



April 11, 2013
NRC:13:018

U.S. Nuclear Regulatory Commission
Document Control Desk
11555 Rockville Pike
Rockville, MD 20852

Response to U.S. EPR Design Certification Application RAI 542, Supplement 2

- Ref. 1: E-mail, Getachew Tesfaye (NRC) to Dennis Williford et al., (AREVA NP Inc.), RAI No. 542 (6336), FSAR Ch. 7 – New Phase 4 RAI “U.S. EPR Design Certification Application,” March 15, 2012.
- Ref. 2: E-mail, Dennis Williford (AREVA NP Inc.) to Amy Snyder (NRC), RAI No. 542 (6336), FSAR Ch. 7 – New Phase 4 RAI, Supplement 1, “Response to U.S. EPR Design Certification Application,” November 29, 2012.
- Ref. 3: Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), ANP-10315P, “U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report,” Revision 1, NRC:11:061, June 13, 2011.

In Reference 1, the NRC provided a request for additional information (RAI) regarding the U.S. EPR design certification application. The schedule to provide the Response to Question 07.01-52 was provided in Supplement 1 (Reference 2) on November 29, 2012.

The enclosure to this letter provides a final Response to Question 07.01-52. The enclosure also includes a red line-strikeout format of AREVA NP Inc. (AREVA NP) Technical Report ANP-10315P (submitted in Reference 3), which supports the Response to Question 07.01-52.

AREVA NP considers some of the material contained in the enclosed to be proprietary. As required by 10 CFR 2.390(b), an affidavit is attached to support the withholding of the information from public disclosure. Proprietary and non-proprietary versions of the enclosure to this letter are provided.

The following table indicates the respective pages in the enclosure that contain the response provided by AREVA NP to the subject question.

Question #	Start Page	End Page
RAI 542 — 07.01-52	2	9

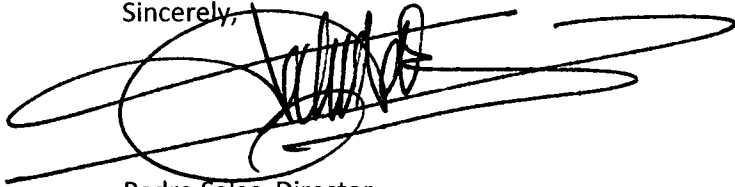
This concludes the formal AREVA NP response to RAI 542. There are no questions from this RAI for which AREVA NP has not provided responses.

AREVA NP INC.

DD77
NRO

If you have any questions related to this information, please contact Len Gucwa by telephone at (434) 832-3466, or by e-mail at Len.Gucwa.ext@areva.com.

Sincerely,

A handwritten signature in black ink, appearing to read 'Pedro Salas', is written over a horizontal line. The signature is somewhat stylized and includes a large circular flourish.

Pedro Salas, Director
Regulatory Affairs
AREVA NP Inc.

Enclosures:

1. Proprietary Response to U.S. EPR Design Certification Application RAI 542, Supplement 2
2. Non-Proprietary Response to U.S. EPR Design Certification Application RAI 542, Supplement 2
3. Notarized Affidavit

cc: A. M. Snyder
Docket 52-020

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:

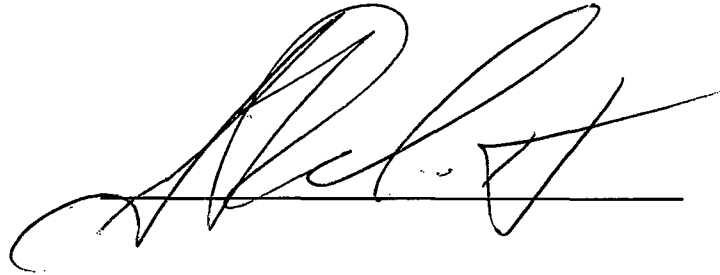
- (a) The information reveals details of AREVA NP's research and development plans and programs or their results.
- (b) Use of the information by a competitor would permit the competitor to significantly reduce its expenditures, in time or resources, to design, produce, or market a similar product or 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 the Document is considered proprietary for the reasons set forth in paragraphs 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.

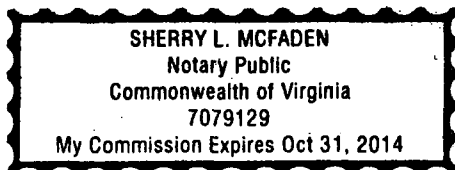
9. The foregoing statements are true and correct to the best of my knowledge, information, and belief.

A large, stylized handwritten signature in black ink, written over a horizontal line.

SUBSCRIBED before me this 11th
day of April 2013.

A handwritten signature in black ink, written over a horizontal line.

Sherry L. McFaden
NOTARY PUBLIC, COMMONWEALTH OF VIRGINIA
MY COMMISSION EXPIRES: 10/31/2014
Reg. #7079129



Response to

Request for Additional Information No. 542, Supplement 2

3/15/2012

U. S. EPR Standard Design Certification

AREVA NP Inc.

Docket No. 52-020

SRP Section: 07.01 - Instrumentation and Controls - Introduction

Application Section: 07.01

**QUESTIONS for Instrumentation, Controls and Electrical Engineering 1
(AP1000/EPR Projects) (ICE1)**

Question 07.01-52:**OPEN ITEM****New Phase 4 RAI**

Provide a consolidated description and diagrams illustrating how the Teleperm XS (TXS) watchdog timer (WDT) would be able to execute the reactor trip function if the Actuation Logic Unit (ALU) processor locks-up. In addition, describe the dependency of the WDT on the ALU software and hardware to perform its functions.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. Clause 5.5 of IEEE Std. 603-1991 requires that the safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Technical Report ANP-10315P, Section 2.2.6.2, addresses the function and operation of the WDT. As currently written, Section 2.2.6.2 does not provide an adequate level of detail on the design function and operation of the WDT. The applicant is requested to provide a detailed description for how the WDT would initiate a reactor trip, in a timely manner, if an ALU function processor experiences a software or hardware-based failure that prevents the ALU function processor from performing its safety function. Specifically, the applicant is requested to provide answers to the following items.

- a. Provide a detailed description within the final safety analysis report or within Technical Report ANP-10315P that clearly explains how the WDT will initiate a reactor trip signal within the Protection System and to verify this action is performed in a timely manner. If the description is provided in Technical Report ANP-10315, provide a pointer in the final safety analysis report to the applicable sections in the report.
- b. Provide a diagram that clearly demonstrates how the WDT interfaces with other TXS function processor components and its reliance upon other components to perform its function.
- c. Provide a logic diagram that demonstrates how the WDT's design configuration facilitates a reactor trip on demand. Specifically, provide a more detailed description and a functional logic diagram that demonstrates how the WDT "hardwired signal" switch off the power supplies of a function processor's I/O modules and how does this lead to a reactor trip signal initiation.
- d. Is the "hardwired signal" used to switch off the affected function processor's I/O power supply the same signal used to initiate the Exception-Handler and are those signals independent of each other?
- e. Describe the impact of an Run-Time Environment software failure on the WDT's operations.
- f. Describe how the WDT's operations are affected once the Exception-Handler is initiated. Specifically, when the applicant states that after a second "exceptional" situation occurs after a reset, which could take as long as five minutes or more, what functions or actions is the WDT performing during the this time frame or during multiple resets of a function processor?
- g. Describe in greater detail the interaction between the Run-Time Environment software with the various types of TXS system hardware components. In particular, describe in

greater detail what hardware components the Run-Time Environment interfaces with (WDTs, LEDs, EEPROMs, Hardware Organizational Tool, etc.) and the method for how this interaction occurs, either directly or indirectly.

Response to Question 07.01-52:

- a. The function of the watchdog timer (WDT) is to provide indication of the loss-of-cyclic operation of the run time environment (RTE), which operates on the SVE2 central processing unit (CPU). The WDT is implemented in separate hardware from the SVE2 CPU.

At the beginning of the processing cycle of the RTE, the local cycle counter is incremented and the watchdog timer is set to a value that is larger (by []) than the activation cycle for the RTEs set in the TELEPERM XS Operating System Software. The hardware WDT must be re-triggered by the RTE software before its expiration. If the software fails to do so, the watchdog times out and a system interrupt signal is generated (called WDG).

When the WDT is activated (i.e., times out) it issues a non-maskable interrupt (NMI) that makes the microprocessor call the exception handler and stop cyclic operation. The exception handler (a special interrupt service) saves the state of the SVE2 CPU (e.g., []) for subsequent analysis and places the SVE2 CPU in a waiting loop (a defined fault state). Activation of the exception handler is indicated by front-plate light emitting diodes (LEDs) on the SVE2 module.

[

] Either method ensures the outputs from the subrack are placed in a safe state, which includes placing the outputs in the trip position for channel reactor trip. This is application-specific hardware circuitry provided outside the TELEPERM XS subrack (see response to Item c for more details).

b. Figure 07.01-52-1 provides an overview of the WDT interfaces.

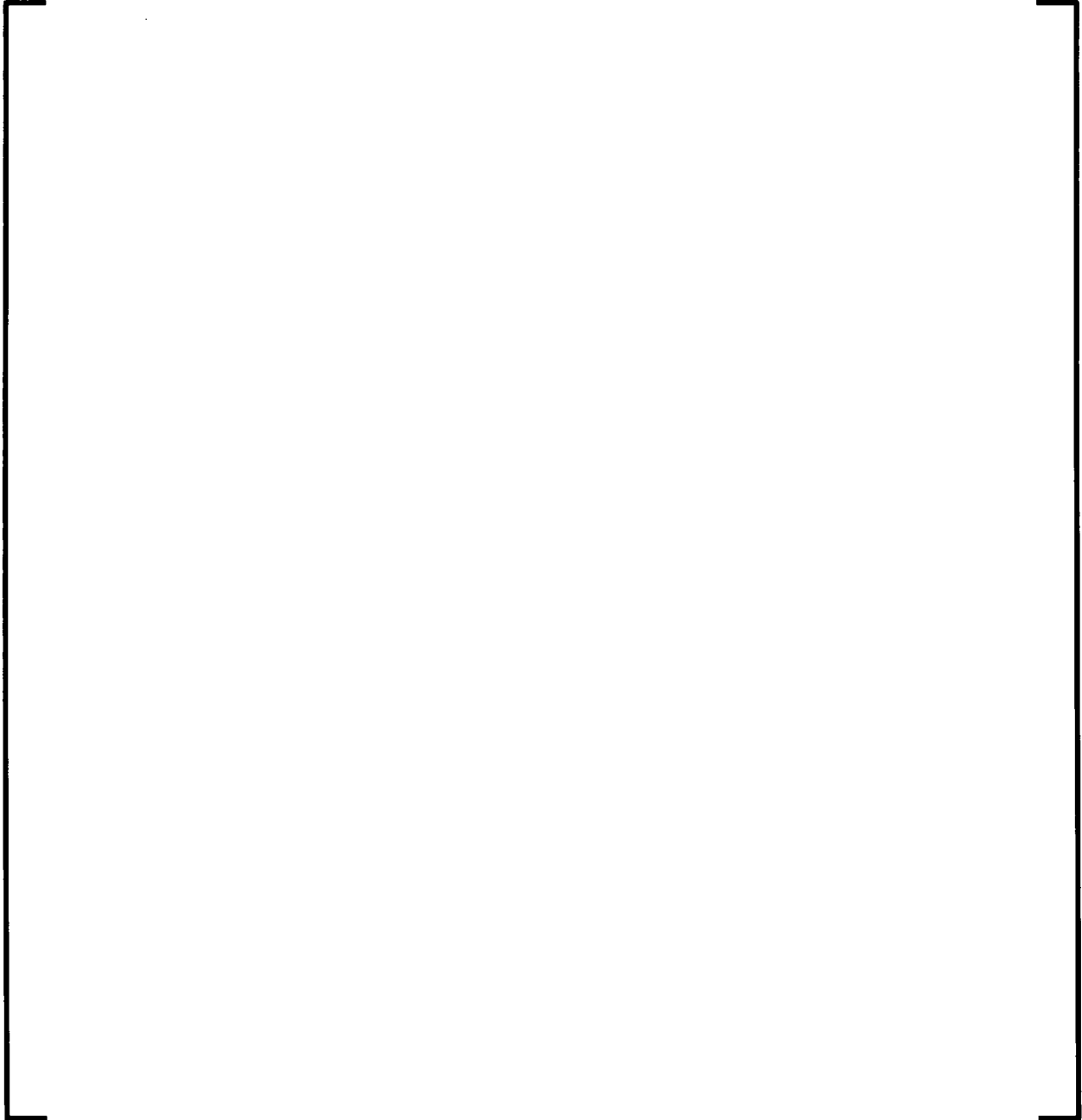


Figure 07.01-52-1: Block Diagram of the SVE2



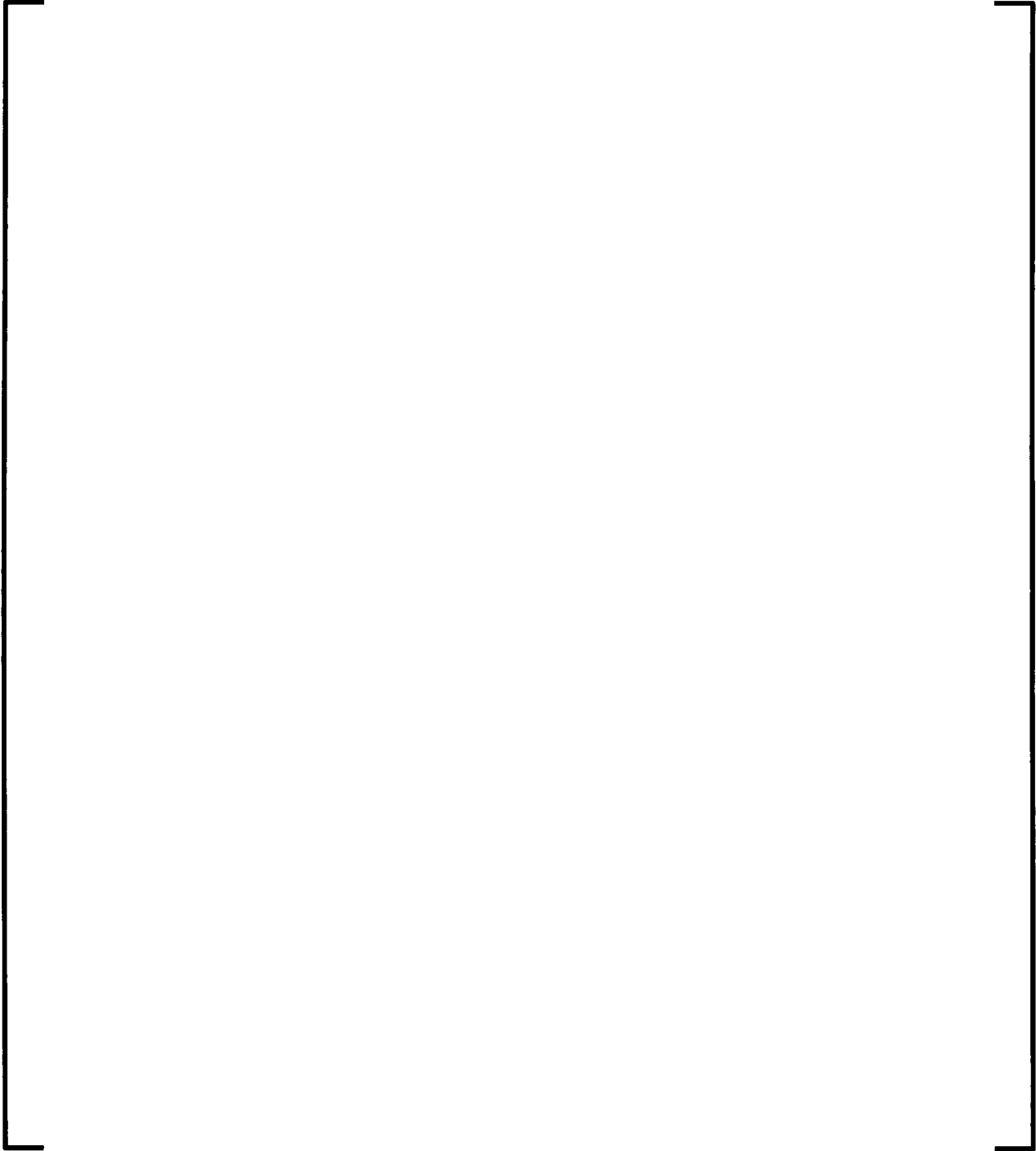


Figure 07.01-52-2: Watchdog Timer Signals on SVE2 Front Panel

- c. As described in the response to Item a, the BASP and WDG signals are used to interrupt the output power supply via a relay operated by the BASP/WDG signal.

The BASP and WDG signals from the front panel connector on the SVE2 module are used to switch off the "ENABLE" signal of the I/O modules. Removing the "ENABLE" signal also cuts the output power supply by using the module-internal electronic switch. This is application-specific hardware circuitry provided outside the TELEPERM XS subrack. This concept is illustrated in the following figures below where the BASP/WDG signal is used to switch off the output module power supply. Figure 07.01-52-3 is for single processor output module. Figure 07.02-52-4 is for a master/checker configuration.



Figure 07.01-52-3: Single Processor Output Board Configuration



Figure 07.01-52-4: Master/Checker Configuration

- d. The watchdog response is used as source for a NMI to the microprocessor of the SVE2 and it is also independently sent to the front connector for use in external circuit designs.
- e. The SVE2 modules are equipped with a hardware watchdog. The monitoring time of the hardware watchdog is defined as the cycle time of the RTE plus [] The hardware watchdog is triggered by the cycle task at the beginning of each RTE cycle. If the software fails to do so, the termination of regular cyclic operation is assumed. The watchdog is activated and indicates the failure by activating the hardwired WDG signal on front connector X4.2 of the SVE2 module, which goes to "low".

The WDG hardware signal is used to signal a processor module failure. It is also used to switch off I/O module power supplies to ensure a defined fail-safe behavior of the affected TELEPERM XS computer, independently from software-based monitoring in the SVE2 processing module.

Additionally, the exception-handler is activated by a hardware exception to initiate a reset or a shutdown of the SVE2. After activation, the exception-handler deactivates all output boards through driver calls. Cyclic communication is stopped.

Switching off the output module power supply through the exception handler is a diverse means to ensure fail-safe behavior of a TELEPERM XS computer. The main means for switching off output power supply is by using the BASP/WDG signal as described in the response to Item b.

- f. If the exception handler is activated by the RTE or a “real” exception the system reaction depends on the elapsed time since the last reset. If the activation happens within a specified period of [] cycles after a reset the SVE2 is shut down (e.g., with 50 millisecond cycle time, the maximum period for exception to trigger shutdown is []), otherwise a reset with automatic restart is performed.

While the exception handler is called/executed, the watchdog is not retriggered. During this time the WDT is not re-triggered and the outputs are placed in a safe state until the reset is complete, as described in responses to Items a, b, and c. While the outputs are in safe state (LOW state), the LED “ERR” on the front panel of the SDO1 module is continuously lit and can be verified by personnel. As soon as the reset is executed (at the end of the exception handler execution), the watchdog is triggered again by the SVE2 software.

- g. The RTE interfaces directly with the SVE2 processor core and local memories. The system section and the bus interface section SVE2 hardware components are indirectly interfaced by the RTE through the processor core and local memories.

The system section comprises the I/O functions (with the exception of the TELEPERM XS backplane bus/interface bus) and the monitoring functions of the SVE2. The I/O functions (i.e., ports, USART, interrupt controller, etc.) and the monitoring functions for multi-processor operation are implemented in an ASIC (i.e., ESSC2). The local sequencer and the swapper are the interface between the system section and the processor. The WDT is a part of the system support controller ESSC2. The LEDs on the front plate of the SVE2 are interfaced by the RTE via the ESSC2.

The activation of the exception-handler is indicated by front-plate LEDs of the SVE2. Also, since the BASP signal is activated, exceptions are indirectly monitored by the cabinet monitoring device.

The bus interface accesses the TELEPERM XS backplane bus. The bus interface is a dual-port random access memory between the system section (local) and the TELEPERM XS backplane bus (global). For communication support several registers are implemented in the bus interface section, which can be addressed locally and partly globally as well.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

ANP-10315 Technical Report Impact:

Section 2.2 and new Figures 2.7, 2.8, 2.9, and 2.10 will be added to Technical Report ANP-10315.

**U.S. EPR™ Surveillance
Testing and TELEPERM XS
Self-Monitoring**

**Technical Report
ANP-10315P**

MARKUPS

List of Figures

Figure 2-1—U.S. EPR PS Testing Philosophy Overview 2-42

Figure 2-2—Sensor Operational Testing Including Black Box Monitoring 2-45

Figure 2-3—Sensor Operational Testing Excluding Black Box Monitoring 2-46

Figure 2-4—APU and ALU Response Time Test 2-48

Figure 2-5 (Sheet 1)—“No-Go” Test Concept 2-49

Figure 2-5 (Sheet 2)—“No-Go” Test Concept 2-50

Figure 2-5 (Sheet 3)—“No-Go” Test Concept 2-50

Figure 2-6—“Go” Test Concept 2-52

Figure 2-7—Block Diagram of the SVE2 2-53

Figure 2-8—Watchdog Timer Signals on SVE2 Front Panel 2-54

Figure 2-9—Single Processor Output Board Configuration 2-55

Figure 2-10—Master/Checker Configuration 2-55

Figure A-1—DAS Testing A-7

RAI 542,
Q. 07.01-52



system via the maintenance laptop.

The test machine only interfaces to the system under test through hard-wired interfaces (24 VDC input and output); therefore, some of the software controls applicable to the maintenance laptop (modifying changeable parameters, issue service request, etc.) are not applicable to the test machine.

Controls for the test machine include the following:

- Storage in physically secure location when not in use.
- Physical access controls to prevent unauthorized individuals from obtaining access.
- Prohibit use for general purpose computing.
- User authorization process.
- Verify that adequate precautions (e.g. patches up-to-date and on demand virus scan) have been taken prior to connecting to the TELEPERM XS system.
- Verify work authorization prior to connecting to the TELEPERM XS system.

2.2.6.22.2.7.2 Hardware Watchdog Timer (Inherent)

The function of the watchdog timer (WDT) is to provide indication of the loss of cyclic operation of the run time environment (RTE), which operates on the SVE2 central processing unit (CPU). The WDT is implemented in separate hardware from the SVE2 CPU.

At the beginning of the processing cycle of the RTE, the local cycle counter is incremented and the watchdog timer is set to a value that is larger (by []) than the activation cycle for the RTEs set in the TELEPERM XS Operating System Software. The hardware WDT must be re-triggered by the RTE software before its expiration. If the software fails to do so, the watchdog times out and an activation signal is generated (called WDG).

↑
RAI 542,
Q. 07.01-52

The WDG hardware signal is used to signal a processor module failure. It is also used to switch off I/O module power supplies to ensure a defined fail-safe behavior of the affected TELEPERM XS computer, independently from software-based monitoring in the SVE2 processing module.

When the WDT is activated (i.e., times out) it issues a non-maskable interrupt that makes the microprocessor call the exception handler (see Section 2.2.7.3) and stop cyclic operation. The exception handler (a special interrupt service) saves the state of the SVE2 CPU (e.g., [

]) for subsequent analysis and places the SVE2 CPU in a waiting loop (a defined fault state). Activation of the exception handler is indicated by front-plate light emitting diodes (LEDs) on the SVE2 module.

[

] This

is application-specific hardware circuitry provided outside the TXS subrack.

The diagram in Figure 2-7 provides an overview of the WDT interfaces.

[

]]

↑
RAI 542,
Q. 07.01-52

L

1

The WDG signal is also made available as a floating signal at the front connector of the SVE2, independent from the microprocessor as shown in Figure 2-8.

~~TXS function processors are equipped with a hardware based watchdog timer. The monitoring time of the watchdog is the cycle time of the runtime environment + 110 millisecond (ms). The hardware watchdog timer must be re-triggered by the runtime environment software before its expiration. If the software fails to do so, an error is assumed and a hardwired signal is used to indicate a processor failure, and to switch off the (input/output (I/O) modules' power supply to verify a defined fail safe behavior of the affected function processor, independently from software based monitoring. Additionally, the exception handler is activated, initiating a specific response (see Section 2.2.6.3).~~

The BASP and WDG signals from the front panel connector on the SVE2 module are used to switch off the "ENABLE" signal of the input/output (I/O) modules. Removing the "ENABLE" signal also cuts the output power supply by using the module-internal electronic switch. While the outputs are in safe state (LOW state), the LED "ERR" on the front panel of the SDO1 module is continuously lit and can be verified by personnel. This is application-specific hardware circuitry provided outside the TXS subrack. This concept is illustrated in Figure 2-9 and Figure 2-10 where the BASP/WDG signal is used to ensure switching off output module power supply.

RAI 542,
Q. 07.01-52

Additionally, the exception-handler is activated by a hardware exception to initiate a reset or a shutdown of the SVE2. After activation, the exception-handler deactivates all output boards through driver calls. Cyclic communication is stopped.

Switching off the output module power supply through the exception handler is a diverse means to ensure fail-safe behavior of a TELEPERM XS computer.

The hardware watchdog timer is periodically tested by the cyclic self-test. For this test, a trip of the watchdog is triggered by the self-test task, and the trip is verified on the associated interrupt signal. The "normal" response to this watchdog-interrupt is blocked for the duration of the test.

RAI 542,
Q. 07.01-52

The activation of the WDT is locally indicated by the exception-handler front-plate LEDs for the impacted SVE2 module and the Cabinet Monitoring Alarm, due to the BASP signal being activated.

2.2.6.32.2.7.3 *Exception-Handler (Inherent)*

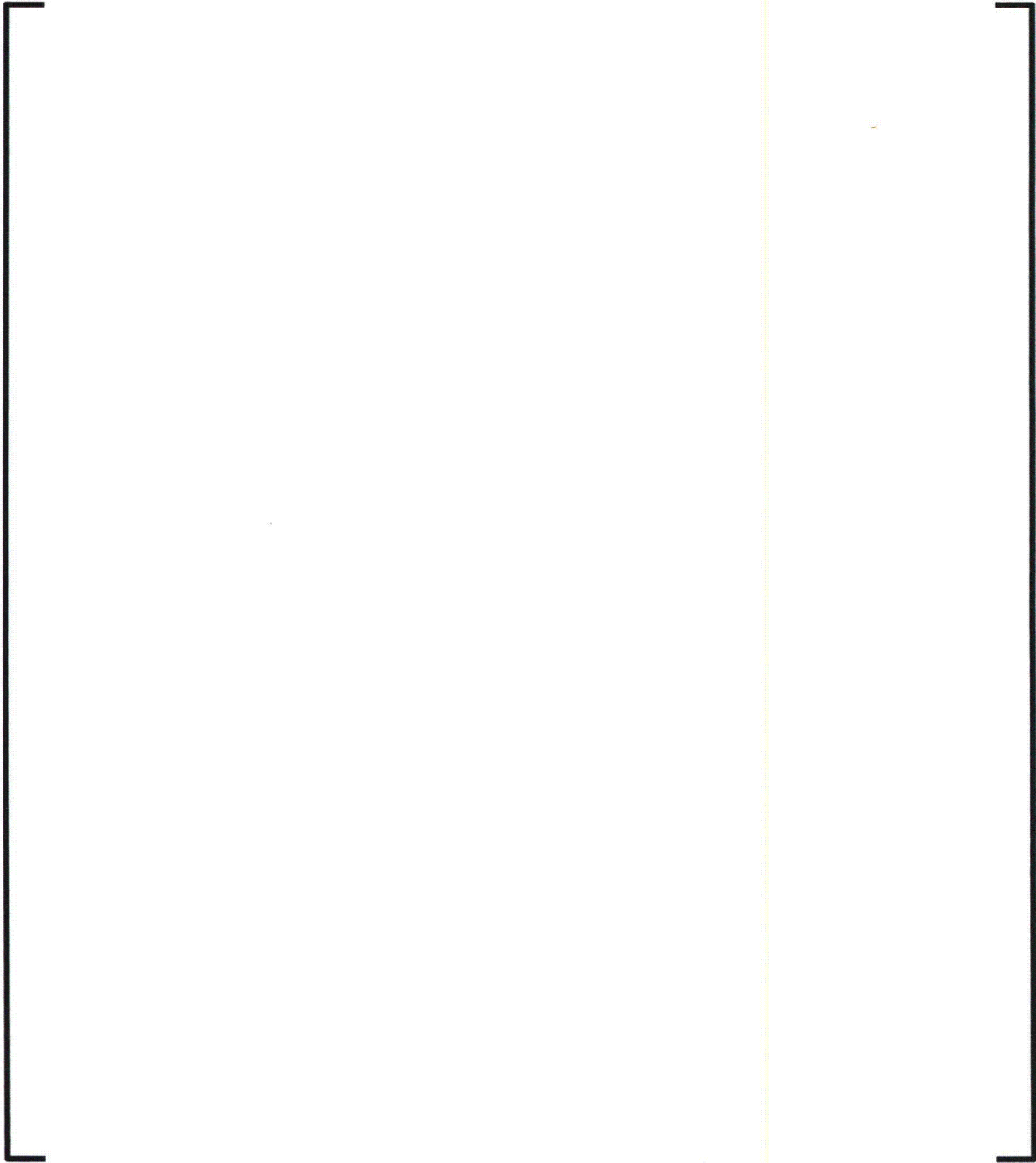
The exception-handler is activated when exceptional situations are encountered during runtime (also in case of a fault detected by the cyclic self-test). After activation, the exception-handler turns off the outputs through driver calls and stops cyclic communication~~deactivates all output boards through driver calls (provides no outputs), and cyclic communication is stopped.~~ Self monitoring result information is saved, which includes: exception type, exception number, exception address, memory dump and stack dump.

Depending on the type of fault, the exception-handler either resets or ~~halts~~the function processor enters a defined fault state and all output signals are set to predetermined safe states. See Technical Report ANP-10309P for information associated with failure states.~~(the processor enters a defined fault state and all output signals are set to predetermined safe states. See Technical Report ANP-10309P for information associated with failure states) the function processor, as indicated.~~ If a second exceptional situation occurs within a specified period after a reset (depends on cycle

RAI 542,
Q. 07.01-52

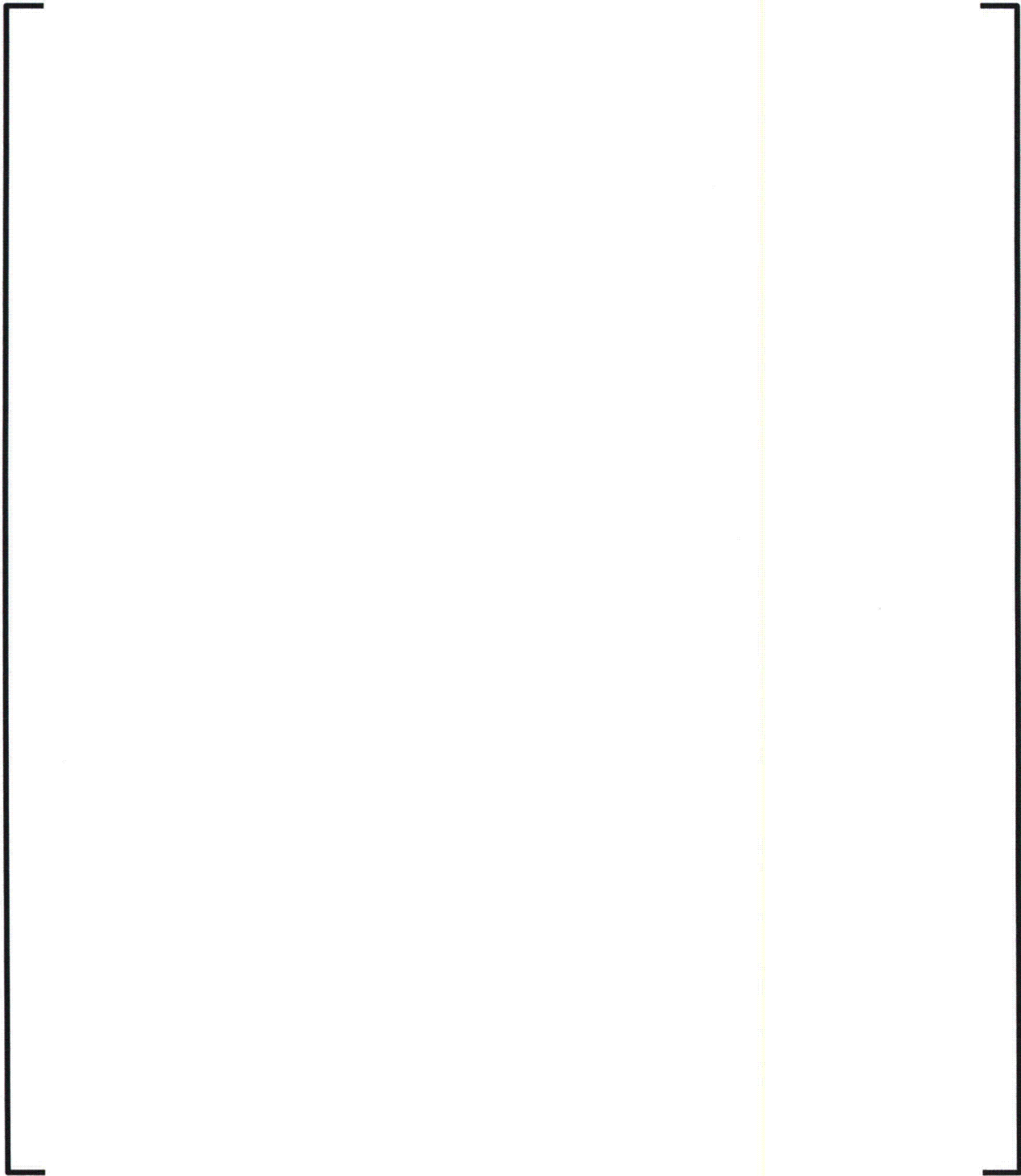


Figure 2-7—Block Diagram of the SVE2



↑
RAI 542,
Q. 07.01-52

Figure 2-8—Watchdog Timer Signals on SVE2 Front Panel



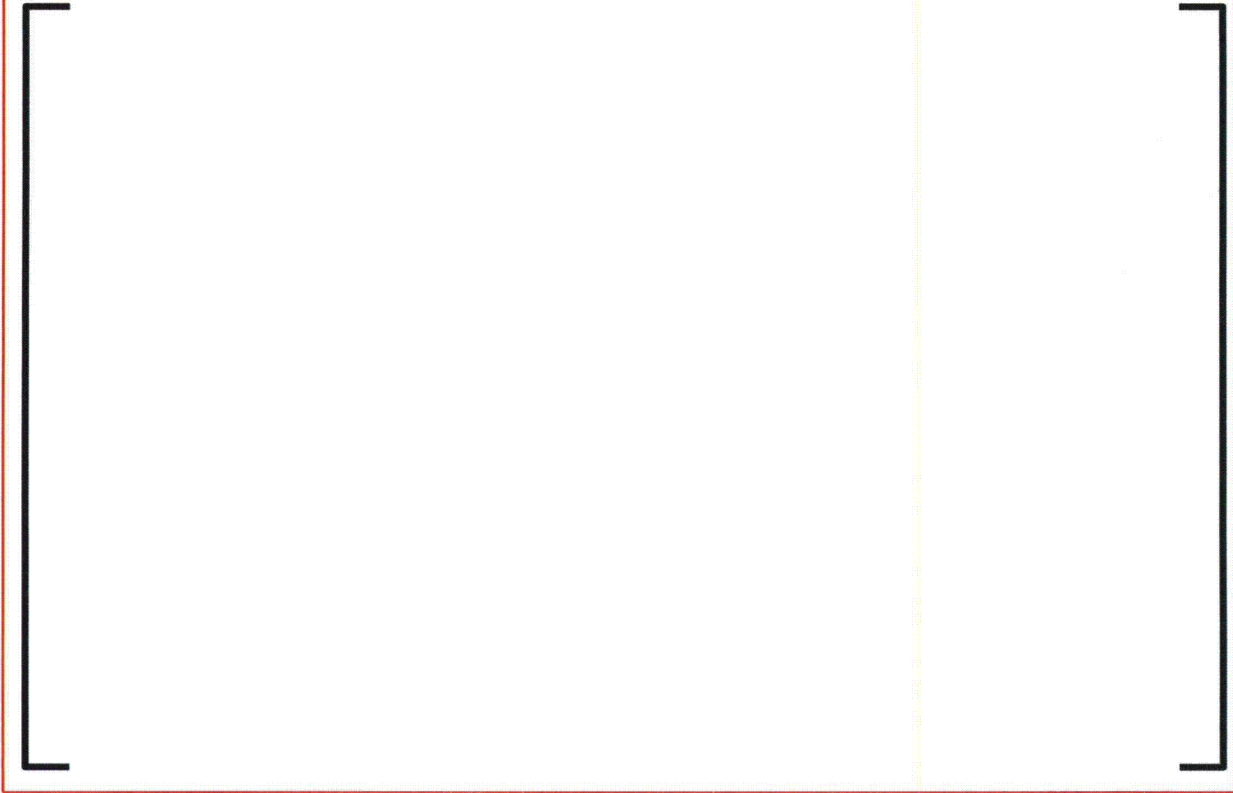
RAI 542,
Q. 07.01-52

Figure 2-9—Single Processor Output Board Configuration



RAI 542,
Q. 07.01-52

Figure 2-10—Master/Checker Configuration



3.0 COMPLIANCE WITH REGULATORY REQUIREMENTS AND CONFORMANCE TO GUIDANCE

RAI 542,
Q. 07.01-52

This section addresses U.S. EPR compliance with regulatory requirements and conformance to guidance relevant to testing provisions for the PS.

3.1 GDC 21 “Protection System Reliability and Testability” [1]

Requirement:

The PS shall be designed to permit periodic testing of its functioning when the reactor is in operation, including a capability to test channels independently to determine failures and losses of redundancy that may have occurred.

4.0 REFERENCES

1. 10 CFR 50 Appendix A, "General Design Criteria."
2. Regulatory Guide 1.22, "Periodic Testing of Protection System Actuation Functions."
3. Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems."
4. Regulatory Guide 1.118, Revision 3, "Periodic Testing of Electric Power and Protection Systems."
5. Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants."
6. NUREG-0800, "Standard Review Plan", BTP 7-17, Revision 5.
7. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."
8. IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems."
9. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
10. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," July 2000.
11. ANP-10309P, Revision 2, "U.S. EPR Digital Protection System Technical Report," May 2011.

12. Technical Report, "TXS Self-monitoring and Fail-safe Behavior from Core-Software Release 3.6.2," PTLC-G/2011/en/0059, Rev. A, 2012-01-20, AREVA NP GmbH.

RAI 542,
Q. 07.01-52