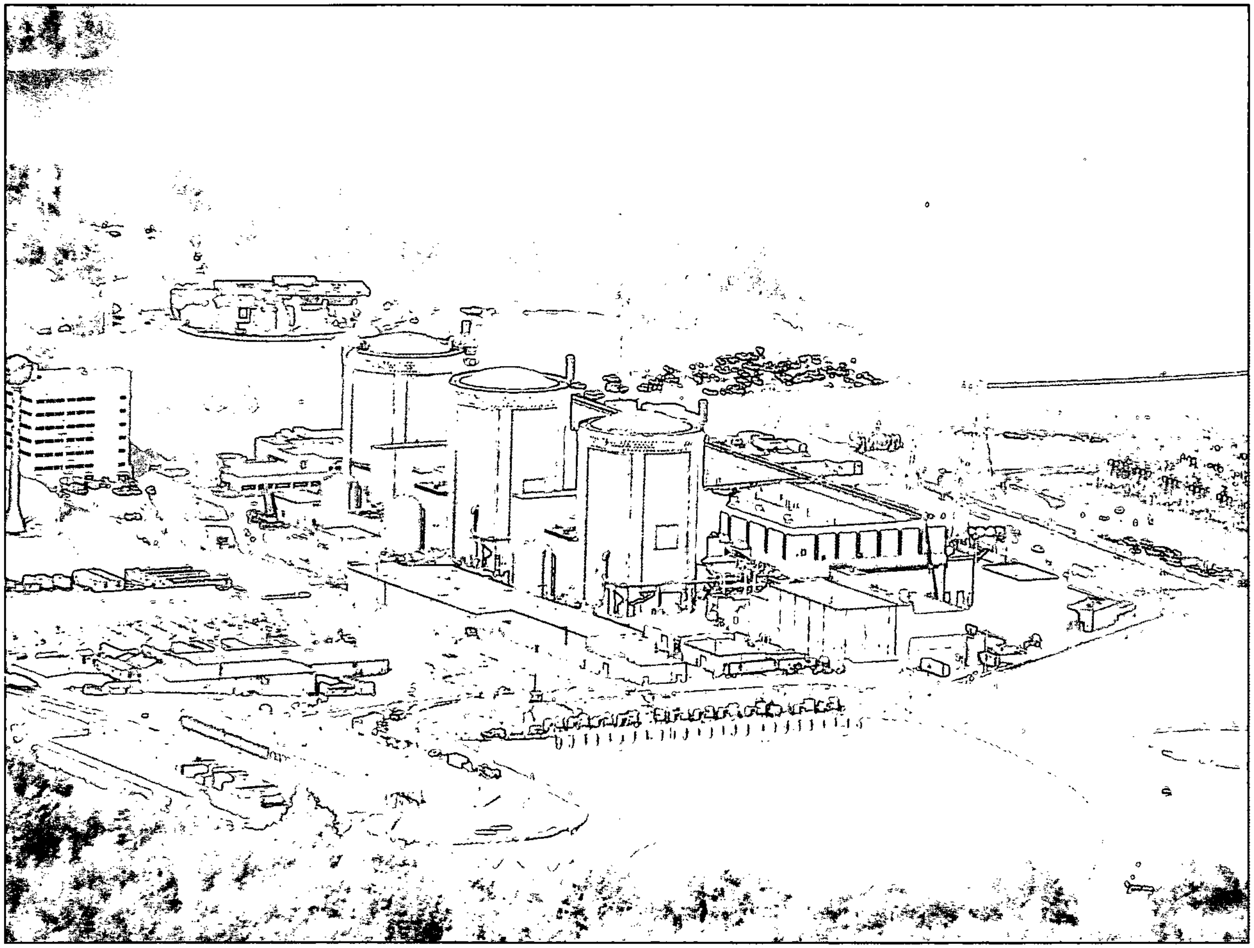
Duke Energy



Oconee Nuclear Station

RPS/ESPS Digital LAR

April 29, 2008

Objectives

- Address NRC concerns on SIVAT tool
- Address NRC concerns on Testing and V&V

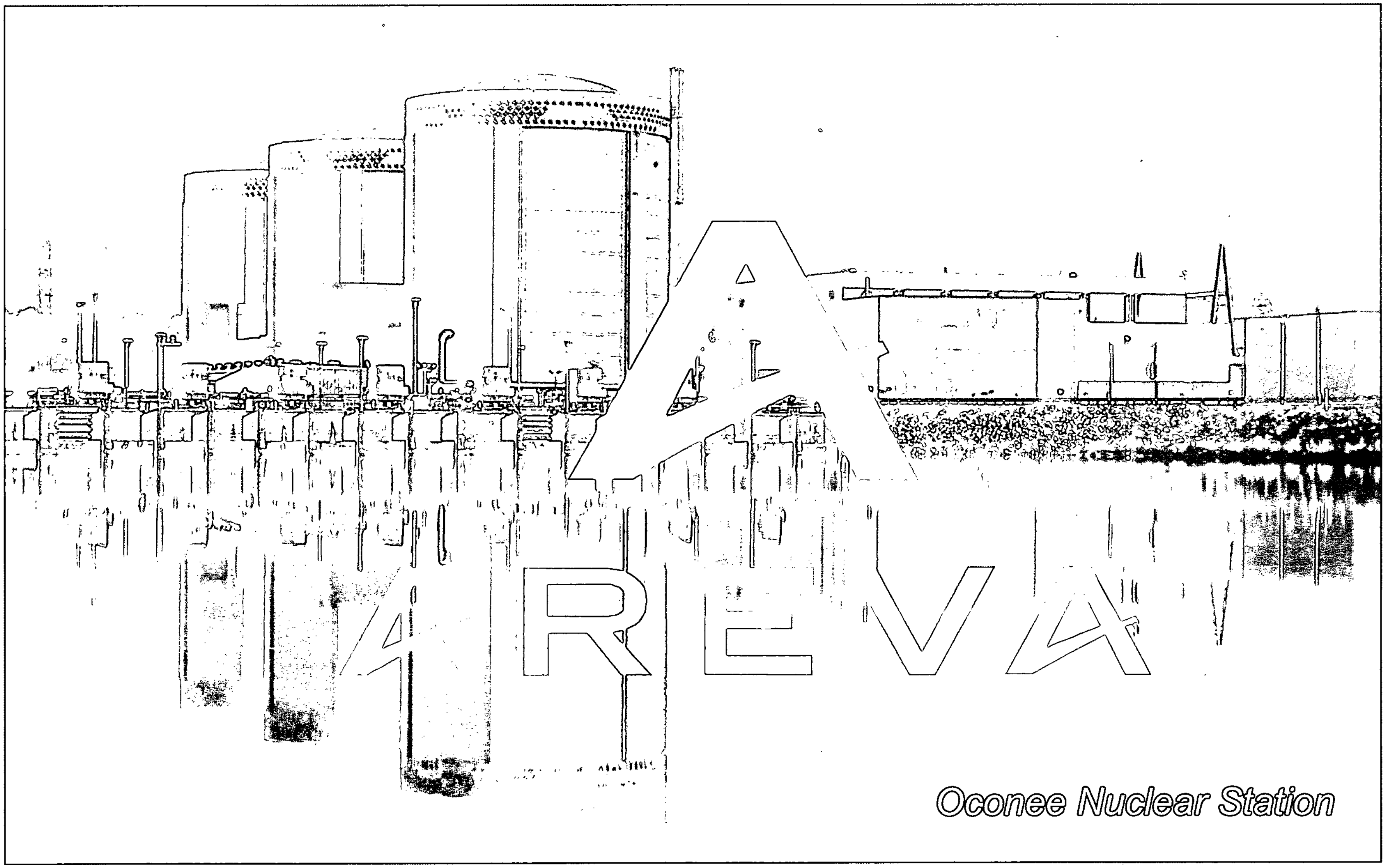
Duke Energy

Agenda

- Qualification of SIVAT Tool for Testing
- Testing and V&V for Oconee RPS/ESPS Project
- SIVAT Demonstration
- Action Items
- Closing Remarks

Duke Energy

Action Items and Closing Remarks



Oconee Nuclear Station

Discussion of TXS Simulation-Based Validation Tool (SIVAT)

Proprietary

Agenda

> Introduction and Background	Mark Burzynski
> TXS Simulation-based Validation Tool	Steffen Richter Andreas Künzel
> SIVAT Documentation	Mark Burzynski
> Closing	

TXS Topical Report
Background Information

> TXS Topical Report describes the simulator-based validation process for TXS application software (Section 2.4.3.3.2).

- □ The simulator validation tool described in the report is SIVAT.
- □ The role of the simulator validation tool in the standard AREVA NP engineering process for TXS project implementation is shown in TXS Topical Report (Figure 2.8).

> The correctness of TXS code generation in the course of application projects is covered by validation activities (i.e., SIVAT and factory acceptance testing).

- □ RETRANS analysis was not considered to be part of the standard TXS engineering process for application software, as noted in the revised response to Software Program Manual RAIs 1 and 53.

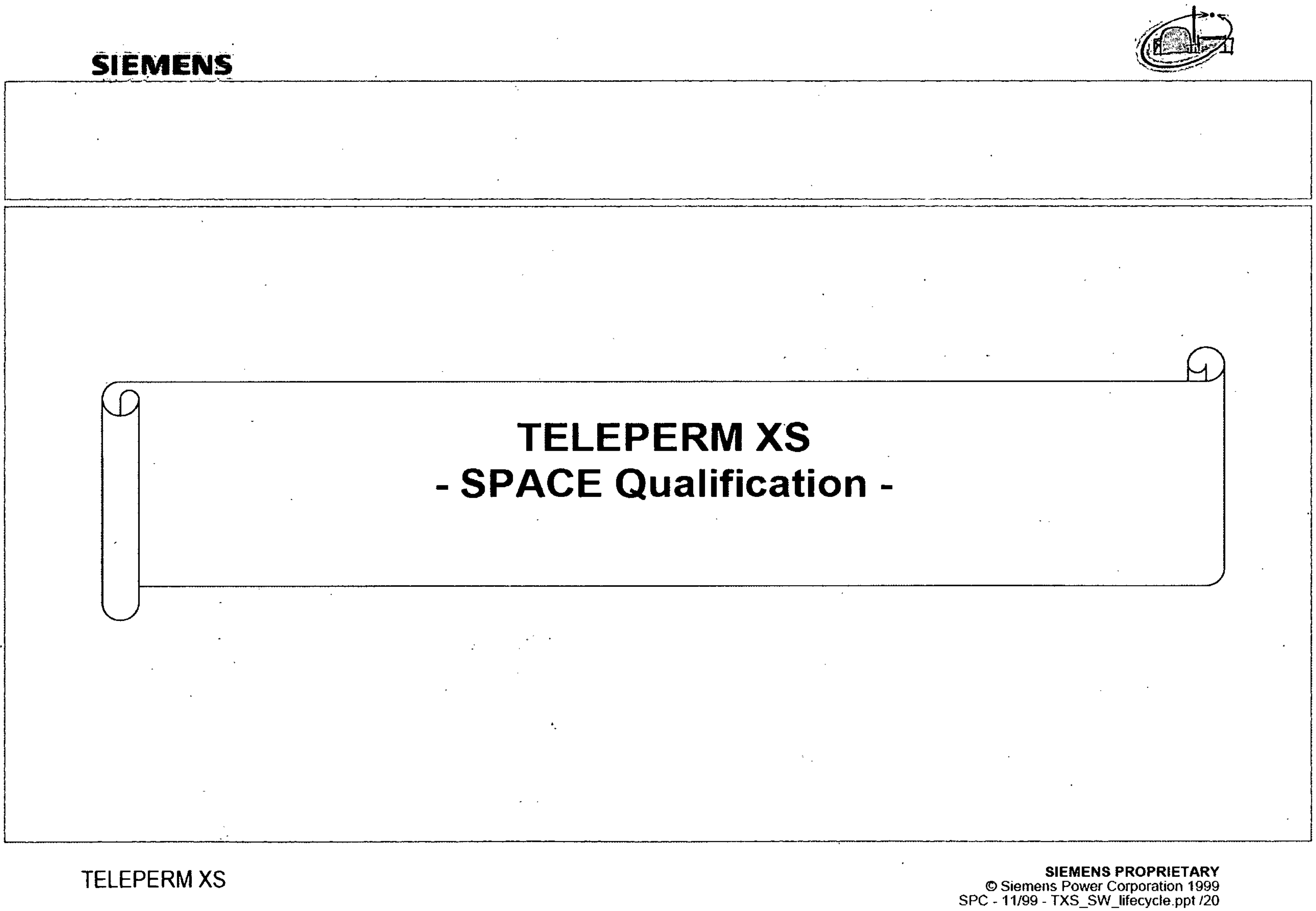
> The TXS Topical Report described generic qualification activities for the TXS SPACE tool automatic code generator (Section 2.4.3.3.3).

- □ RETRANS is the independent code verification tool used in the qualification process of the TXS automatic code generator in the SPACE Tool.

> Discussed during December 19, 2007, NRC audit of the TXS Software Program Manual.

- □ Supported by original 1999 slides from initial meeting with NRC.

TXS Topical Report
Background Information



SIEMENS

TELEPERM XS
- SPACE Qualification -

TELEPERM XS

SIEMENS PROPRIETARY

SPC - 11/99 - TXS_SW_lifecycle.ppt /20

Proprietary

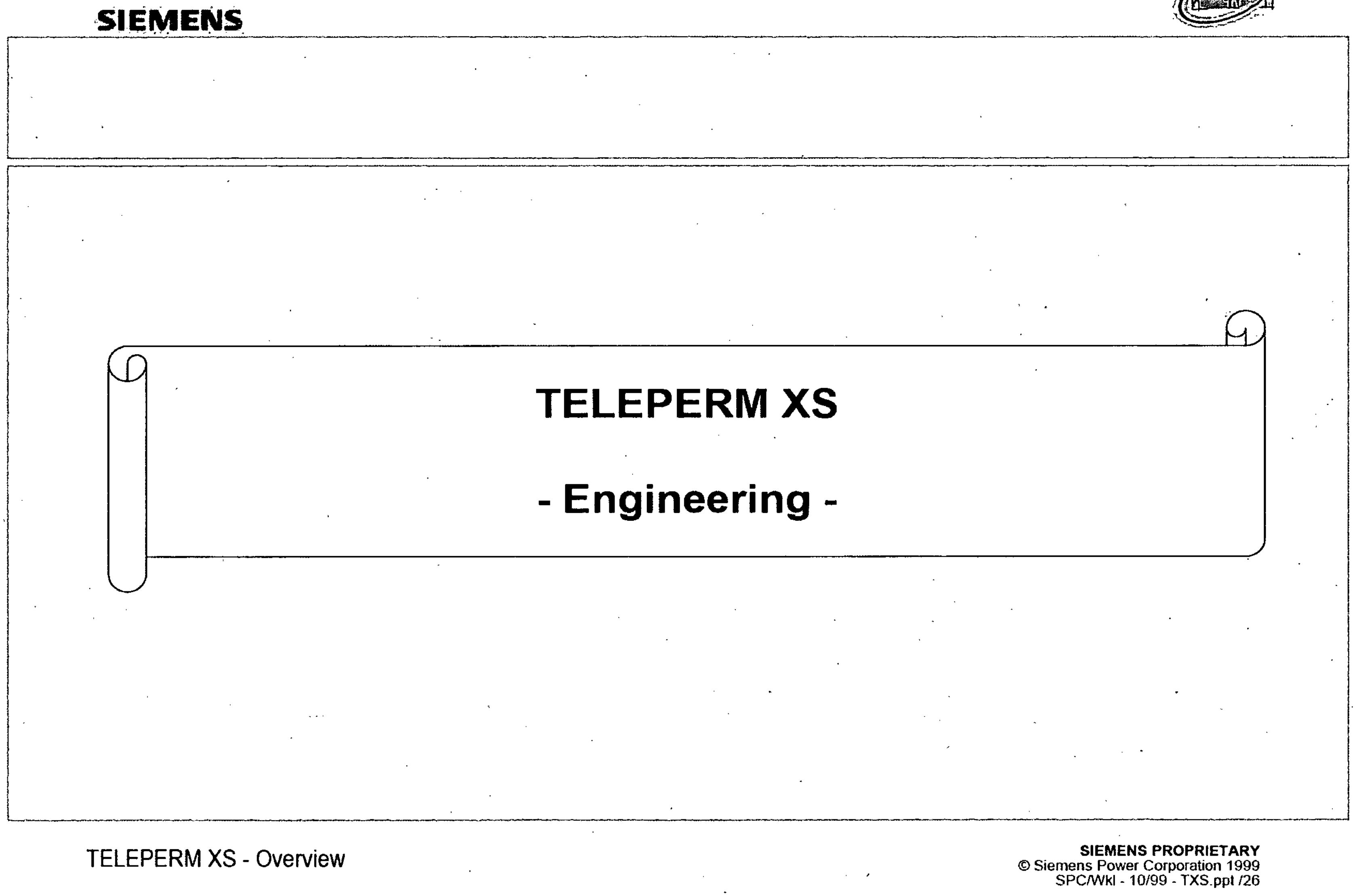
TXS Topical Report
Background Information

AREVA

Proprietary

TXS Topical Report
Background Information

TXS Topical Report
Background Information



SIEMENS

TELEPERM XS

- Engineering -

TELEPERM XS - Overview

SIEMENS PROPRIETARY

SPC/Wkl - 10/99 - TXS.ppt /26

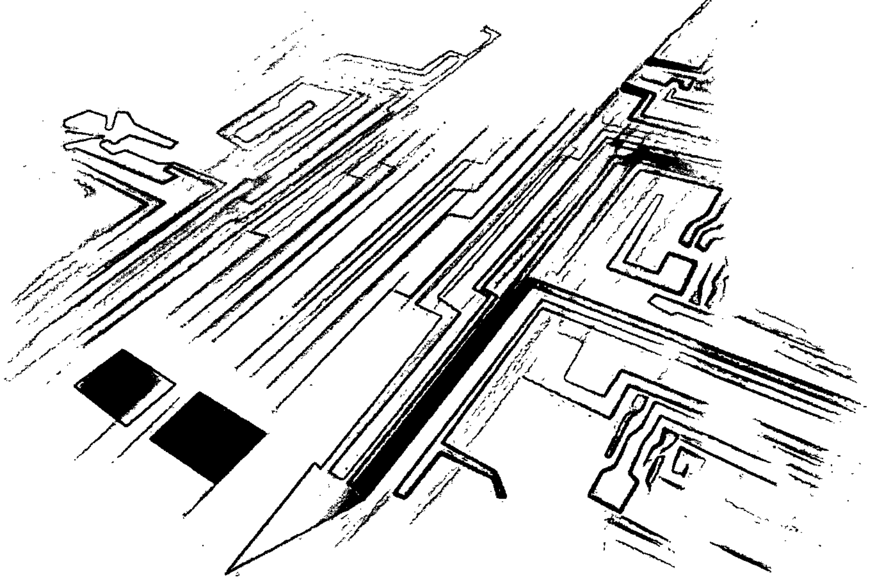
TXS Topical Report

Background Information

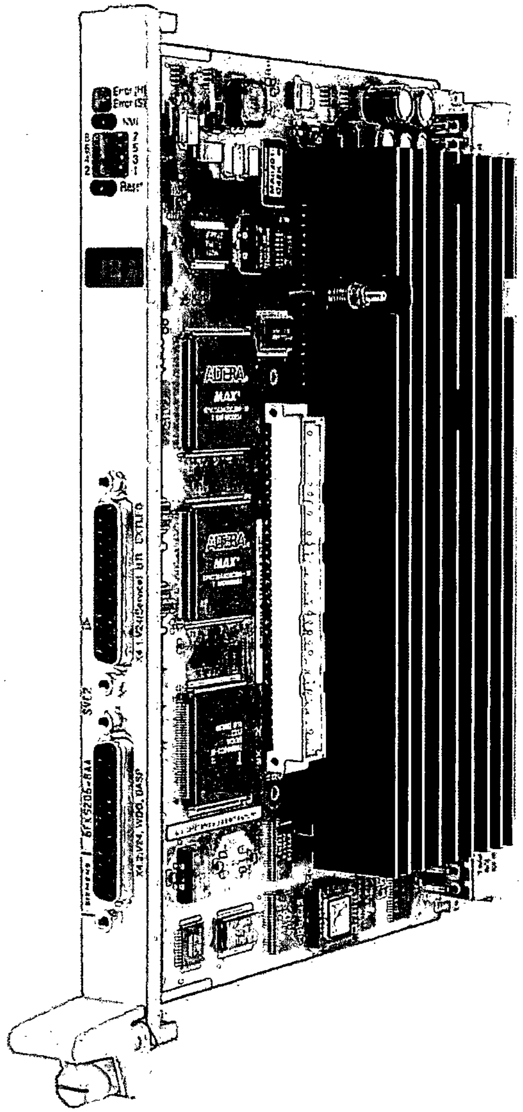
Proprietary

Safety Instrumentation & Control

TELEPERM XS



Simulation-based Validation Tool SIVAT



Purpose of Simulation Testing using SIVAT

> Validation of the application software functionality of a specified TELEPERM XS I&C system

> Verification of the specified I&C system as against the functional requirements

> Early identification of specification errors in order to reduce effort for correction

> Features:

- *Automatic generation of the simulator program*
- *Wide variety of manipulation functions (i.e. built-in malfunctions)*

Proprietary

SIVAT in the TELEPERM XS Engineering Process

AREVA

Proprietary

Two Tasks of SIVAT

Basic Requirements for the TXS SIVAT

> Utilization of a modern simulator control system

> Visibility of all signals and variables (up to 400,000)

> Restart ability by using Initial Conditions (IC)

> No functional changes to the original TXS code

> Simulation of malfunctions for I/O boards, CPU boards and communication bus failure

> Simple including of own models (process, aggregate) (C and FORTRAN modules)

Basic Requirements for the TXS SIVAT (cont.)

> *Easy handling by graphical user interface for the automatic generation and the use of the simulation tool*

> *Script-based simulation (to reconstruct simulation any time)*

> *Interface with the dynamic function diagram logic viewer for monitoring*

> *Creating an individual simulation environment for each project database and user*

> *Running on LINUX workstation or PC (SUSE LINUX distribution)*

> *Short time for generation of the simulator models*

Software Validation by SIVAT Capabilities

- Using the original TXS application C code
- Full-scope function test of application software
- Test of specified parts of the application software
- Test of safety setpoints and safety criteria
- Test of the correctness of specified alarm messages
- Test of system behaviour for assumed failure of individual system components
  - Malfunctions of input signals, CPUs, messages

AREVA

Proprietary

Application of SIVAT
Project References through 2005 (since 1998)

Plant/nuclear power plant	TXS system
Unterweser (Germany)	Reactor control and limitation
Neckarwestheim 1 (Germany)	Reactor control and limitation
Bohunice V1 (Slovakia)	Reactor safety system
Bohunice V2 (Slovakia)	Reactor safety system
Philippsburg 1 (Germany)	Emergency system EKU, local nucleus monitoring LKU and VENO
Research reactor FRM2 (Germany)	Complete safety I&C
Beznau 1 and 2 (Switzerland)	Reactor safety system and control
Tianwan 1 and 2 (China)	Complete safety I&C (incl. Diesel and ventilation facility)
Research reactor AKR2 (Germany)	Complete safety I&C
Biblis B (Germany)	Reactor control and limitation
Biblis A and B (Germany)	Emergency supply steam generator (secondary)
Paks 1-4 (Hungary)	Reactor safety system
Forsmark (Sweden)	Rod control
Oskarsham 1-3 (Sweden)	Neutron flux
Atucha (Argentina)	Reactor safety (second heat sink)
Diverse systems (Germany)	I&C for turbine-generator set (LAT)
Emsland (Germany)	Reactor control
Kozloduy (Bulgaria)	Diesel control, coolant pressure monitoring
Grohnde (Germany)	Power distribution monitoring (LVUE)

Components of SIVAT Tool

AREVA
Proprietary

Generation of the TXS Simulator
Tasks of CATS-SDE

> *Controlling the whole process of generation of the simulator for a certain TXS project data base (SPACE data base)*

- *Starting the TXS code generators fdg-cg / rte-cg*
- *Adding all necessary TXS signals to the simulator database using the SDE-Tool DBE*
- *Adapting application software for each TXS CPU to run under SDE*
- *Automatic generation of special models (optional)*
- *Controlling the compiling and linking of the simulator using the SDE-Tool DBB*

AREVA
Proprietary

Principle of the TXS Simulation

[

]

AREVA

Proprietary

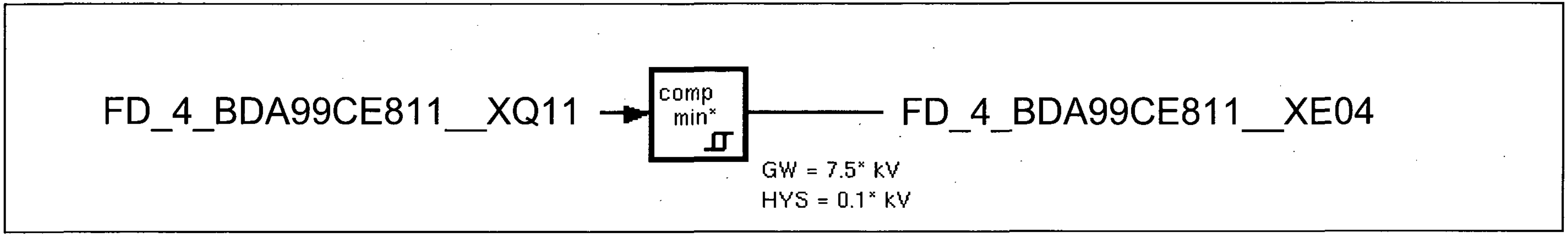
Components of the TXS Simulator

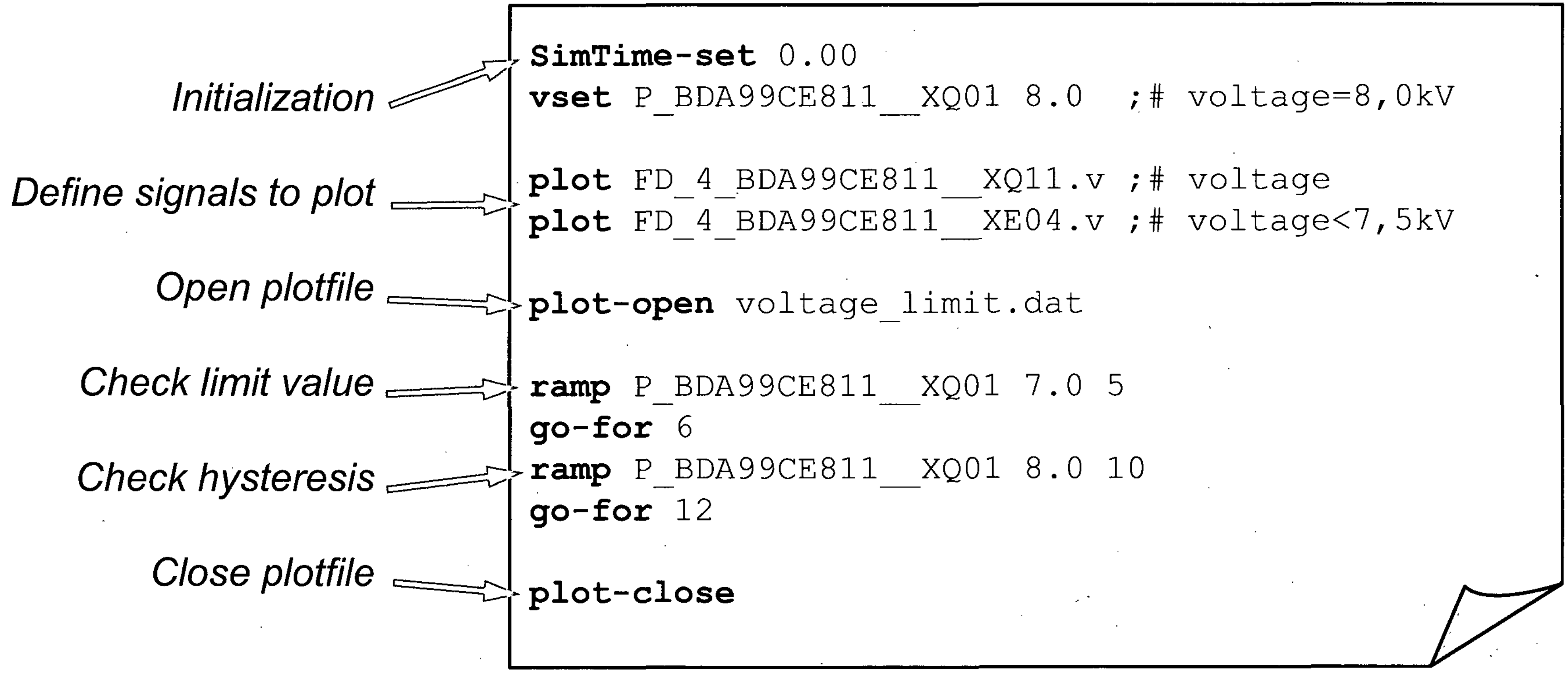
AREVA

Proprietary

Using Test Scripts for Simulation

Test Script - Example



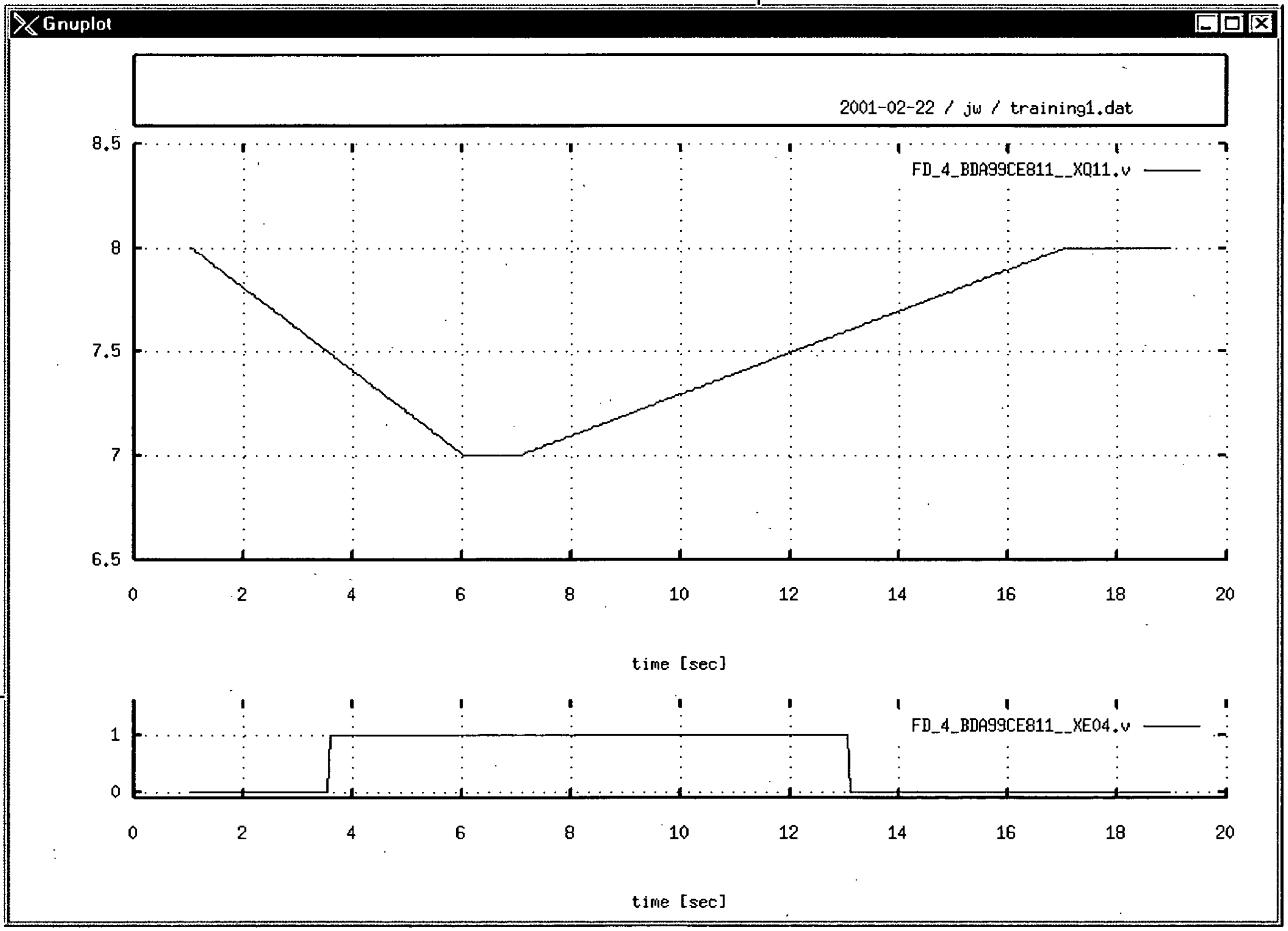


```
SimTime-set 0.00
vset P_BDA99CE811__XQ01 8.0   ;# voltage=8,0kV

plot FD_4_BDA99CE811__XQ11.v ;# voltage
plot FD_4_BDA99CE811__XE04.v ;# voltage<7,5kV

plot-open voltage_limit.dat

ramp P_BDA99CE811__XQ01 7.0 5
go-for 6
ramp P_BDA99CE811__XQ01 8.0 10
go-for 12

plot-close
```

Test Script - Result

```
* Time FD_4_BDA99CE811__XQ11.v FD_4_BDA99CE811__XE04.v
...       ...      ...
3.450     7.52     0
3.500     7.51     0
3.550     7.5      0
3.600     7.49     1
3.650     7.48     1
3.700     7.47     1
...       ...      ...
12.950    7.59     1
13.000    7.595    1
13.050    7.6      1
13.100    7.605    0
13.150    7.61     0
13.200    7.615    0
...       ...      ...
```

Content of the plotfile (extract)



AREVA

Proprietary

Monitoring the Simulation Process using the Dynamic Logics Viewer

AREVA

Proprietary

Manipulation Functions - Malfunctions
Example: One Faulty I/O Board

Proprietary

Manipulation Functions - Malfunctions Example: Two Faulty I/O Boards

Proprietary

Manipulation Functions - Malfunctions Example: Three Faulty I/O Boards

Advantages of SIVAT Application

> Allows for simulation testing early in the course of engineering

- Early identification of specification errors
  - long time before having TXS hardware available in test-bay

> Efficient tool environment for V&V activities during project implementation of TXS I&C systems

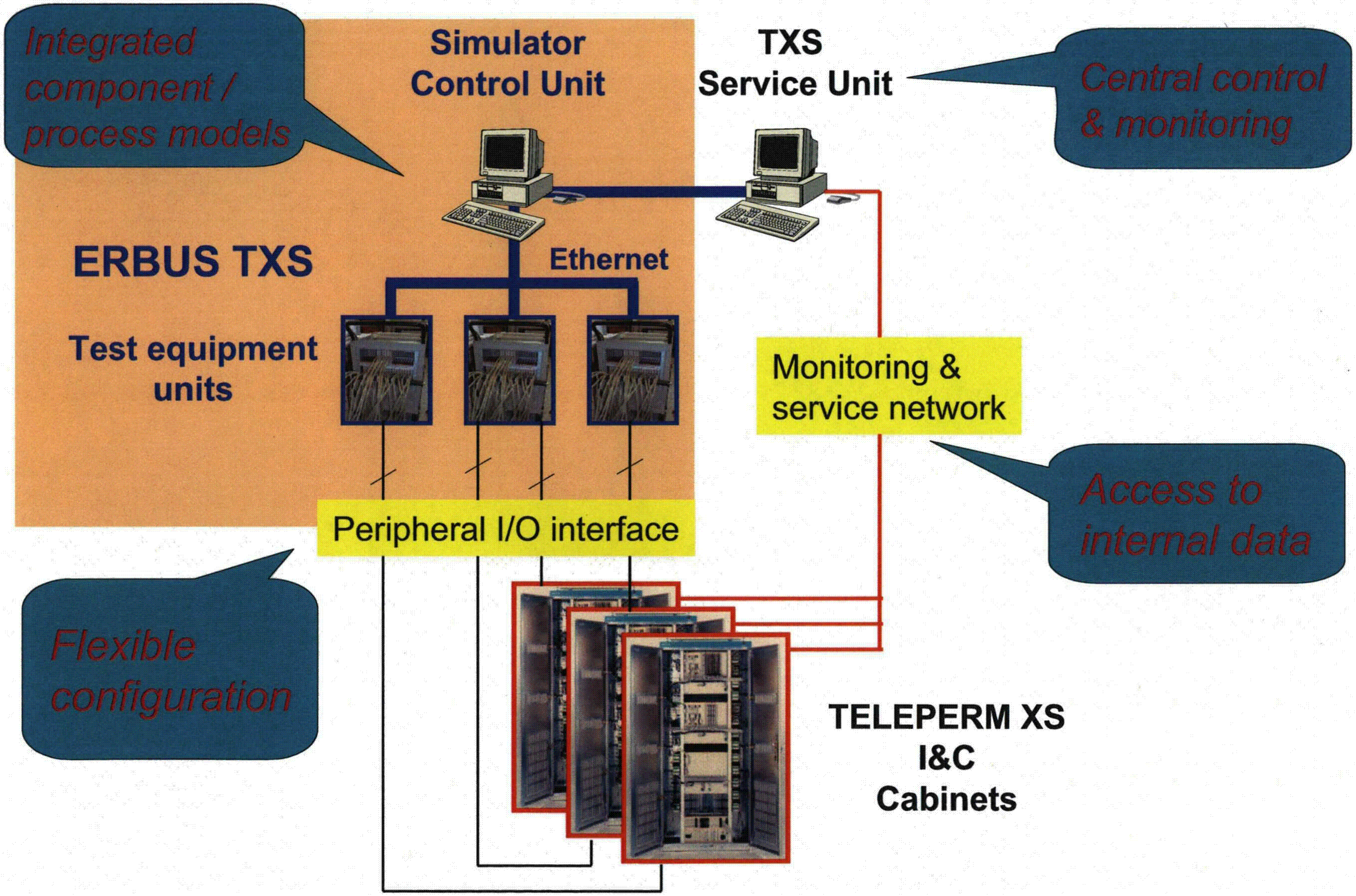
> Suitable to evaluate effects of planned changes to already installed systems

AREVA
Proprietary

Limitations of SIVAT Simulation

> The following system characteristics are not tested by SIVAT

Full-scope Test Bay Environment ERBUS TXS



Integrated component / process models

Simulator Control Unit

TXS Service Unit

Central control & monitoring

ERBUS TXS

Ethernet

Test equipment units

Monitoring & service network

Access to internal data

Peripheral I/O interface

Flexible configuration

TELEPERM XS I&C Cabinets

Validation and Use of SIVAT Tool

> SIVAT simulation of NPP Unterweser application (1996; 2000)

- Retrofit of reactor control & limitation system using TELEPERM XS
  - Validated in 1996 in a test bay and with a linked process model
  - In addition, test cases were verified with the UNISYS simulator control system (predecessor to SIVAT).
- Functional upgrade of this system prepared in 2000, but no test bay was available (TXS hardware already in operation in the plant)
- Validation approach based on SIVAT (available as V&V tool for TXS since 1998).
  - Test cases from UNISYS simulation environment and the test bay were recalculated with SIVAT.
    Since the results matched, the verification of the modified I&C functionality was also implemented with SIVAT.
  - A closed-loop system test (load shedding from 71% reactor power to own power consumption) was recalculated by SIVAT and the process model (system model NLOOP Unterweser)
- Very high concordance between the actual system behavior and the simulation results lead to the authorization for installing the modified TXS application functions based on SIVAT validation
- Plant commissioning took place without findings concerning the new I&C application functions
  (just some adjustments to parameter settings)

Validation and Use of SIVAT Tool

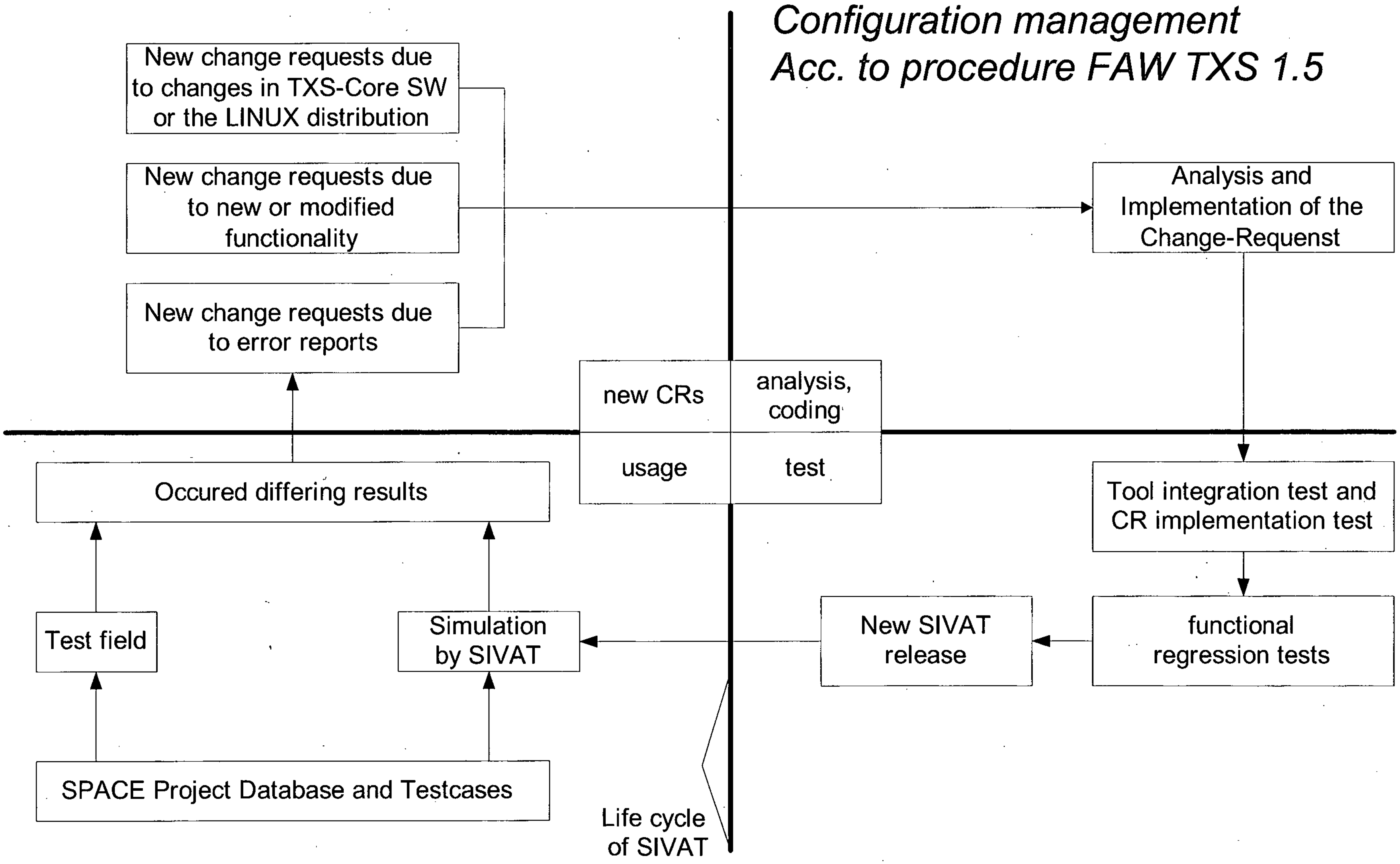
> **SIVAT simulation of NPP Philippsburg 1 application (2000-2001)**

- *Step-wise retrofit of emergency system using TELEPERM XS (redundant trains 7 and 6)*
- *A number of test field tests were verified with SIVAT as part of the TXS retrofitting in the Philippsburg 1 nuclear power plant*
- *Very high concordance made it possible to implement individual changes in the TXS application after the test bay tests*
  - *OK to commissioning after validation exclusively with SIVAT*

> **SIVAT application being part of standard TXS engineering process**

- *Many references of successful tool application, 10 years of experience*
- *Activities for comparing SIVAT and test bay results in every new project*
- *Majority of specification errors identified by SIVAT; before start of test bay*

Life Cycle Management of SIVAT Tool



Configuration management
Acc. to procedure FAW TXS 1.5

New change requests due to changes in TXS-Core SW or the LINUX distribution

New change requests due to new or modified functionality

New change requests due to error reports

Analysis and Implementation of the Change-Requenst

new CRs

analysis, coding

usage

test

Occured differing results

Tool integration test and CR implementation test

Test field

Simulation by SIVAT

New SIVAT release

functional regression tests

SPACE Project Database and Testcases

Life cycle of SIVAT

SIVAT Documentation
Summary of Information

> AREVA NP Report No. NGLP/2004/en/0094, “TELEPERM XS Simulation - Concept of Validation and Verification,” provides a detailed description of SIVAT.

- Section 2.0 describes SIVAT and its use
- Section 2.4.7 provides an example of the testing methodology.
- Section 4.1 describes the development processes and procedures
- Section 4.2 summarizes experience in using SIVAT for testing TXS application software.

> SIVAT conforms to Clause 5.3.2 of IEEE Std 7-4.3.2

- The quality assurance process and operating experience provide basis for conformance.

SIVAT report has been submitted to NRC to support the Oconee LAR (Item 25)

SIVAT
Conclusions

> SIVAT provides a effective simulation-based test environment for project-related TXS application software used to validate the application software prior to installation into the target hardware.

> SIVAT was developed and is maintained with quality-related life-cycle and configuration management processes.

> AREVA NP has substantial experience in using SIVAT in the development of TXS application software.

> SIVAT conforms to the guidance in clause 5.3.2 of IEEE Std 7-4.3.2-2003.

>Closing

Oconee Nuclear Station

AREVA

Proprietary

Discussion of Testing and V&V for Oconee Project

Agenda

► Background on Testing	Mark Burzynski
► Oconee Factory Acceptance Testing	Werner Baltes
► Oconee SIVAT Testing	Farhad Abbasbanaey
► Discussion on Testing V&V	Steve Yang
► Closing	

AREVA

Proprietary

Background on Testing

Mark Burzynski

Background on Testing

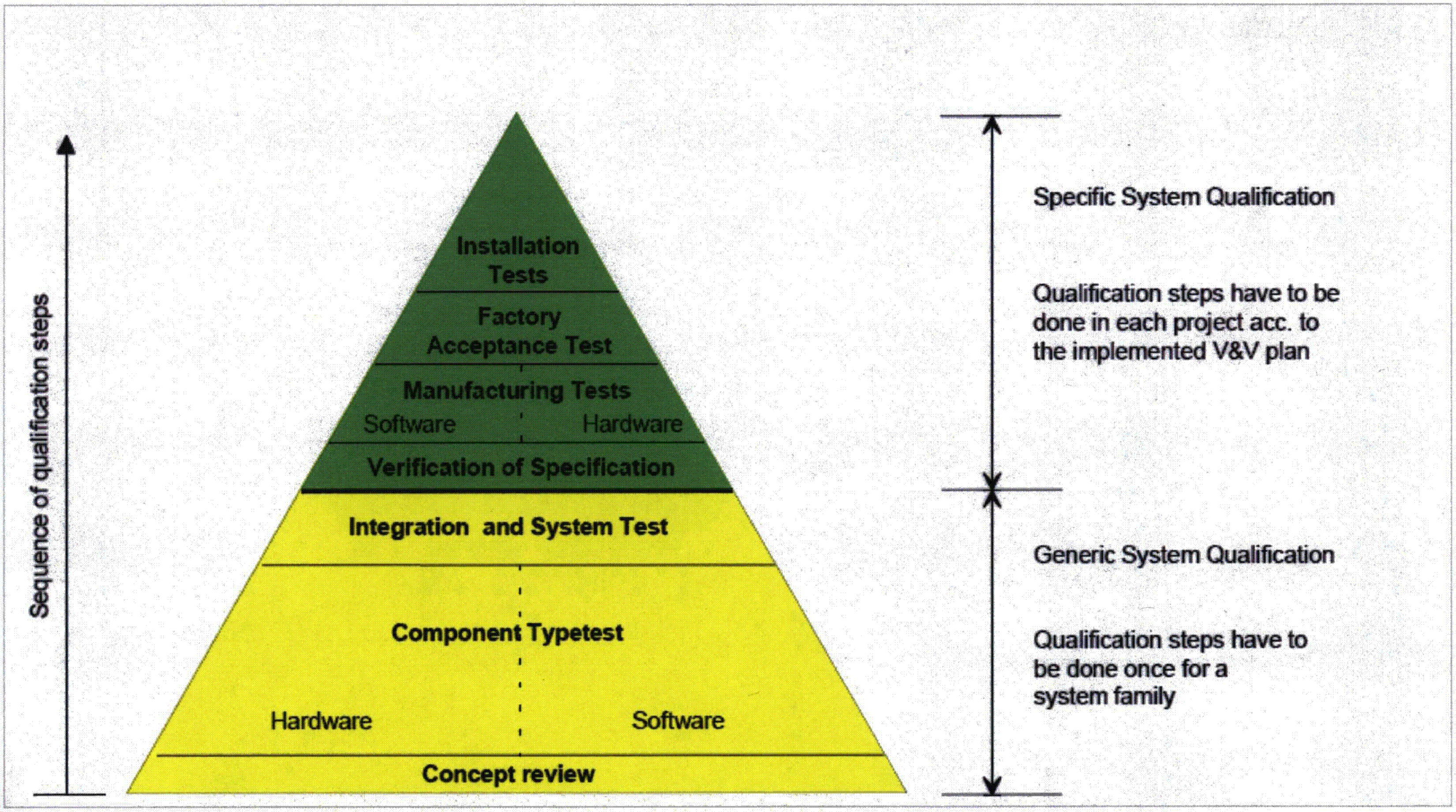
TXS System Development Testing

- TXS system is a fully integrated suite of hardware and software designed specifically for nuclear safety applications.
- TXS system has significant nuclear operating experience.
- TXS system is described in the TXS Topical Report.
- NRC approved the TXS Topical Report in a safety evaluation report issued in May 2000.
- Overall application independent qualification process is described in Section 2.2 of the TXS Topical Report.

The TXS platform has been fully qualified as an integrated platform

Background on Testing

TXS System Development Testing


Sequence of qualification steps
Installation Tests
Factory Acceptance Test
Manufacturing Tests
Software
Hardware
Verification of Specification
Integration and System Test
Component Typetest
Hardware
Software
Concept review
Specific System Qualification
Qualification steps have to be done in each project acc. to the implemented V&V plan
Generic System Qualification
Qualification steps have to be done once for a system family

TXS generic system qualification process included several layers of testing

Background on Testing

TXS Project-Specific Activities

- Application software is implemented using the TXS Specification and Coding Environment (SPACE) tool.
- This tool is used to implement functional logic.
- Software code is automatically generated from Function Diagrams by the code generation tools.

The project-specific TXS system is developed from qualified hardware and software modules using the qualified development tools

AREVA

Proprietary

Background on Testing

SPACE - Graphical User Interface for Engineering and Service

Logical 'software integration' occurs at this stage

Background on Testing

SPACE - Graphical User Interface for Engineering and Service

- SPACE is an engineering design tool that connects qualified components into network diagrams and qualified function blocks into function diagrams.
  - It is similar to designing a module-based analog system.
- There is no manual code generation for the safety system software.
  - Software is automatically generated from the networks diagrams and function diagrams by the qualified SPACE tool.
  - SPACE provides tools to verify proper links of the function blocks.
- SPACE can also generate diagrams that can be checked by an independent team, similar to the conventional design quality assurance requirements.

TXS SPACE tool eliminates certain important human errors and supports independent verification

Background on Testing

TXS Project-Specific SIVAT Testing

- SIVAT tests the same C Code produced by SPACE tools for the safety system.
- SIVAT tests validate that the specified safety system software requirements have been correctly implemented in the SPACE function diagrams.
- Access to all the internal and external signals as well as the function block parameters and internal memory is available during testing in the simulation environment.
- If realistic feedback is required from the process for the purpose of assessing the functional response, the code to be tested can also be coupled to a plant or component model.

Background on Testing

SIVAT in the Engineering Process

SIVAT testing validates that software automatically generated from SPACE satisfies required functionality for input/output response

Background on Testing

TXS Project-Specific FAT

- Physical software integration occurs during the factory acceptance test (FAT) stage, when the application software is loaded on the TXS processors.
- The project-specific FAT Plans cover the approach and activities associated with the Software and Hardware Integration.
- A project-specific Software Generation and Download Procedures is issued for each project to control and document the generation of each application software release.

Background on Testing

Alignment with IEEE Std 1012 Testing Activities

- IEEE Std 1012-1998 describes four testing activities:
  - ◇ Component Testing
  - ◇ Integration Testing
  - ◇ System Testing
  - ◇ Acceptance Testing
- IEEE Std 1012-1998 Figure 2 shows a progression of test activities occurring during the development process.

Background on Testing

Alignment with IEEE Std 1012 Testing Activities

IEEE Std 1012 Testing Activity	Generic TXS Testing	Project-Specific Testing
Component Testing	**X** (hardware and software type tests)	**Not Applicable** (based on use of qualified hardware and software modules)
Integration Testing	**X**	Application Software: SIVAT for integration of Function Block modules **Optional X** (see Note 1)
		System Components: Pre-FAT prerequisites and procedure dry runs (manufacturing tests)
System Testing	**X**	**X** (integrated in FAT based on use of qualified system components and development tools)
Acceptance Testing	**Not Applicable**	

Legend: **X** indicates alignment with IEEE Std 1012 testing.

Note 1 – For the case where SIVAT testing is performed by development organization with a complete FAT of application software functionality, the V&V team only performs the reviews of the SIVAT plan and results. Alternately, the V&V team can trace the requirements through the SIVAT testing as performed by development group, in which case application software integration tests can be eliminated from the scope of the FAT (called 'reduced' FAT).

Background on Testing
Conclusion

- The project-specific TXS system can only be developed from qualified hardware and software modules through the use of the qualified SPACE tool.
- SIVAT testing validates that software automatically generated from SPACE satisfies required functionality for input/output response.
- The combination of TXS generic qualification testing and project-specific testing addresses all of the testing activities in IEEE Std 1012-1998.

AREVA
Proprietary

Oconee Factory Acceptance Testing

Werner Baltes

AREVA
Proprietary

Oconee FAT

FAT Plan

- The FAT plan is the document that
  - ◇ Specifies the scope of FAT testing
  - ◇ Provides an overview of FAT preparation and FAT activities
  - ◇ Provides an overview of the test coverage
  - ◇ Provides an overview of the test field environment
- FAT Plan and revisions are approved in accordance with the AREVA NP Quality Management Manual and by Duke Energy.

Oconee FAT

Test Objectives

- The FAT tests validate the correct functionality of the RPS/ESPS as an integrated system, i.e. with all software implemented, with all interfaces and all peripheral equipment that is in the scope of the delivery.
- Additional tests are performed to provide sufficient overlap with equipment that cannot be involved in the functional channel tests.

Tests are performed to validate functional requirements in design and customer specifications

AREVA

Proprietary

Oconee FAT

Test Objects and Interfaces

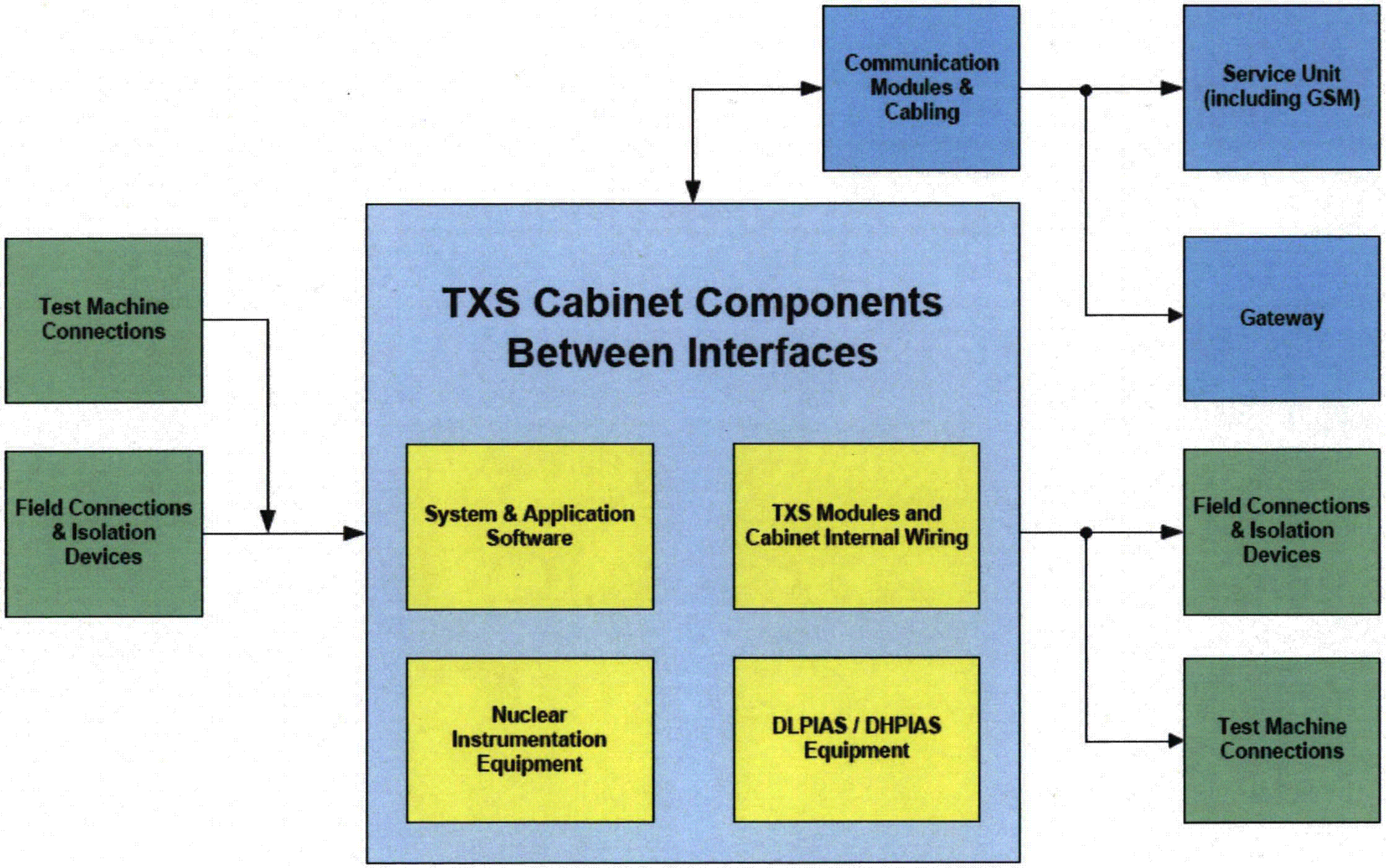
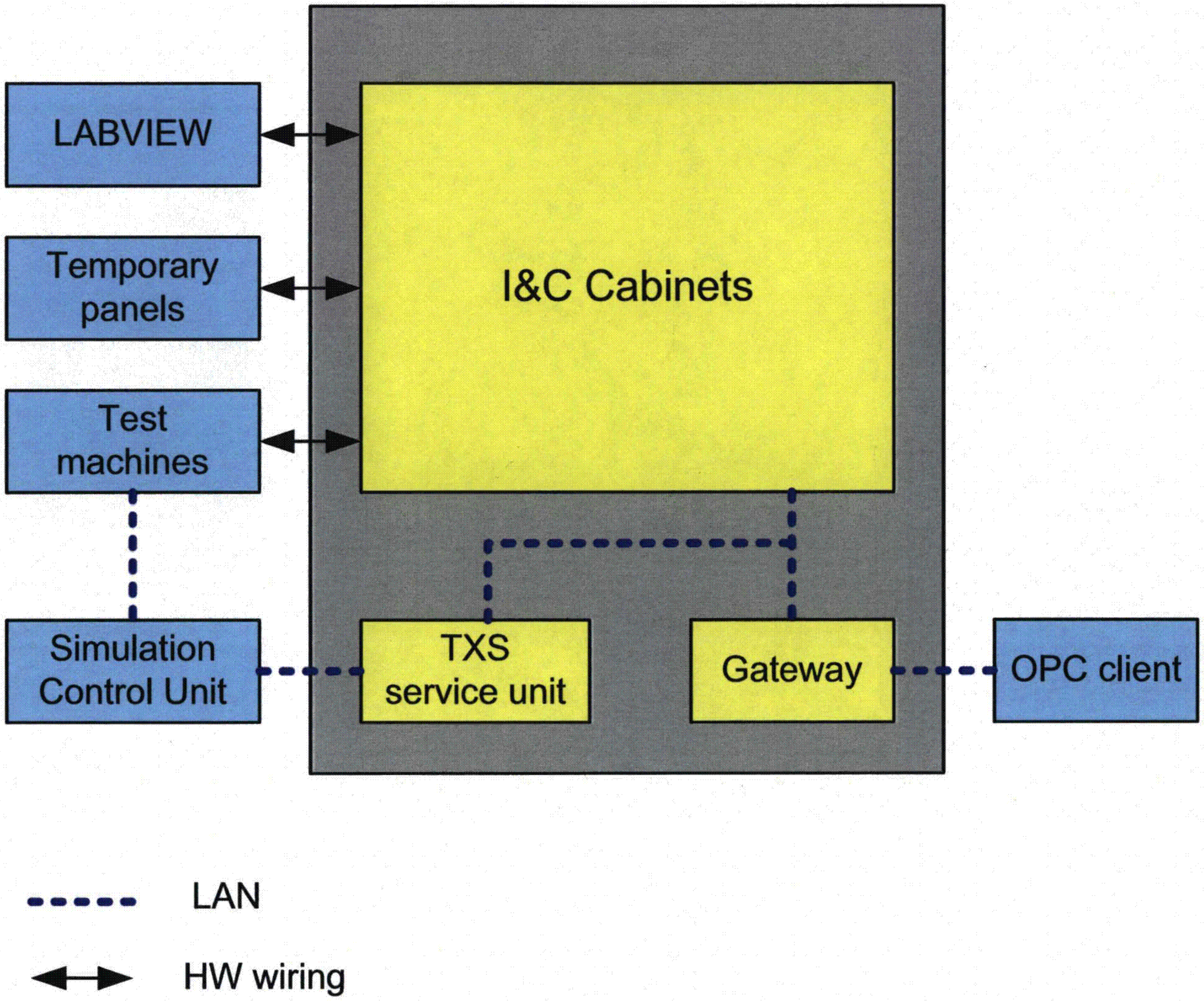

Communication Modules & Cabling
Service Unit (including GSM)
Gateway
Test Machine Connections
Field Connections & Isolation Devices
TXS Cabinet Components Between Interfaces
System & Application Software
TXS Modules and Cabinet Internal Wiring
Nuclear Instrumentation Equipment
DLPIAS / DHPIAS Equipment
Field Connections & Isolation Devices
Test Machine Connections

Figure 1: Test Objects and Interfaces of the ONS RPS/ESPS TXS System

Oconee FAT

Test Field Environment



Oconee FAT
General Approach

- General overview of the FAT activities and support activities:

1. Plan the FAT activities
2. Develop the Test Specifications / Procedures using approved design documents
3. Prepare test field and test equipment for FAT
4. Complete FAT prerequisites
5. Perform test activities
6. Evaluate test results to acceptance criteria
7. Develop the Test Summary Report and the Test Incident Report

Oconee FAT

General Approach

Figure 2: General Approach to the Factory Acceptance Test

Oconee FAT

Major System Segment and Test Procedure

Test Objects and Interfaces (from Figure 1)	Corresponding Tests (from Figure 2)
Field Connections & Isolation Devices	1, 2, 12, 13
Test Machine Connections	3, 4, 5, 6, 9, 10, 11
Communication Modules & Cabling	3, 4, 7, 8, 14
TXS Service Unit (including GSM)	3, 4, 7, 14
TXS Gateway	3, 4, 8
System & Application Software	3, 4, 5, 6, 9, 10, 11, 12, 13, 14
TXS Modules & Cabinet Internal Wiring	1, 2, 3, 4, 5, 6, 12, 13
Nuclear Instrumentation Equipment	2, 12
DLPIAS/DHPIAS Equipment	1, 13

Oconee FAT

Software Test Documentation

- The following tests are considered software tests:
  - RPS Functional Test
  - ESPS Functional Test
  - Graphic Service Monitor (GSM)
  - Gateway to OAC

[ ]

- The Test Specifications incorporate the Test-Design Specification and Test-Case Specification, as defined in IEEE Std 829-1983, into a single document.
- Each Test Specification shall have the following information and structure:
  - Test, verify, and document that the system meets design and customer specifications.
  - Validate functionality under a comprehensive set of realistic operating conditions.
  - Specific acceptance criteria with individual Test Procedures developed using the Software and Hardware design documents.

Oconee FAT

Test Procedures

- For Software Tests: Test Specifications and Test Procedures are utilized.
  - Test specifications outline the test design and describe the test cases and the test steps.
  - Software Test Procedures follow the test steps described in the Test Specifications.
  - Software Test Procedures largely consist of Test Scripts, the necessary steps for executing them, and the detailed expected results.
    - Test Scripts allow for the test steps to be performed automatically.
- For Hardware Tests: Only utilize Test Procedures.
  - The Hardware Test Procedures describe the procedural steps in detail, specify the expected results and, contain auxiliary Test Scripts (if needed).
    - Test Scripts facilitate the process, but they will not make up a majority of the work as they do in Software Test Procedures.

Oconee FAT

RPS Function Tests

- RPS Functions are tested to validate compliance with design and customer specifications.
  - ◇ RPS Trip #1: Nuclear Overpower (Neutron Flux) Trip
  - ◇ RPS Trip #3: Nuclear Overpower Flux/Flow/Imbalance Trip
  - ◇ RPS Trip #4: RCS High Pressure Trip
  - ◇ RPS Trip #5: RCS Low Pressure Trip
  - ◇ RPS Trip #6: RCS Variable Low Pressure Trip
  - ◇ RPS Trip #7: RCS High Outlet Temperature Trip
  - ◇ RPS Trip #8: Reactor Building High Pressure Trip
  - ◇ RPS Trip #9: Loss of Both Main Feedwater Pumps Trip
  - ◇ RPS Trip #10: Main Turbine Trip
  - ◇ RPS Trip #11: Reactor Coolant Pump Power/Flux Trip
  - ◇ RCS Delta Pressure Average Function
  - ◇ RPS Channel E/MSI Functions
  - ◇ RPS Miscellaneous Functions

Oconee FAT

ESPS Function Tests

- ESPS Functions are tested to validate compliance with design and customer specifications.
    - ESPS Trip #1: RCS Pressure Low Trip
    - ESPS Trip #2: RCS Pressure Low Low Trip
    - ESPS Trip #3: Reactor Building Pressure High Trip
    - ESPS Trip #4: Reactor Building Pressure High High Trip
    - ESPS Miscellaneous Functions

The trip function for each RPS and ESPS channel is tested independently and then the trip functions are tested as a combined system

Oconee FAT

Additional Tests

- Additional tests are performed to validate functionality of support and monitoring equipment, and other functionality as required by design and customer specifications.
  - Cabinet Alarm Monitoring

  ( )

  - Diverse Low Pressure Injection Actuation System
  - Diverse High Pressure Injection Actuation System
  - Reactor Coolant Pump Power Monitor
  - Nuclear Instrumentation
  - RPS/ESPS Hardware Failures
  - RPS/ESPS Response Times
  - System Tests

  ( )

AREVA
Proprietary

Oconee FAT

Features Not Tested

- Features not within the scope of AREVA NP supplied equipment.
- Features validated by other means.
- Features that are of a nature that does not impact overall system functionality.

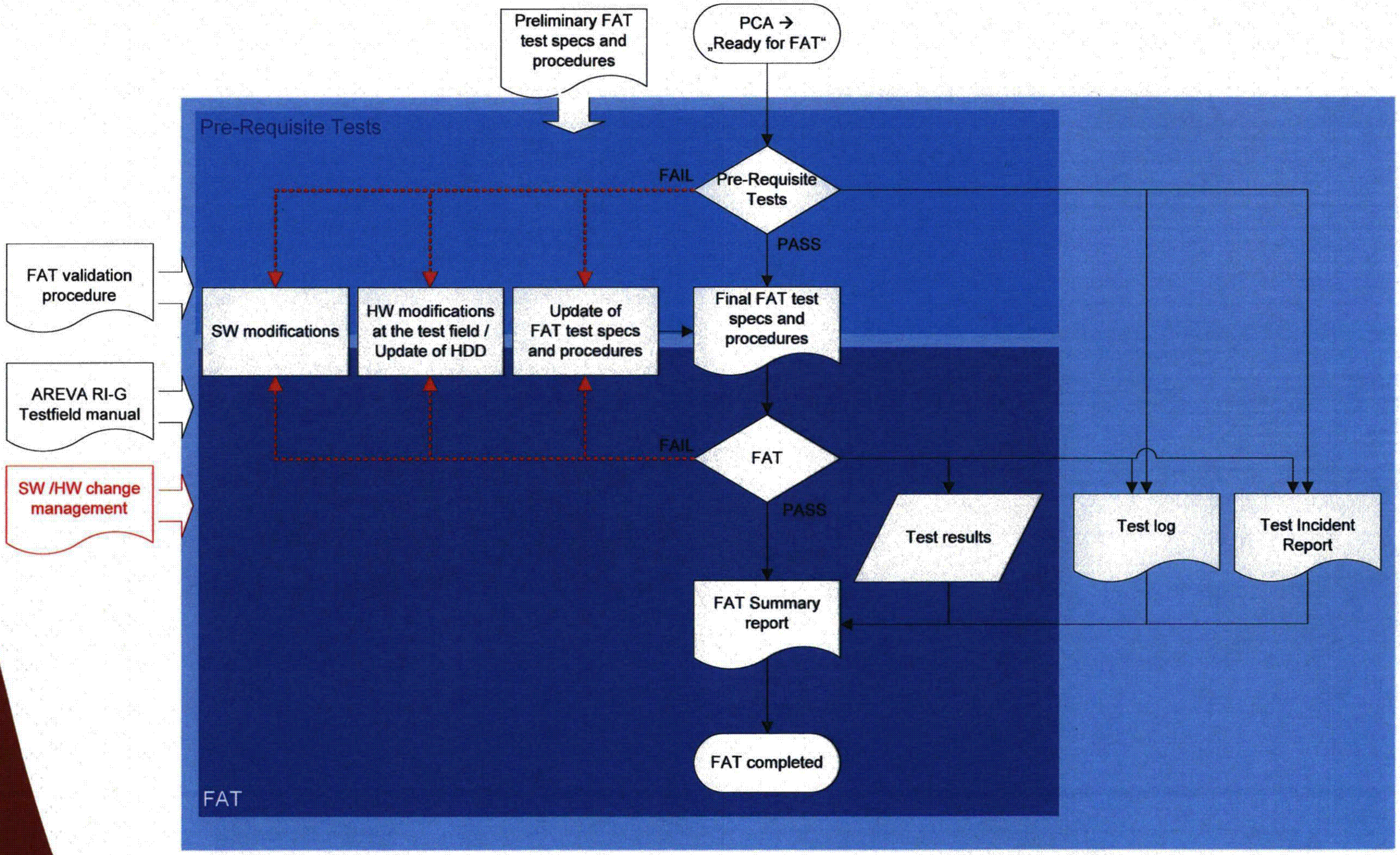
Oconee FAT

Acceptance Criteria

- Each Test Specification / Procedure details the specific, required acceptance criteria in order to determine if the test is completed successfully.
- These criteria are developed from design and customer specifications.
- Test results are evaluated during testing to ensure compliance with test requirements.
- Any deviations between the test results and the acceptance criteria (i.e., the expected results) shall be dealt with in accordance with the FAT Plan.
- The role of V&V with regards to V&V test acceptance is described in the Software V&V Plan.
- Software Quality Assurance with regards to item pass / fail criteria is described in the Software Quality Assurance Plan.

Oconee FAT

Handling of Variances



Oconee FAT

Coverage and Overlap of SW and HW Tests

- The following three tables provide an overview of which test checks which parts of the system and how sufficient overlap between the tests and for hardware and software is ensured.
- The following legend applies to the tables:

Legend:

🟦	Hardware
🟩	Hardware / Software Interface
🟨	Software
X	this test covers the corresponding HW / SW
F	includes testing of failure behavior

AREVA

Proprietary

Oconee FAT

Coverage and Overlap of SW and HW Tests

AREVA

Proprietary

Oconee FAT

Coverage and Overlap of SW and HW Tests

AREVA

Proprietary

Oconee FAT

Coverage and Overlap of SW and HW Tests

Oconee FAT
Conclusions

- The Oconee Unit 1 FAT satisfies the project-specific aspects of IEEE Std 1012-1998 requirements for application software integration, system, and acceptance testing to satisfy IEEE Std 1012 testing requirements.
- The Oconee Units 2 and 3 FATs satisfies the project-specific aspects of IEEE Std 1012-1998 requirements for system and acceptance testing to satisfy IEEE Std 1012-1998 testing requirements.
  - Project-specific application software integration testing will be performed with SIVAT to satisfy IEEE Std 1012-1998 testing requirements.

AREVA

Proprietary

Oconee SIVAT Testing

Farhad Abbasbanaey

AREVA
Proprietary

Oconee Unit 1 SIVAT

- Oconee Unit 1 SIVAT testing was used as a debug tool during the detailed software design phase prior to FAT.
- SIVAT testing verified that the functional requirements of the SRS and the software design in the SDD were properly implemented into the project database as shown in the Application Software Code document.
- Test Item was the RPS/ESPS Application Software that was compiled and linked using the SIVAT simulation-environment of the TXS system.

AREVA

Proprietary

Oconee SIVAT

RPS Function Tests

- RPS Functions were tested to validate compliance with design and customer specifications.
  - RPS Trip #1: Nuclear Overpower (Neutron Flux) Trip
  - RPS Trip #3: Nuclear Overpower Flux/Flow/Imbalance Trip
  - RPS Trip #4: RCS High Pressure Trip
  - RPS Trip #5: RCS Low Pressure Trip
  - RPS Trip #6: RCS Variable Low Pressure Trip
  - RPS Trip #7: RCS High Outlet Temperature Trip
  - RPS Trip #8: Reactor Building High Pressure Trip
  - RPS Trip #9: Loss of Both Main Feedwater Pumps Trip
  - RPS Trip #10: Main Turbine Trip
  - RPS Trip #11: Reactor Coolant Pump Power/Flux Trip
  - RCS Delta Pressure Average Function
  - RPS Channel E/MSI Functions
  - RPS Miscellaneous Functions

AREVA
Proprietary

Oconee SIVAT
ESPS Function Tests

- ESPS Functions were tested to validate compliance with design and customer specifications.
  - ◇ ESPS Trip #1: RCS Pressure Low Trip
  - ◇ ESPS Trip #2: RCS Pressure Low Low Trip
  - ◇ ESPS Trip #3: Reactor Building Pressure High Trip
  - ◇ ESPS Trip #4: Reactor Building Pressure High High Trip
  - ◇ ESPS Miscellaneous Functions

The trip function for each RPS and ESPS channel is tested independently and then the trip functions are tested as a combined system

Oconee SIVAT

Features to be Tested

- Functionality specified in the Unit 1 SDD was tested to determine if the software elements correctly implement the software requirements.
  - Compliance with functional requirements.
  - Performance at boundaries, interfaces, and under error conditions.
- The following characteristics were checked:
  - Signals to Output boards must have no fault status at all times, even under error conditions.
  - Test results must be verified from start of test until the completion of the test in order to verify that no unexpected intermediate results are present.
  - Correct setting of function block parameters must be verified against software requirements.

Oconee SIVAT

Features Not Tested

- The testing of TXS system software components (Operating System, I/O Drivers, Communication Software, Runtime Environment, and Function Blocks) were not within the scope of this test.
  - These system software components were validated through the TXS generic qualification process

Oconee SIVAT

Test Results

- Baseline Test Summary
  - Four separate SIVAT runs performed on Unit 1 software
  - Two functional errors identified in software
  - Other problems identified with test procedures, acceptance criteria descriptions, and test scripts
    - These problems were corrected and tests reperformed
  - One software design error identified after SIVAT testing during previous equipment testing
    - Software error corrected and retested

Software design errors have been corrected and successfully retested

AREVA
Proprietary

Oconee SIVAT
Test Results

- Supplemental Test Summary
  - Testing was created because of design changes from Open Item and changes to customer requirements
  - One SIVAT run was performed on the updated Unit 1 software
  - Zero functional errors identified in software
  - Zero problems identified with test procedures, acceptance criteria descriptions, and test scripts

Software design errors have been corrected and successfully retested

Oconee SIVAT

Test Results

- Insights and Lessons Learned
  - Lessons learned from Baseline SIVAT testing incorporated into the Supplemental Testing methodology
  - Eliminated errors produced
  - Automation of script execution allows less error likely situations (e.g., script typos, signal ID verification)
  - Lessons learned to be factored in to Unit 2 and 3 SIVAT testing

Oconee SIVAT

Unit 1 Test Documentation

- ***Position Paper**: Deviation of the Simulation Based Validation Tool (SIVAT) Documentation Compared to IEEE Std 829-1983 and IEEE Std 1008-1987*
  - Assessed specific deviations between Oconee Unit 1 SIVAT test documentation and IEEE Stds 829-1983 and 1008-1987.
  - Deviations are primarily format or have minor content variations, with no technical inadequacies.
  - AREVA NP and Duke Energy have determined that Unit 1 SIVAT test documentation is of sufficient technical content and clarity.
- Regulatory Guides 1.170 and 1.171 provide a certain amount of latitude in development of testing documentation, as stated in the Regulatory Positions.
  - Variances in test documentation are allowed as long as the documentation meets the regulatory requirements.
- Subsequent Unit 1 test reports correct the deviations noted in the position paper.

Oconee SIVAT
Conclusions

- Oconee Unit 1 SIVAT testing was used as a debug tool in the detailed software design phase.
- Unit 1 SIVAT test results were not used to demonstrate independent validation of software functional requirements.
  - V&V did not review Unit 1 SIVAT test specifications and procedures
  - Original test document did not conform to IEEE Std 829.
- Unit 2 and 3 SIVAT testing will be used for integration testing of the application software to satisfy IEEE Std 1012-1998 testing requirements.

Oconee Testing Verification and Validation

Steve Yang

Proprietary

Oconee V&V

Organization

TXS Software Program Manual

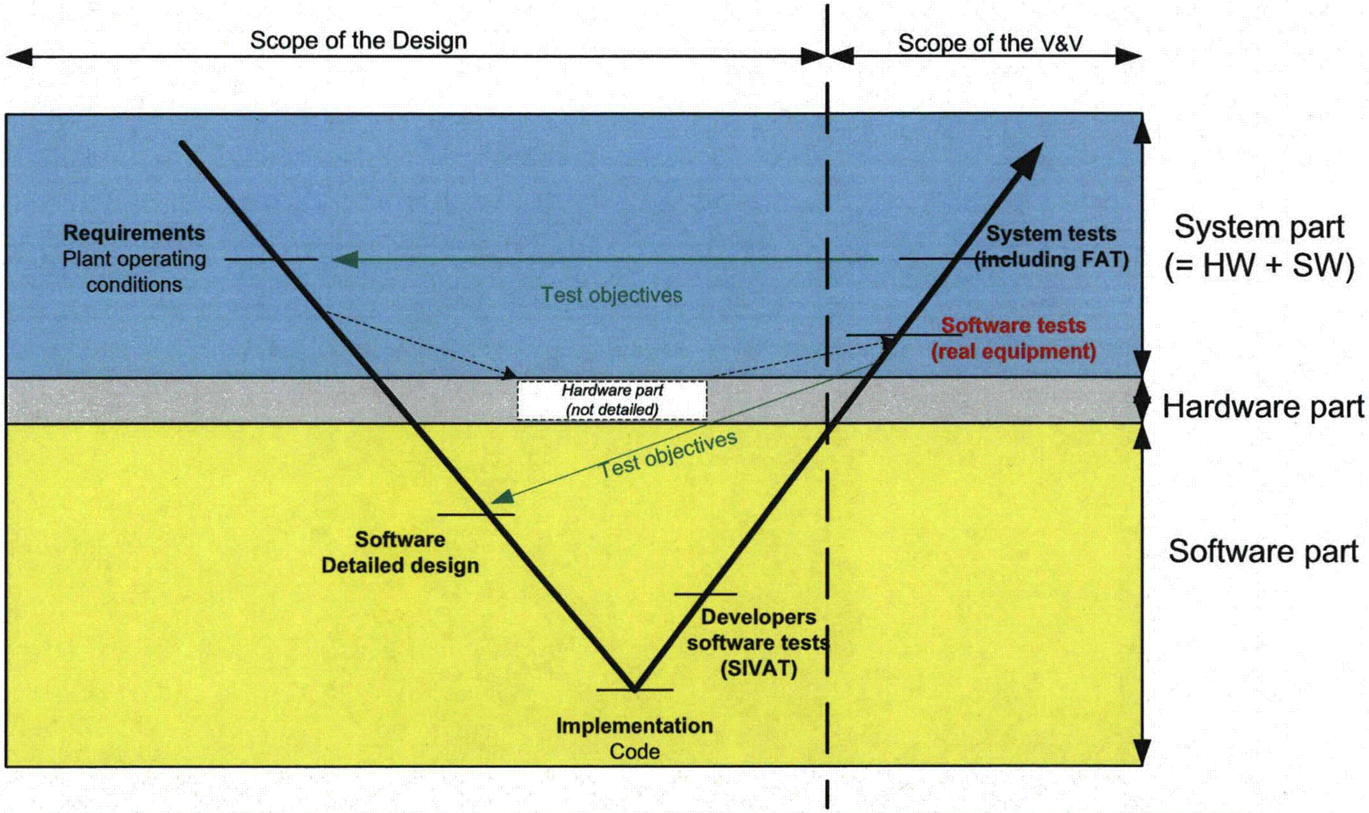
Testing and V&V Options

- TXS Software Program Manual outlines three methods for software testing and V&V:
  1. SIVAT testing is performed by design engineering, with a 'complete' FAT (standard FAT augmented with software integration tests), the V&V team only reviews SIVAT plan and results, and a FAT with software tests is performed.
  2. SIVAT testing as performed by design engineering, V&V traces requirements through the SIVAT testing, and with a standard FAT (called 'reduced' FAT in Software Program Manual).
  3. V&V team can plan and perform SIVAT testing in addition to tracing, in which case a standard FAT is performed.

AREVA
Proprietary

Software Program Manual Testing Option 1

Oconee Unit 1 Testing

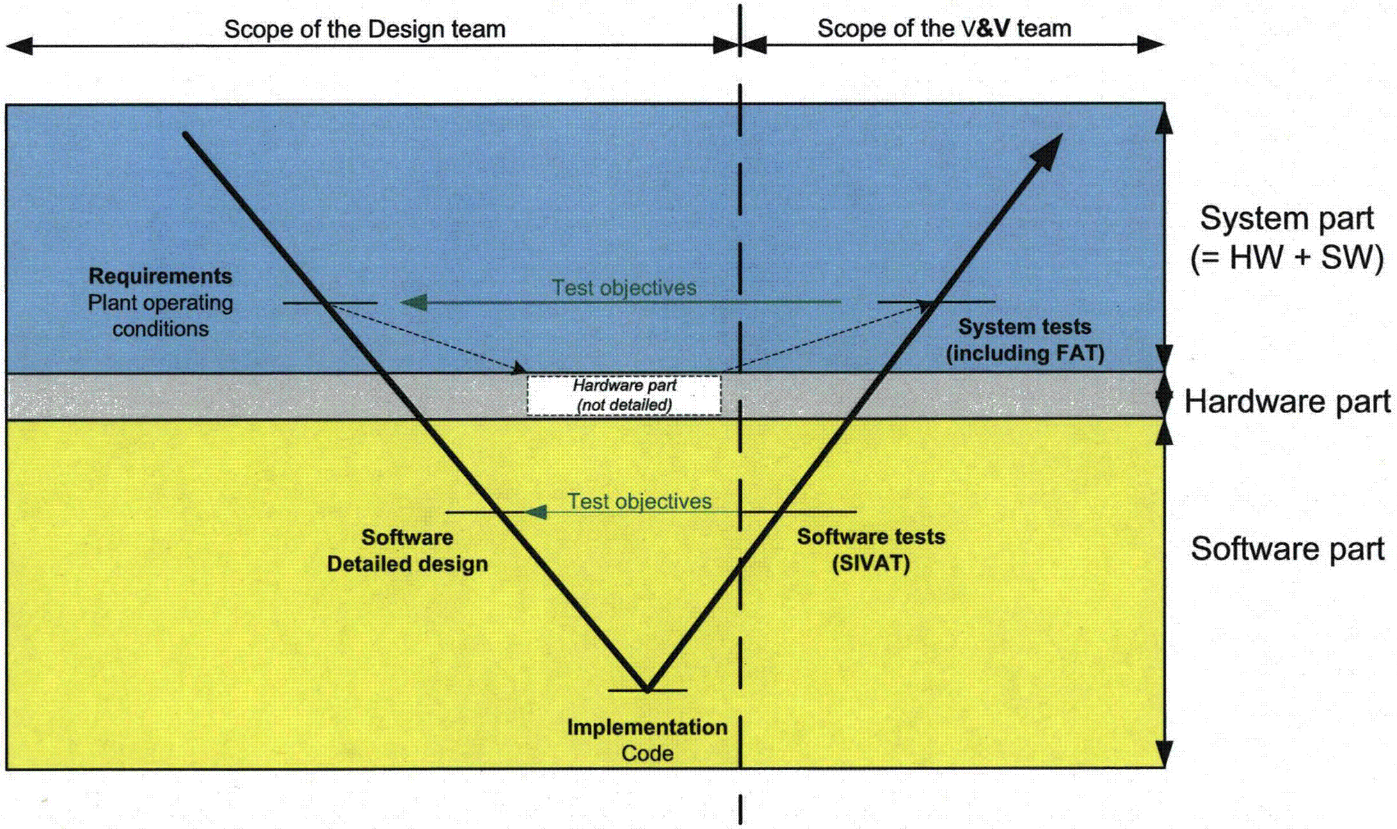


'Complete FAT' (standard FAT augmented with application software integration tests) addresses both software and systems tests

AREVA
Proprietary

Software Program Manual Testing Option 2

Oconee Units 2 and 3 Testing



'Reduced FAT' (standard FAT) addresses systems tests and SIVAT addresses application software tests

Testing V&V

TXS Approach to Simulation Testing

Layers of V&V are used to ensure quality to demonstrate proper application software functionality.

1. TXS development process has features specifically designed to improve application software reliability.
   - ◇ Use of standard Function Block library provides large experience base for standard modules.
   - ◇ Use of SPACE tool to automatically generate code eliminates important human error sources associated with manual code generation (errors of translation and introduction of complexity by engineers optimizing coding).
   - ◇ SPACE tool and Function Block library are generically qualified, which provides a very high degree of V&V independence commensurate with the importance of generic system qualification.
   - ◇ TXS development process requires use of SPACE tool and Function Block library to create code from Function Diagrams and Function Diagram Group modules.

Testing V&V

TXS Approach to Simulation Testing

2. SIVAT testing is performed by the development group and is an integral part of the TXS engineering process.
   - ◇ SIVAT is an additional layer of development testing performed on Function Diagrams and Function Diagram Group Modules.
   - ◇ SIVAT test plans, procedures, and results are prepared in accordance with 10 CFR Part 50 Appendix B quality assurance requirements.
   - ◇ The SIVAT tool is used to validate application software functionality using a wide variety of manipulation functions (i.e. built-in malfunctions).

Testing V&V

TXS Approach to Simulation Testing

3. SIVAT test plan and results are verified by V&V group to ensure software functionality.
   - ◇ V&V group is completely independent of software development.
   - ◇ I&C functionality can be fully assessed by verification of SPACE diagrams.
     - Equivalent to code verification in other code development systems.
     - Code generation verification checks performed by SPACE can be readily verified.
   - ◇ SIVAT testing methods and results can be readily verified.
     - Verification of function diagrams is facilitated by commonly understood notation used to prepare Function Diagrams.
     - NRC evaluation of the automatic code generation process was documented in SER for TXS topical report.
   - ◇ V&V group can also trace requirements through SIVAT testing specifications and procedures or perform independent testing, and can require additional test cases and analysis.

AREVA
Proprietary

Testing V&V

Simulation Testing for Oconee

- For Unit 1, the V&V group reviews SIVAT test plans and results.
  - V&V documents problems identified during review as Open Items.
  - V&V ensures that resolution of Open Items generated during the reviews is acceptable.
  - V&V method for SIVAT testing is different for Unit 1.
    - SIVAT tests were performed prior to the test plan review by V&V group.
    - Unit 1 SIVAT test results are not used to demonstrate independent validation of software functional requirements.
    - FAT for Unit 1 will test all elements of the application software.
- For Units 2 and 3, the V&V group will perform the independent verification (including requirements tracing) and Appendix B design review of the SIVAT test plans, procedures, and results to ensure software functionality.
  - V&V will document problems identified during the review as Open Items.
  - V&V ensures that resolution of Open Items generated during the reviews is acceptable.
  - Resolution of Open Items may include performing selected SIVAT testing again, performing new SIVAT test cases, or ensuring that FAT fully tests software functionality not tested by SIVAT.
- The V&V group also has the authority to perform independent SIVAT testing, as deemed necessary.

Testing V&V

Value of Formal SIVAT Testing

- A balance is drawn between performing software tests during complete FAT (later in the development process) to support customer quality assurance observation and monitoring and performing more formal software testing with SIVAT earlier in the process.
- IEEE Standard 1008-1987, IEEE Standard for Software Unit Testing," recognizes that:

  There are significant economic benefits in the early detection of faults. This implies that test set development should start as soon as practical following availability of the unit requirements documentation because of the resulting requirements verification and validation. It also implies that as much as practical should be tested at the unit level. (Paragraph B2.4)
- The early detection of faults through simulation testing with formal V&V also serves to reduce project risks earlier in the development process.

Testing V&V

TXS Approach to Acceptance Testing

Layers of V&V are used to ensure FAT quality to demonstrate proper integrated system performance.

1. Generic TXS platform software and hardware integration is generically qualified, as described in the TXS topical report.
   - ◇ This approach provides a very high degree of V&V independence commensurate with the importance of generic system qualification.
2. FAT is performed by a test group (comprised of hardware and software personnel from the design organization).
   - ◇ This testing method ensures that the proper hardware and software personnel are used in an integrated fashion to develop and conduct the FAT.
   - ◇ The FAT plans, procedures, and results are prepared in accordance with 10 CFR Part 50 Appendix B quality assurance requirements.
     - ∘ This approach enables the hardware and software engineers to compare the test results to the design and customer specifications.

Testing V&V

TXS Approach to Acceptance Testing

3. V&V defines criteria and performs independent verification (including requirements tracing) and Appendix B design review of FAT procedures and results to ensure system functionality.
   - ◇ V&V performs verification work in accordance with Software Verification and Validation Plan.
   - ◇ Independent V&V group has authority to perform independent acceptance testing or require additional test cases and analysis, as deemed necessary.

The TXS approach to testing V&V has the benefit of two diverse groups addressing testing methods and results: two heads are better than one!

V&V Methodology

Requirements Traceability

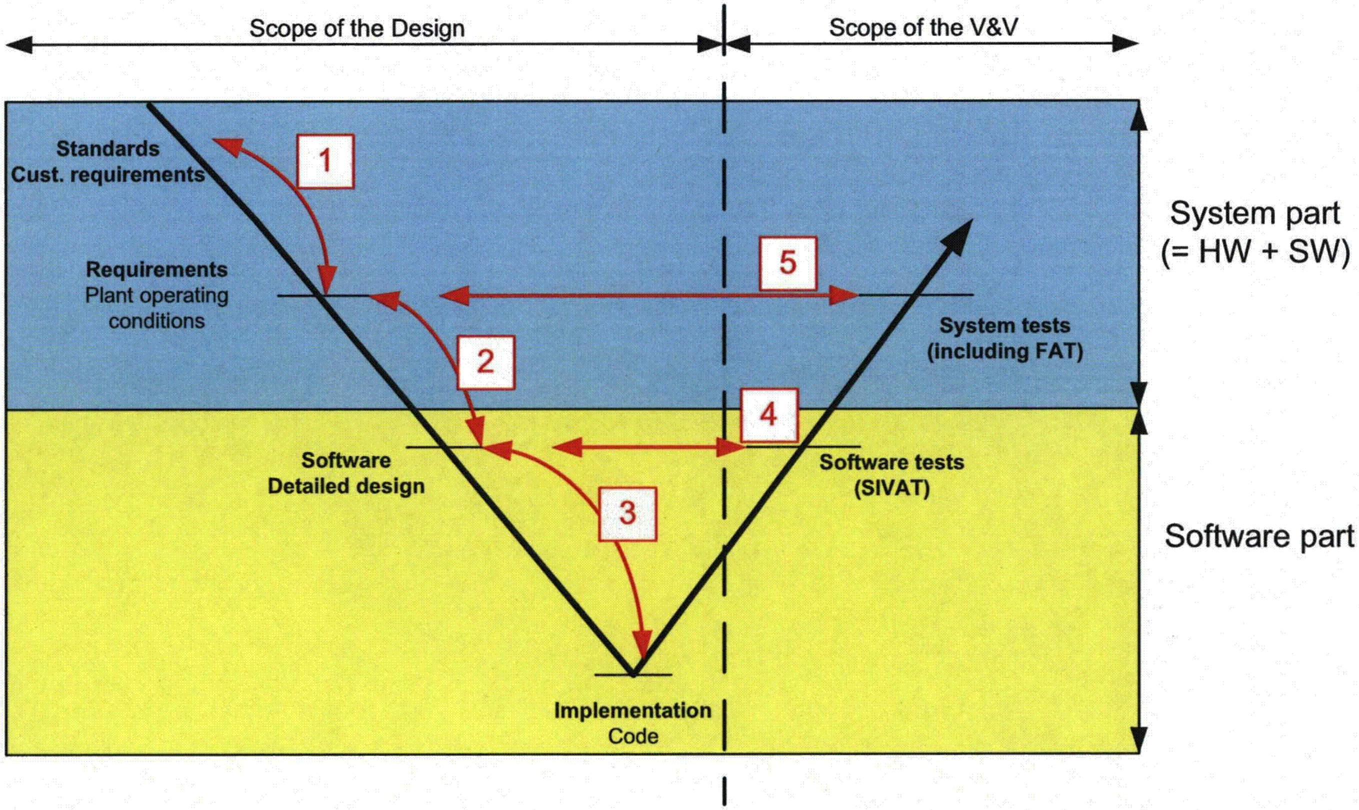
- FAT is a formal project milestone that will be attended by both AREVA NP Quality Assurance and Duke Energy personnel.
- FAT fulfills requirement for validation.
- During FAT, V&V engineers observe testing and verify that testing follows approved FAT procedures.
- V&V team uses software requirements traceability matrix to ensure that original requirements have been tested.
- V&V engineers independently verify that software versions being tested match those in Software Configuration Management list.

AREVA

Proprietary

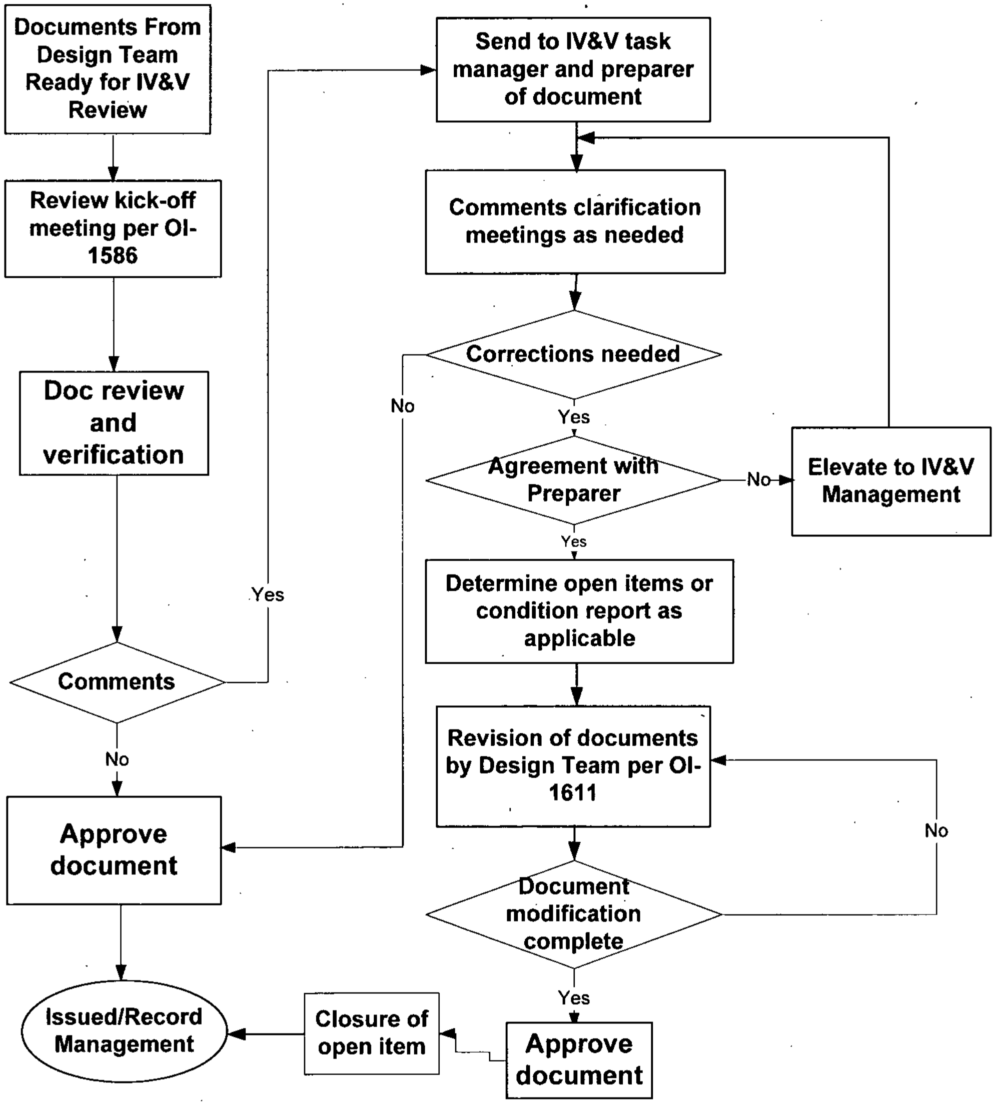
Software Program Manual Testing Option 2

Oconee Units 2 and 3 Tracing and Testing



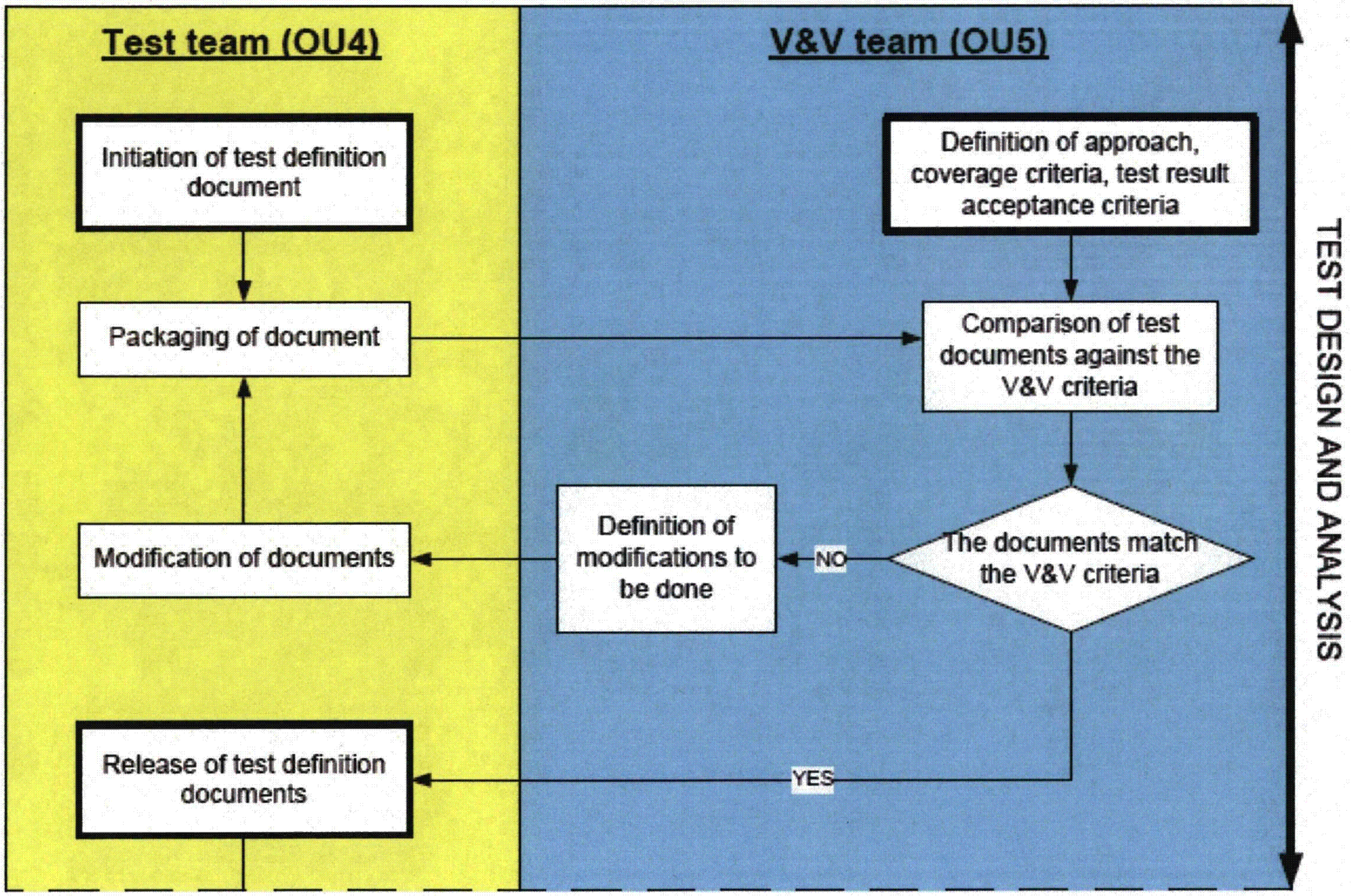
Review & Verification Activities

General Process


Documents From Design Team Ready for IV&V Review
Review kick-off meeting per OI-1586
Doc review and verification
Comments
Yes
No
Approve document
Issued/Record Management
Send to IV&V task manager and preparer of document
Comments clarification meetings as needed
Corrections needed
No
Yes
Agreement with Preparer
No
Elevate to IV&V Management
Yes
Determine open items or condition report as applicable
Revision of documents by Design Team per OI-1611
Document modification complete
No
Yes
Approve document
Closure of open item

AREVA
Proprietary

Testing V&V
Methods

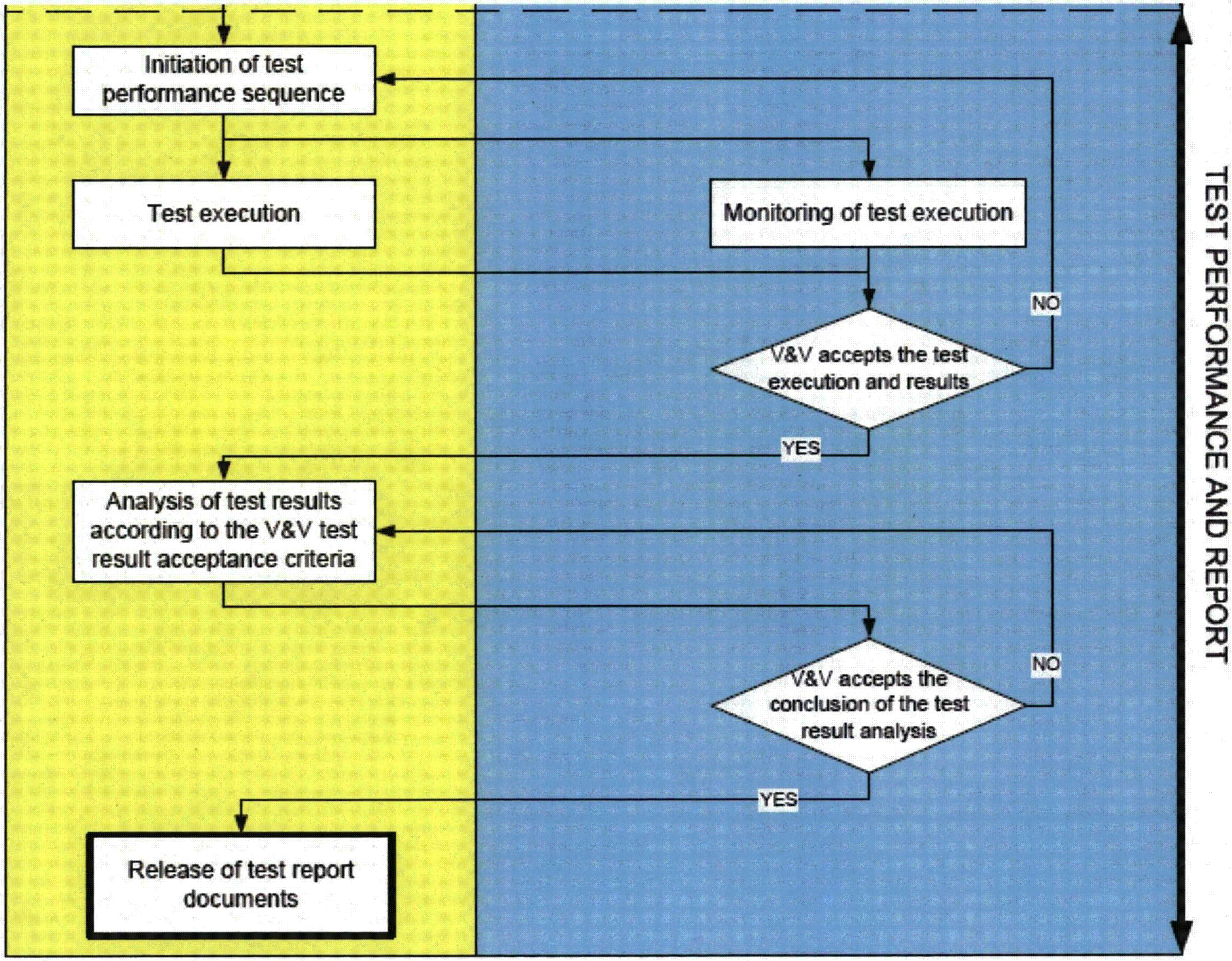

Test team (OU4)
V&V team (OU5)
Initiation of test definition document
Packaging of document
Modification of documents
Release of test definition documents
Definition of approach, coverage criteria, test result acceptance criteria
Comparison of test documents against the V&V criteria
The documents match the V&V criteria
NO
Definition of modifications to be done
YES
TEST DESIGN AND ANALYSIS

AREVA

Proprietary

Testing V&V

Methods



Initiation of test performance sequence
Test execution
Monitoring of test execution
NO
V&V accepts the test execution and results
YES
Analysis of test results according to the V&V test result acceptance criteria
NO
V&V accepts the conclusion of the test result analysis
YES
Release of test report documents
TEST PERFORMANCE AND REPORT

AREVA
Proprietary

Testing V&V
Conclusions

- The V&V approach to testing is equivalent or better than methods identified in IEEE Std 1012-1998.
  - ◇ Use of two diverse groups to assess testing method and results provides a stronger test than a single test perspective.
- No manual code generation for the safety system software.
  - ◇ Software is automatically generated from the network diagrams and function diagrams by the qualified SPACE tool.
- SPACE generates diagrams that can be readily checked by an independent team to verify that requirements are met and that validation testing is correct.

Testing V&V

Availability of Oconee Tests V&V Reports

- The following Oconee Unit 1 software V&V reports will address testing activities:

Oconee Unit 1 Software V&V Report	Target Availability
Design V&V Activity Summary Report • SIVAT Test Plan Verification • Acceptance Test Plan Verification	June 2008
Implementation V&V Activity Summary Report • SIVAT Test Report and Test Incident Report Verification	August 2008
Test V&V Activity Summary Report • Acceptance Test Design Specification Verification • Acceptance Test Case Specification Verification • Acceptance Test Procedure Verification • Acceptance Test Verification	March 2009

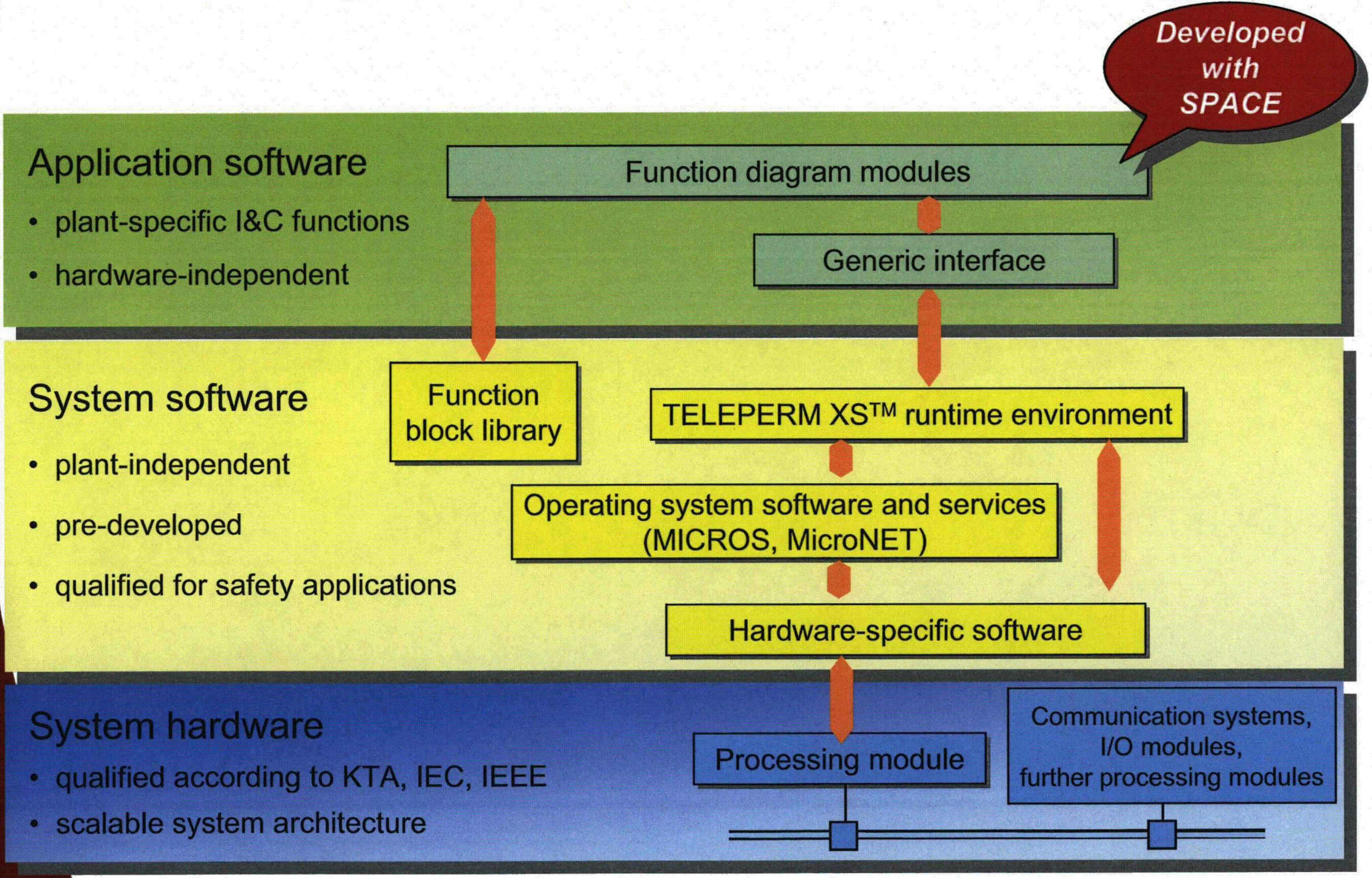
Closing

AREVA

Proprietary

Backup Slides

TELEPERM XS^{TM} System Platform Architecture
Layered Software Structure on a Processing Module



Developed with SPACE

Application software

- plant-specific I&C functions
- hardware-independent

Function diagram modules

Generic interface

System software

- plant-independent
- pre-developed
- qualified for safety applications

Function block library

TELEPERM XS^{TM} runtime environment

Operating system software and services (MICROS, MicroNET)

Hardware-specific software

System hardware

- qualified according to KTA, IEC, IEEE
- scalable system architecture

Processing module

Communication systems, I/O modules, further processing modules