802-02 was issued for Self-Monitoring version 2.00 issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

I/O Drivers

The ISTec - TÜV Qualification Certificate No. 0122528655H/2 Revision I was issued for I/O Drivers versions 1.40 and 1.40a issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

Exception Handler

The ISTec - TÜV Qualification Certificate No. 0122528655H/1 Revision D was issued for Exception Handler version 1.10 issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

Code Generators FDGM and RTE-CG

ISTec Qualification Certificate No. TXS-AUCG-1102-06 was issued for Code Generator for the Runtime Environment version 2.40. ISTec Qualification Certificate No. TXS-FPGCG-1102-06 was issued for Code Generator for FD/FDG Modules version 2.40 issued with TXS software release 3.0.2 demonstrating that the modules were qualified by test to the specified requirements.

L2-CP and H1-CP Firmware

ISTec Certificate No. TXS-L2CP-1102-02 for Firmware for L2-CP version 1.20 dated 2002-11-18 and ISTec Certificate No. TXS-H1CP-1102-02 for Firmware for H1-CP version 6.20 dated 2002-11-18 were issued demonstrating that the modules were qualified by test to the specified requirements.

Integration and System Test Program for Qualified (Safety-Related) Software Modules

The modified online software as well as the two code generators (FDGM and RTE-CG) were subjected to an external qualification test by ISTec and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. In addition, implementation of the modification procedure was analyzed. On completion of the external qualification test, a test certificate was issued by the independent expert for each qualified software component and a test report was written.

The following system characteristics were confirmed during the external qualification testing:

1. The type-tested hardware and software components can be assembled to an operable system if the engineering system SPACE is used.

2. Processing and communication cycle times are not influenced by external process states (measured signals, amount of alarms and monitored information).

3. Mutually independent I&C functions are processed as specified according to their chronological order and their input signals.

4. Mutually independent processing units (in accordance with report KWU NLL5/1996/110c) do not affect each other regarding their operating modes and their time behavior. Processing units which exchange signals but are otherwise mutually independent have only effect on each other's time response within the limits of the engineered communication functions.

5. Interference on cables with violation of the measuring range and input module failures are detected, marked as signal failures, and indicated. Signals detected as faulty are processed and indicated by the system components (runtime environment, I/O drivers, and function blocks) as defined in the specification.

6. Transmission failures on TXS Ethernet (H1) and TXS PROFIBUS (L2) busses are detected, processed, and indicated in accordance with the specification. Single message failures are tolerated by the system. Furthermore, on TXS Ethernet (H1) busses double message failures are tolerated. Interference caused by a receiving unit on the sending one is impossible.

7. Sending and receiving processing units execute their functions asynchronously if no "expedited messages" are sent via serial bus links, with the exception of voter sub-units monitoring each other. Lost messages are treated like transmission errors. Thus failures of individual sending processing units are always tolerated if signal information is distributed via redundant trains and special fault propagation barrier function blocks are used on the receiving processing modules.

8. Single failures of active and passive hardware modules are detected and indicated corresponding to the implemented monitoring mechanisms (self-monitoring, monitoring of the communication, cabinet annunciation system). Multiple failures are detected and indicated if sufficient resources (for example communicating processing units and communication processors) are provided. The cabinet annunciation system is activated according to the specification.

9. Fault propagation barriers are effective provided that no plant-specific fault suppression measures are engineered (for example status correction). Signal status is changed by the runtime environment as specified, i.e., if required, status is changed to ERROR but never from ERROR or TEST to OK.

10. The runtime environment behaves in the operating modes start-up, operation, parameterization, functional test, and diagnosis as specified. It changes between operating modes according to the specification. Permissive signals for operating modes are designed individually according to project requirements and are not dealt with in the integration test.

11. The runtime environment can be controlled by means of service requests. Disabling and enabling of service requests are effective as required for the respective operating mode.

12. The user software can be loaded from a centralized unit using the network connections. This function can be deactivated by a hardware switch on the processing modules.

13. The system is consisting of several individual computers SVE1 and SVE2. When one or more computers are integrated or eliminated, the system still behaves as specified. SVE1 and SVE2 can be used together at one backplane.

14. Fail-safe behavior: Signals marked as faulty (ERROR and/or TEST status) are issued as 0 signals via output modules. Exceptions cause output of 0 signals via output modules and cause shut down or restart of the computers affected.

15. The system behavior with respect to I&C functionality is entirely defined by the application software. The minimum response times of the system are determined by the cycle times of the processing modules involved if the processing time of the

function diagram / function diagram group modules plus the processing time required for execution of service requests do not exceed the specified cycle time.

ISTec-TÜV Certificate No.: TXS-AUST-1006-03, *TELEPERM XS integration test (AUST-II)*, was issued to document that the system met the 15 criteria listed above. These characteristics are the same as those validated for the software supporting the SVE1 module.

2.2 New SCP2 Communication Processor Module

The designed function of the SCP module is to communicate (exchange data) with the service unit or gateways within a TXS system. The SCP / IM LAx module send and receive the data via the Ethernet protocol IEEE 801.2, *Standard for Local and Metropolitan Area Networks: Overview and Architecture.*

[

]

TÜV Qualification Certificate No. 968/K 110.04/08 was issued for SVE2 module revision 5 demonstrating that the module was qualified by analysis to the specified requirements.

2.3 Revised SL21 Communication Module L2

The TXS Communication module L2 SL21 is designed as an extension board for the SVE2 processing module. It is used in combination with the SVE2 as the basic module. Two different applications are provided:

[

]

TÜV Qualification Certificate No. TXS-HW-PZ06 was issued for the revised SL21 module demonstrating that the module was qualified by analysis to the specified requirements.

2.4 New SHO1 Optical Transceiver Module Revision

The SHO1 module is an optical transceiver used to connect Data Terminal Equipment to a TXS Ethernet LAN (H1) via a fiber optic cable. The only usage of the SHO1 is in the Monitoring and Service Interface, where it converts the SCP2 Ethernet for transmission over fiber optic cable.

The type test program included function testing (worst case scenario), environmental, seismic, and EMC testing as specified by:

- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*
- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 2, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The test program included:

- Environmental tests - The environmental tests were performed in accordance with the guidance of EPRI TR-107330.

- Seismic tests - Two different seismic tests were performed: one in accordance with the KTA 3503 requirements the other in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility) tests - The SHO1 is an OEM product manufactured by Hirschmann. The OEM preformed EMI/RFI tests with the Transceiver (i.e., radiated emission tests, radiated and conducted immunity tests, burst test, and electrostatic discharge tests). The test levels for the tests are given in the EN 50082-2 standard, which is comparable to the EPRI TR-102323, Revision 2, requirements.

The new SHO1 module is a commercial product that is dedicated for nuclear use by AREVA NP (GmbH). No separate TÜV qualification certificate was issued for the new module, since it was not designed by AREVA NP.

2.5 Revised SLLM L2 Link Modules

The TXS SLLM L2 link module is designed for use in optical PROFIBUS field bus networks on the TXS system. It converts electrical PROFIBUS interfaces (i.e., RS 485 level) to optical PROFIBUS interfaces and vice versa.

The original TÜV Qualification Certificate No. 945/K 735/97 issued for the SLLM module is still valid and demonstrates that the module was qualified by test to the specified requirements.

2.6 New S466 Analog Input Module Version

The design function of the TXS analog input module S466 is to collect the analog input signals at the front plug and convert these signals to digital signals, which will be provided at the back plane bus.

These changes required a complete type test program. The type test program included functional testing under worse case environmental stress, seismic, and EMI/RFI tests as specified by:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*
- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The test program included:

- Environmental tests – The environmental tests were performed in accordance with the guidance of EPRI TR-107330.
- Seismic tests – The seismic tests were performed in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility and power surge withstand capability) tests - The EMC tests were designed to qualify the new S466 module in accordance with EPRI TR-102323, Revision 1.

TÜV Qualification Certificate No. TXS-HW2-PZ466-2004A was issued for the new S466 module version demonstrating that the module was qualified by test to the specified requirements.

2.7 New SRB1 Relay Module

The design function of the SRB1 is to convert signals from the 24V signal level to an application required signal level. The contact level is galvanic isolated from the coil (24V signal) level.

The SRB1 Relay Module is a new TXS component and is used for the Oconee RPS/ESPS project. The type test program included functional testing under worse case environmental stress, seismic, and EMI/RFI tests as specified by:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*
- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The test program included:

- Environmental tests – The environmental tests were performed in accordance with the guidance of EPRI TR-107330.
- Seismic tests – The seismic tests were performed in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility and power surge withstand capability) tests - The EMC tests were designed to qualify the new SRB1 module in accordance with EPRI TR-102323, Revision 1.

TÜV Qualification Certificate No. 968/K 736/04 was issued for the new SRB1 module demonstrating that the module was qualified by test to the specified requirements.

2.8 New SAA1 Analog Signal Module

The design function of the SAA1 module is to provide current to voltage converter.

The SAA1 Analog Signal Module is a new TXS component and is used for the Oconee RPS/ESPS project. The type test program included functional testing under worse case environmental stress, seismic, and EMI/RFI tests as specified by:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*

- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The test program included:

- Environmental tests – The environmental tests were performed in accordance with the guidance of EPRI TR-107330.
- Seismic tests – The seismic tests were performed in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility and power surge withstand capability) tests - The EMC tests were designed to qualify the new SAA1 module in accordance with EPRI TR-102323, Revision 1.

TÜV Qualification Certificate No. 968/K 740/99 was issued for the new SAA1 module demonstrating that the module was qualified by test to the specified requirements.

2.9 New SNV1 Analog Signal Module

The design function of the SNV1 module is to multiply one analog input signal to four output signals. The input signal could be a voltage or a current signal. The SNV1 provide a galvanic isolation between the input and the outputs and to the power supply.

The SNV1 Analog Signal Module is a new TXS component and is used for the Oconee RPS/ESPS project. The type test program included functional testing under worse case environmental stress, seismic, and EMI/RFI tests as specified by:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*
- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The test program included:

- Environmental tests – The environmental tests were performed in accordance with the guidance of EPRI TR-107330.
- Seismic tests – The seismic tests were performed in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility and power surge withstand capability) tests - The EMC tests were designed to qualify the new SAA1 module in accordance with EPRI TR-102323, Revision 1.

TÜV Qualification Certificate No. 968/K 740/99 was issued for the new SAA1 module demonstrating that the module was qualified by test to the specified requirements.

2.9 New SNV1 Analog Signal Module

The design function of the SNV1 module is to multiply one analog input signal to four output signals. The input signal could be a voltage or a current signal. The SNV1 provide a galvanic isolation between the input and the outputs and to the power supply.

The SNV1 Analog Signal Module is a new TXS component and is used for the Oconee RPS/ESPS project. The type test program included functional testing under worse case environmental stress, seismic, and EMI/RFI tests as specified by:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*
- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The test program included:

- Environmental tests – The environmental tests were performed in accordance with the guidance of EPRI TR-107330.
- Seismic tests – The seismic tests were performed in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility and power surge withstand capability) tests - The EMC tests were designed to qualify the new SNV1 module in accordance with EPRI TR-102323, Revision 1.

TÜV Qualification Certificate No. 968/K 105.00/01 was issued for the new SNV1 module demonstrating that the module was qualified by test to the specified requirements.

2.10 New SBG3 Subrack

[redacted]

The SBG3 Subrack is used for the Oconee RPS/ESPS project. The type test program included functional testing under worse case environmental stress, seismic, and EMI/RFI tests as specified by:

- IEEE Std 323-1983, *IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Systems*
- IEEE Std 344-1975, *IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generation Stations*

- EPRI TR-107330, *Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants*
- EPRI TR-102323, Revision 1, *Guidelines for Electromagnetic Interference Testing in Power Plants*

The test program included:

- Environmental tests – The environmental tests were performed in accordance with the guidance of EPRI TR-107330.
- Seismic tests – The seismic tests were performed in accordance to the IEEE Std 344-1975 and followed the guidance of EPRI TR-107330.
- EMC (EMI/RFI susceptibility and power surge withstand capability) tests - The EMC tests were designed to qualify the new SBG3 module in accordance with EPRI TR-102323, Revision 1.

[ ]

The addition testing and analysis for the SBG3 rack is summarized in AREVA NP document 66-501 5893-03, *TELEPERM XS Supplemental Equipment Qualification Summary Test Report*, which was submitted to NRC as item 20 in LAR Supplement 1.

3. Software Changes

The TXS software changes made since the TXS Topical Report was submitted to NRC are outlined on the following pages. The information is organized by software release. This organization best illustrates both the chronology of the changes as well as the breadth of changes associated with each release. The summary of the software changes was taken from the product information summary document prepared for each software release.

Each qualified (online) TXS software module change was made in accordance with the high quality development process described in part a above. The development process for the qualified components of the TXS system platform included comprehensive verification and validation activities by AREVA NP GmbH, as well as by an external appraisal of the development and test results by independent test institutes: Gesellschaft für Anlagen- und Reaktorsicherheit (German Society for Plant Safety and Reactor Safety known as GRS), Institut für Sicherheitstechnologie (Institute for Safety Technology known as ISTec), and Technischer Überwachungs-Verein (German Technical Inspection Agency known as TÜV).

The development process for the qualified components of the TXS system platform included comprehensive verification and validation (V&V) activities by the manufacturer, as well as by an external appraisal of the development and test results by test institutes (GRS, ISTec, and TÜV). The V&V activities which are performed during development comprise:

- Reviews of the development documentation and test specifications
- Module tests of the vital software components – Testing included a regression test and a test of the implemented modifications. All possible branches within the function to be tested are executed in this process. The major part of the functionality of the software can be verified with this test. Exceptions to this include direct hardware accesses as well as interactions between the individual software components.
- Code inspections - A code inspection of the complete source code was performed for the runtime environment (the central software component) to ensure that the modifications which were integrated into RTE were implemented correctly. For other software components, which had minor changes, a code inspection of the modified sections was performed.
- Functional tests of the software components - A component test was performed for all modified software components on the target system. The main emphasis of these tests was to check the adaptation for the SVE2 as well as the modified functionality. These tests also included checks of direct hardware accesses. For the software components which were not modified, selected regression tests were performed which proved compatibility with SVE2.

The development process for the qualified components of the TXS system platform included comprehensive V&V activities by the manufacturer, as well as by an external appraisal of the development and test results by test institutes (GRS, ISTec, and TÜV). The modified software modules were subjected to an external qualification test by ISTec and/or the TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety Systems in Nuclear Power Stations*

A qualification certificate was issued by the test institute for each new version of the qualified software modules demonstrating that the modules were qualified by test to the specified requirements.

Beside qualified software modules, releases of the TXS software also contained non-safety related software modules. These include tools other than the TXS code generating tools.

Functional expansions and changes to the non-safety related software tools have been tested internally by means of developer's tests as well as integration tests performed in the course of the release preparation. Those tests focused on the effectiveness of the modifications introduced into the tools as well as on the applicability of the tools for their purpose in the engineering process or for TXS monitoring/service activities.

Change requests concerning non-safety (offline) software and tools have been handled in accordance with AREVA NP GmbH procedure FAW-TXS 1.5, *Configuration Management.* TXS tools have proven themselves by the experience gained from the engineering, project V&V and operation of several TXS application projects. Suitability of tools has also been assessed and certified by external experts in the course of the plant-independent system test.

3.1 Release 2.33 of the TXS Software for Windows NT and for HP-UX (October 1999)

This release modified the Code Generators and other support software modules to make minor enhancements and error corrections.

Qualified (Safety-Related) Software Modules

Code Generator FDGM

[ ]

The development process for Code Generator FDGM included comprehensive V&V activities by the AREVA NP GmbH. The modified software module was subjected to an external qualification test by GRS and ISTec. The implemented modifications were

evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety Systems in Nuclear Power Stations*

The GRS-ISTec qualification certificate was issued for Code Generator FDGM version 2.30 issued with TXS software release 2.33 demonstrating that the module was qualified by test to the specified requirements.

Code Generator Runtime Environment (RTE)

[ ]

The development process for Code Generator RTE included comprehensive V&V activities by the AREVA NP GmbH. The modified software module was subjected to an external qualification test by ISTec. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety Systems in Nuclear Power Stations*

The ISTec qualification certificate was issued for Code Generator RTE version 2.30 issued with TXS software release 2.33 demonstrating that the module was qualified by test to the specified requirements.

Other (Non-Safety Related) Software Modules

[ ]

3.2 Release 2.34 of the TXS Software for Windows NT and for HP-UX (October 1999)

This release modified support software modules to make minor enhancements and error corrections.

Qualified (Safety-Related) Software Modules

No Changes

Other (Non-Safety Related) Software Modules

[redacted]

3.3 Release 2.35 of the TXS Software for Windows NT and for HP-UX (December 1999)

This release modified support software modules to make minor enhancements and error corrections.

Qualified (Safety-Related) Software Modules

No Changes

Other (Non-Safety Related) Software Modules

[redacted]

3.4 Release 2.36 of the TXS software for Windows NT and HP-UX (May 2000)

This release 2.36 modified Function Blocks, added English language versions of the Function Block definitions and SPACE forms. Minor extensions and error corrections were made to other support software modules.

Qualified (Safety-Related) Software Modules

Function Blocks: FB

[

]

The development process for Function Block Library software modules included comprehensive V&V activities by the AREVA NP GmbH. The new and modified Function Block modules were subjected to an external qualification test by GRS and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety-Systems in Nuclear Power Stations*

The GRS-TÜV qualification certificate was issued for Function Blocks version 2.21 issued with TXS software release 2.36 demonstrating that the module was qualified by test to the specified requirements.

Function Block definition (English language version)

- The function blocks are generally equipped with German texts. FB definitions (English) are now available in the form of scripts which exchange the German texts against English ones in project databases. These scripts are not subjected to a type-test. The exchange is performed by means of the database administration tool *dbadmin.*

Database Definition of the Forms for SPACE

- The SW component 'forms' has been extended by scripts which exchange the German texts in the forms against English ones and reverse in a project database. The exchange is performed by means of the database administration tool *dbadmin.*

Other (Non-Safety Related) Software Modules

Qualified (Safety-Related) Software Modules

No Changes

Other (Non-Safety Related) Software Modules

3.6 Release 2.38 of the TXS-Software for Windows NT and for HP-UX (March 2001)

The release provides five extensions (with six new FBs), two optimizations, and two error corrections to the Function Block library. The release also provides error corrections and extensions to five support software modules.

Qualified (Safety-Related) Software Modules

Function Blocks: FB

The development process for Function Block Library software modules included comprehensive V&V activities by the AREVA NP GmbH. The new and modified Function Block modules were subjected to an external qualification test by GRS and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety-Systems in Nuclear Power Stations*

The GRS-TÜV qualification certificate was issued for Function Blocks version 2.30 issued with TXS software release 2.38 demonstrating that the module was qualified by test to the specified requirements.

Other (Non-Safety Related) Software Modules

[redacted]

[

]

3.7 Release 2.38A for Windows NT and for HP-UX (July 2001)

The release provides two error corrections and one optimization to software component Alphanumeric Service Monitor. Moreover, the application notes on the *sms* should be observed (section 2.2).

Qualified (Safety-Related) Software Modules

No Changes

Other (Non-Safety Related) Software Modules

[

]

3.8 Release 2.38B for Windows NT and for HP-UX (April 2002)

This release extends the TXS function block library with an additional block S-PID (PID step controller).

Qualified (Safety-Related) Software Modules

[

]

The development process for Function Block Library software modules included comprehensive V&V activities by the AREVA NP GmbH. The new Function Block module was subjected to an external qualification test by GRS and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety-Systems in Nuclear Power Stations*

The GRS-TÜV qualification certificate was issued for Function Blocks version 2.32 issued with TXS software release 2.38B demonstrating that the module was qualified by test to the specified requirements.

Other (Non-Safety Related) Software Modules

No Changes

3.9 Release 2.38C for Windows NT and for HP-UX (June 2002)

This release provides a new version of the Function Blocks with an improved block K-PID (PID controller) and a new version of the mic file analyzer tool *scanmic*.

Qualified (Safety-Related) Software Modules

Function Blocks: FB

The development process for Function Block Library software modules included comprehensive V&V activities by the AREVA NP GmbH. The modified Function Block modules were subjected to an external qualification test by GRS and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety-Systems in Nuclear Power Stations*

The GRS-TÜV qualification certificate was issued for Function Blocks version 2.33 issued with TXS software release 2.38C demonstrating that the module was qualified by test to the specified requirements.

Other (Non-Safety Related) Software Modules

3.10 Release 3.0.2 of the TXS Software (November 2003)

The release addresses the necessary adaptations to the online software and tools for the SVE2. These software module changes are described in the discussion of SVE2 hardware change. Additional changes to address minor errors or enhancements were included with the release and are described below.

Note: Releases 3.0.0 and 3.0.1 were developmental releases.

Qualified (Safety-Related) Software Modules

Function Blocks: FB

[ ]

The development process for the Function Block Library software modules included comprehensive V&V activities by the AREVA NP GmbH. The new and modified Function Block modules were subjected to an external qualification test by ISTec and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety Systems in Nuclear Power Stations*

The ISTec-TÜV qualification certificate no. 0122527623H/1 Revision Na was issued for Function Blocks version 2.50 issued with TXS software release 3.0.2 demonstrating that the module was qualified by test to the specified requirements.

Other (Non-Safety Related) Software Modules

[redacted]

[

]

3.11 Release 3.0.3 of the TXS Software (November 2003)

This release contains one error correction and two optimizations.

Qualified (Safety-Related) Software Modules

Firmware H1-CP

[

]

The modified firmware for H1-CP was subjected to an external qualification test by ISTec. The implemented modifications were evaluated and their correct

implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 60880-1986, *Software for Safety-Systems in Nuclear Power Stations*

The ISTec qualification certificate was issued for Firmware H1-CP version 6.21 issued with TXS software release 3.0.3.

Other (Non-Safety Related) Software Modules

[ ]

3.12 Release 3.0.4 of the TXS Software (January 2004)

The new release contains four new function blocks.

Qualified (Safety-Related) Software Modules

Function Blocks: FB

[ ]

The development process for the Function Block Library software modules included comprehensive V&V activities by the AREVA NP GmbH. The new and modified Function Block modules were subjected to an external qualification test by ISTec and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition
- IEC Std. 880-1986, *Software for Safety-Systems in Nuclear Power Stations*

The ISTec-TÜV qualification certificate was issued for Function Blocks version 2.60 issued with TXS software release 3.0.4.

Other (Non-Safety Related) Software Modules

No Changes

3.13 Release 3.0.5 of the TXS Software for LINUX (May 2004)

The only difference between the new release and its predecessor is that it contains an extended version of the Graphical Service Monitor Client.

Qualified (Safety-Related) Software Modules

No Changes

Other (Non-Safety-Related) Software Modules

[ ]

3.14 Release 3.0.6 of the TXS Software for LINUX (May 2004)

The main improvements in the new release over the previous version are the function block expansions. These expansions require small modifications in the *fde* editor environment. In the *sveload* and *L2cpconfig* programs, a dependency on libraries has been corrected. The Service Monitor Tool was made an optional software package.

Qualified (Safety-Related) Software Modules

Function Blocks: FB

The development process for the Function Block Library software modules included comprehensive V&V activities by the AREVA NP GmbH. The modified Function Block modules were subjected to an external qualification test by ISTec and TÜV. The implemented modifications were evaluated and their correct implementation (including the tests) checked. The type test program was based on the following standards:

- KTA 3503, *Type Testing of Electrical Modules of the Reactor Protection System,* November 1986 edition

- IEC Std. 880-1986, *Software for Safety-Systems in Nuclear Power Stations*

The ISTec-TÜV qualification certificate was issued for Function Blocks version 2.61 issued with TXS software release 3.0.6.

Other (Non-Safety Related) Software Modules

[ ]

Release 3.0.7 of the TXS Software under LINUX (May 2005)

Qualified (Safety-Related) Software Modules

No Changes

Other (Non-Safety Related) Software Modules

[ ]

Release 3.0.7A of the TXS Software under LINUX (August 2005)

Qualified (Safety-Related) Software Modules

No Changes

Other (Non-Safety Related) Software Modules

[ ]