RAI 61: *Provide further description and details that demonstrating how the testing performed on the AV42 achieves the same results as described by the Communications interim staff guidance.*

Topical Report ANP-10273P and previous RAI responses imply that the AV42 has been 100 percent tested. However, the testing as described in RAI-29 is described as decomposition testing of subfunctions that had little interaction with each other. DI&C-ISG-04, "Highly Integrated Control Rooms – Communications Issues," Section 2, describes 100 percent testing, as intended by the interim staff guidance, to mean that every possible combination of inputs and every possible sequence of device states is tested, and all outputs are verified for every case. In order to verify that the testing performed on the AV42 meets the same objective of the 100 percent testing described in the interim staff guidance, the staff would need a comparison of the AV42 testing to the testing described in the interim staff guidance, and the basis for why any differences between the two testing methods would meet the intent of the interim staff guidance (i.e., demonstration of error-free software).

Response to RAI-61:

1.0 Approach

Taking into account the number of input signals and the fact that AV42 uses in the Programmable Logic Device (PLD) based logics several memory functions, a100% combinatory testing of the PLD logic and of all its internal states is practically not possible. However, regarding the structure of the logic, consisting of sub-functions with interfaces of limited complexity and limited number of signal exchanges, an adequate degree of test coverage is achieved.

The qualification testing (in addition to the developer tests performed during the design phase) was defined taking into account this decomposition into subfunctions.

Figure 61-1 provides an overview of the overall structure of the functions implemented in the PLD, and Figure 61-2 through Figure 61-7 show the logics implemented in a simplified way, so as to give an understanding of the interactions of the subfunctions.

Testing of the AV42 was performed with the module installed in a test machine which allows:

- commands to be sent via the Profibus interface and all check-back information read via the Profibus interface.
- binary input signals to be sent to all pins of the module.
- all binary output signals to be read and recorded from the module's pins.

Testing is controlled by a test software which performs every test case as a sequence of steps where:

- (in every step) one or several input signals change their value.
- All expected outputs are specified, read back and the observed values are compared to the expected ones.

- Testing is in general performed automatically, and automatically recorded so as to ensure that the test can be reproduced.
- For a few steps, manual intervention is necessary (e.g. placing simulation pins; reading LED values, disconnecting the load relay to verify the open circuit monitoring function).

Test cases have been defined either with focus on the functions of the PLD (safety functions of the module), or with focus on the drive control and drive monitoring functions.

2.0 Overview diagrams for the logic of the PLD

Figure 61-1—Overview of the function blocks of the AV42 logics in the PLD

Figure 61-2—Priority handling between simulation commands and between safety I&C commands

Figure 61-3—Processing of check-back signals and overlapping test logics

Figure 61-4—Priority between operational I&C and desktile commands (simplified; "non-safety processing" of desktile commands in the microprocessor not shown)

Figure 61-5—Processing of torque check back signals

Figure 61-6—Command output and command termination (principles)

Figure 61-7—Command output and command termination (taking into account some termination options through parameters TRQSF, ONTL, OFFTL)

[ ]

3.0 Signal names, pin assignment, signals with special consideration for qualification testing

[ ]

4.0 Overview of the test cases

A large number of test cases have been specified and executed in the course of the qualification program of the AV42 module. The test cases dedicated to the qualification testing of VA42 together with TÜV Rheinland as independent assessor have been specified in TÜV Rheinland reports as test specifications, and results referenced in the TÜV test reports. The test cases are in detail specified in the programming of the test computer, and documented in an additional description document. The descriptions and explanations below are based on these documents (see detailed references, answers to RAI-76), a description of the test program ("Beschreibung AV42-V8B.SIE. Prüfprogramm für die AV42 Funktionsprüfung mit ERBUS und SIETAL (description of the test program for AV42 function testing with ERBUS and SIETAL). AREVA NP GmbH, internal note (154 pages, German language)), and the test program itself.

The test cases written in italics have been specified and executed in the course of theoretical and practical qualification testing with independent assessors from TÜV Rheinland, and are mainly dedicated to the safety functions in the PLD.

The other test cases have been executed in the course of practical qualification testing in addition to the scope specified for the qualification testing of the safety functions. The tests focus on drive control and drive monitoring functions implemented in the AV42's microprocessor. Since all commands pass through the PLD, PLD functions are included in these tests.

5.0 Test cases with focus on the PLD's functions

RAI 70: *Describe in detail the procedures and methods used to address manual verification of automatic testing.*

DI&C-ISG-04, "Highly Integrated Control Rooms – Communications Issues," Section 2, calls for manual verification of automatic testing.

Response to RAI-70:

Input signals as specified in the test program and the expected module responses are translated into EXCEL tables, by the independent assessors from TÜV Rheinland.

The test program, along with the ERBUS test machine, is then executed test step by test step. For each of these test steps, the outputs of the AV42 module are visually examined and entered in the EXCEL table for comparison with the expected outputs.

This table is part of the test documentation and test logs are recorded at TÜV Rheinland.

RAI 71: *What technical aspects does the German standard KTA 3503 cover in relationship to the AV42?*

The standard KTA 3503 was mentioned in the AVERA NP topical report ANP-10273P as one of quality standards that involve safety requirements that the AV42 satisfied.

Response to RAI-71:

The KTA 3503 Standard "Type Testing of Electrical Modules for the Safety Related Instrumentation and Control System" specifies:

- the process for type testing as method for qualifying I&C modules
- the documents to be submitted to the independent assessor involved in the type testing procedure (test specification; critical load analysis; reliability data respectively failure rate calculation etc.)
- the type of practical tests to be performed:
  - Visual inspection
  - Function tests, focused on the module's functions
  - EMC tests
  - Climatic tests
  - Mechanical / seismic tests
  - Criteria for function monitoring to be applied during the environmental tests, and for intermediate function tests between individual tests
- Minimum number of test specimen to be used (3)
- The procedure how to handle faults / failures during the tests
- Scope of test documentation.

The document is enclosed for your review.

RAI-76: *Provide on the docket (as proprietary) the test plan, test results, and test reports, not already requested, that support the logic testing of the PLD.*

The staff will use these documents to evaluate the sufficiency of the testing performed on the AV42.

Response to RAI-76:

Test specifications related to the logic testing of the AV42 functions focused on the testing the PLD functions are:

1. Prüfspezifikation für die praktische Prüfung der Vorrangbaugruppe AV42 des Systems TELEPERM XS der Firma Framatome ANP GmbH. TÜV Rheinland report 968/K 102.01/02 (2002-06-26) (73 pages, German language).
2. Documentation of theoretical and practical testing in accordance with KTA 3503 of priority module AV42 in the TELEPERM XS system from Framatome ANP GmbH. TÜV Rheinland test report 968/K 102.00/02 (2002-06-26) (51 pages).
3. Prüfspezifikation für die Änderungsprüfung der Vorrangbaugruppe AV42-8AA des Systems TELEPERM XS der Firma AREVA NP GmbH (Test specification for the assessment of modifications of the module AV42-8AA). Test report TÜV Rheinland 968/K 102.09/07 (2007-04-26) (17 pages, German language).
4. Assessment on the amendments to priority module AV42-8AA of the TELEPERM XS system of AREVA NP GmbH. Test report TÜV Rheinland 968/K 102.10/07 (13 pages, translation of the test report in German language).
5. Prüfspezifikation für die Änderungsprüfung der Vorrangbaugruppe AV42-8BA bzw. –CA des Systems TELEPERM XS der Firma AREVA NP GmbH (Test specification for the assessment of modifications of the module AV42-8BA and -8CA]. Test report TÜV Rheinland 968/K 102.07/07 (2007-05-29) (41 pages, German language).
6. Dokumentation der theoretischen und praktischen Prüfung nach KTA 3503 der Vorrangbaugruppe AV42-8BA des Systems TELEPERM XS der Firma AREVA NP GmbH (Documentation of theoretical and practical testing according to KTA 3503 of the priority module AV42-8BA). TÜV Rheinland report 968/K 102.08/07 (2007-05-29) (51 pages, German language).
7. Dokumentation der theoretischen und praktischen Prüfung nach KTA 3503 der Vorrangbaugruppe AV42-8CA des Systems TELEPERM XS der Firma AREVA NP GmbH (Documentation of theoretical and practical testing according to KTA 3503 of the priority module AV42-8CA]. TÜV Rheinland report 968/K 102.11/07 (2007-08-20) (35 pages, German language)
8. Beschreibung AV42-V8B.SIE. Prüfprogramm für die AV42 Funktionsprüfung mit ERBUS und SIETAL (description of the test program for AV42 function testing with ERBUS and SIETAL). AREVA NP GmbH, internal note (154 pages, German language).

The documents listed above are not available in English; however, the response provided in RAI 61 is a narrative of the test methods and processes called out in these documents in order to fully test the AV42 module. The information contained in the documents provides no additional significant information relative to the testing as described in RAI 61. This response combined with the technical documents provided in previous submittals represent a comprehensive technical basis for NRC approval of the AV42 module as a safety related component of the TXS System Platform. These documents and the RAI responses submitted to the staff support a reasonable assurance positive safety determination for the AV42 module as relates to relevant Regulatory Guidance, IEEE standards and NRC Regulations.

As additional evidence of the effective implementation of the quality processes used in the design and testing of the TXS system, AREVA has included excerpts from an NRC vendor inspection conducted at our Erlangen Facility, March 10-14, 2008. The inspection concluded that the design, configuration management, testing and procurement processes for the overall TXS system, which includes the AV42 module, are sound as indicated in NRC Inspection Report 99901371/2008-201.

U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NEW REACTORS
DIVISION OF CONSTRUCTION INSPECTION AND
OPERATIONAL PROGRAMS

VENDOR INSPECTION REPORT

Report No: 99901371/2008-201

Organization: AREVA-NP GmbH

Paul-Gossen-Strasse 100
91001 Erlangen, Germany

Vendor Contact: Mr. Hans-Joachim Nisslein, QEM Liaison Officer

AREVA-NP GmbH
Paul-Gossen-Strasse 100
91001 Erlangen, Germany
email: Hans-joachim.Nisslein@areva.com

Nuclear Industry: AREVA-NP GmbH (AREVA) is a world-wide supplier of digital I&C systems for use in safety-related and nonsafety-related applications for commercial nuclear power plants.

Inspection Dates: March 10-14, 2008

Inspection Team Leader: Greg S. Galletti, DCIP/NRO

Inspector: Juan Peralta, DCIP/NRO

Inspector: Milton Concepcion, DCIP/NRO

Inspector: Mario Gareri, DE/NRO

Observer: Mr. Stefan Schielke, from the German Federal Ministry for the Environment, Nature Conservation, and Nuclear Safety (BMU)

3.1 DESIGN CONTROL

c. Conclusions
The inspectors concluded that AREVA design control program requirements are consistent with the regulatory requirements of Criterion III of Appendix B to 10 CFR Part 50. Based on the limited sample of TXS platform and application design, CM, and testing documentation reviewed, the inspectors determined that the AREVA design control procedures were being effectively implemented.

3.2 PROCUREMENT CONTROL

c. Conclusions
The inspectors concluded that the AREVA procurement control program requirements

are consistent with the regulatory requirements of Criterion IV, “Procurement Document Control,” of Appendix B to 10 CFR Part 50. Based on the limited sample reviewed, the inspectors also determined that the AREVA QEM and associated procurement control procedures were being effectively implemented.

3.3 CONTROL OF PURCHASED MATERIAL EQUIPMENT AND SERVICES

c. Conclusions
Except for the issue identified as Nonconformance 99901371/2008-201-01, the inspectors concluded that the AREVA program requirements are consistent with the regulatory requirements of Criterion VII, “Control of Purchased Equipment, Material, and Services,” of Appendix B to 10 CFR Part 50. Based on the limited sample reviewed, the inspectors also determined that the AREVA QEM and associated procurement control procedures were being effectively implemented.

3.4 NONCONFORMANCE AND CORRECTIVE ACTIONS

c. Conclusions
Except for the examples identified in Nonconformances 99901371/2008-201-02 and 99901371/2008-201-03, the inspectors concluded that the AREVA control of nonconformances and corrective action program requirements are consistent with the regulatory requirements of Criterion XV, “Nonconforming Materials, Part, or Components,” and Criterion XVI, “Corrective Action,” of Appendix B to 10 CFR Part 50. Based on the limited sample reviewed, the inspectors determined that the AREVA QEM and associated nonconformance and corrective action procedures were being effectively implemented.

3.5 10 CFR PART 21 PROGRAM

c. Conclusions
Except for the issue identified in Violation 99901371/2008-201-01, the inspectors concluded that the AREVA 10 CFR Part 21 program requirements are consistent with the regulatory requirements.

4.2 PARTIAL LIST OF PERSONNEL CONTACTED

Dr. Patrick Weber	Senior Vice-President I&C and Electrical Systems, AREVA
Dr. Steffen Richter	Director I&C Development, AREVA
Dr. Wolfgang Michel	Director Quality Management and Processes, AREVA
Hans-Joachim Nisslein	QEM Liaison Officer, AREVA
Tom Nickel	QEM Engineer, AREVA
Arthur Gottschick	Quality Engineer, AREVA
Stefan Frauenknecht,	Quality Engineer, AREVA
Pete Heisenstein	Test Bay Leader, AREVA
Mark Milo Manager	I&C Quality, AREVA
Vic Fregonese	U.S. EPR Technical Manager, AREVA

4.3 OBSERVER

Mr. Stefan Schielke, from the German Federal Ministry for the Environment, Nature Conservation, and Nuclear Safety, participated as an observer of the AREVA inspection.

Documents reviewed related to the AV42 Module, items 2-4 previously submitted:

1. Teleperm XS AV42 Priority Module 01-1007841-00 1.0 02-06
2. Engineering Information Record 51-5052273-00 2004-10-20
3. Summary Test Report (STR) 66-5065211-00
4. Teleperm XS AV42 Priority Module 01-1007841-00
5. PACS-SCPSSA-PS-HBS-SA I&C 2007-08-22

RAI-80: *Explain the connection and interaction between the PLD and the watchdog timer output from the PLD.*

The response to RAI-08 provided information on watchdog timers, however the discussions of April 16, 2008 indicated that additional interactions with the PLD had not been identified by the RAI response that left some unanswered concerns.

Response to RAI-80:

The response indicated in RAI-08 describes the complete interaction of the watchdog timer and the PLD.

[ ]

RAI-82: *Explain what types of information (i.e. programs, runtime parameter types, passwords, etc. rather than exact individual items) are stored in the non-volatile memory of the microprocessor verses what types of information are read from the back-plane connector parameters and what, if any, information is uploaded into RAM or "runtime memory" on initialization or network initialization.*

As part of the verification that the non-safety portion will not interfere with the safety function, a clear understanding is needed on what the microprocessor depends upon when it validates a network message received and any susceptibility of the designed, approved, and tested microprocessor program being changed by any run-time network action.

Response to RAI-82:

The microprocessor stores in its non-volatile memory (Flash-memory) the following information, in three separate zones:

- the executable runtime code.
- software parameters used by runtime code, which are exclusively used and needed by the microcontroller (and not by the PLD). This comprises all parameter settings exclusively used for actuator monitoring, and used for those actuator control functions performed by the microcontroller. Examples are:
  - Parameters for runtime monitoring: enabled/disabled; monitoring time.
  - Type of checkback contact for motor temperature monitoring.
  - Type of checkback contact for ON/OPEN and OFF/CLOSED checkback (the same information, for processing in the PLD, is also provided by a hardwired parameterization pin).
  - Parameters for creation of change-of-state signaling via the Profibus: signaling may be selected on or off.
  - Preferred status of the AV42 outputs on interruption of the Profibus.
  - Log of state changes in the form of time-tagged data, for diagnostic purposes. This is only done if these data cannot be transmitted because the AV42 is operated without connection to the Profibus, or if the Profibus link is interrupted.

The executable runtime code is fixed in the EPROM, and cannot be modified via the Profibus.

The software parameters are downloaded to the microcontroller through the Profibus interface, and then stored in the nonvolatile memory in their specific memory segment.

The code is executed from the Flash memory. Software-parameters which are derived from the value of the parameterization pins (e.g. the Profibus address) are maintained only in RAM.

There are 12 parameter pins on the back-plane connector of the AV42. Six of these parameters are directed to the PLD, and the other six are directed to the Profibus Micro-controller. These parameters are set on the backplane of the cabinet at the female connector. If an AV42 is removed and replaced with a different AV42 module, the parameters will remain the same. The newly installed AV42 module will take on the same parameters via the backplane.

[ ]

RAI-83: *What happens if a cyclic command network message, coming into the microprocessor, suddenly stops before the command is actually completed?*

As part of the verification of that the non-safety portion will not interfere with the safety function, a clear understanding and assurance is needed that even if the microprocessor program locks up or is in a "long wait", the safety function can be performed.

Response to RAI-83:

The physical layer controller makes the Profibus message available to the microcontroller. It fills an incomplete or inconsistent message with zeroes (check performed based on checksum). This is then considered as a failure of the Profibus link. The failure is signaled by the microcontroller (hardwired binary signal), and the default command assigned to the failure of the Profibus link is issued by the microcontroller to the PLD (this default command may be specified by parameterization: "stay as is"; "On/open", "Off/close").

If, as a worst case assumption, the microcontroller locks up, the watchdog will initiate a reset of the Profibus controller, and operation will start again with proper initialization.

PLD operation is not affected by any of these states of the microcontroller, and will continue to perform processing of the various inputs with the appropriate priorities. Inputs from the microcontroller are not needed to perform the safety functions.

RAI-85: *When the AV42 is initially powered up, what state do the non-basic logic components (registers, flip-flops, etc, if any) take and how are these verified to be correct during initial AV42 component and/or module test at the factory? Upon initial power-up of the AV42, will the status of the non-logic components reflect, or need to reflect, the status of various actuation devices that the AV42 may control?*

Again, the regulations require a quality product. This means understanding the basic operations and testing of the AV42.

Response to RAI-85:

[ ]