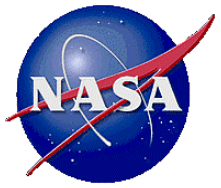
NASA
IV&V
Facility



IV&V Test Verification Methodologies in Highly Parallel Development Projects

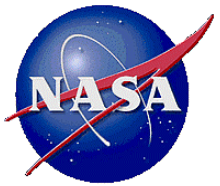
Sarma Susarla

IV&V team lead

Sarma.V.Susarla@nasa.gov

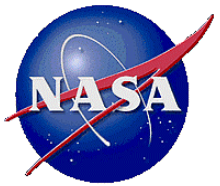
9/11/2012

IV&V Test Verification Methodologies in Highly Parallel Development Projects



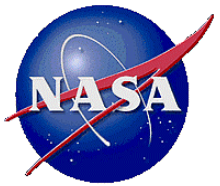
Presentation describes how IV&V performs CSCI's Formal Qualification Testing (FQT) reviews in sustaining phase of development in very large distributed System which has highly parallel development activities

IV&V Test Verification Methodologies in Highly Parallel Development Projects



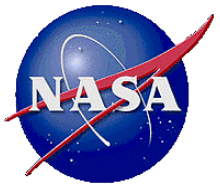
Contents

Introduction



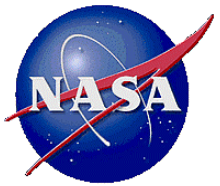
- **Formal Qualification Testing (FQT) verifies that the released CSCI software meets documented requirements**
  - Requirements Documented in Software Requirement Specifications (SRS)
  - Requirements also Documented in Interface Control Documents (Software interfacing requirements between):
    - The CSCI and other CSCIs
    - The CSCI and Firmware controllers Communicating to the CSCI through the hardware interfaces.
- **The CSCI is to be tested like a black-box with some exceptions here and there.**
  - Intrusive test code will be required to test FDIR requirements where hardware exceptions and faults have to be created.

Introduction



IV&V's Verification Objectives

- **Verify that the test cases are designed per the guidelines in the "*Houston Software Integration and Verification Test Design and Implementation Standards and Guidelines*", Reference item 5 of Table 2.**
- **Confirm that the test cases that are related to changed requirements are appropriately modified to test the changes in the requirement and the testing for the unchanged portion of the requirement is not affected.**
- **Confirm that new test cases are developed for testing new requirements and that these test cases fully verify the requirements.**
- **For requirements that use a Pre-Positioned Load (PPL) file, verify that the operational software behavior is verified for different PPL values.**
  - **PPL is a data table operational software uses during execution.**
  - **PPLs are changed to suit mission phase**
- **Confirm that the tests that verify code-only changes recreate the specific scenario described in the associated Software Change Request (SCR)**
- **Confirm that the test anomalies are correctly analyzed and software failures are reported correctly in new SCRs or reference existing SCRs.**
- **Confirm that test failures are traced correctly to the requirements.**



Introduction

CSCI life cycle

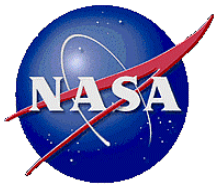
FQT Platform

Test Analysis

Test Review Process

IV&V's Test Review impacts

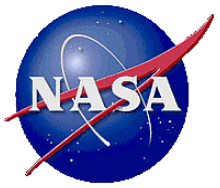
CSCI Life Cycle



- In normal Waterfall mode, the life cycle Sequence is SRR, PDR, CDR, TRR, and FQT.
  - IV&V performs artifact review and issue feed back for each of the reviews.
  - Review artifacts are normally provided 1 month in advance
  - This process enables IV&V to plan resource usage and support concurrently other CSCI developments
  - In large systems this model is only followed for the first release or first few releases
  - Subsequent releases following a different model.

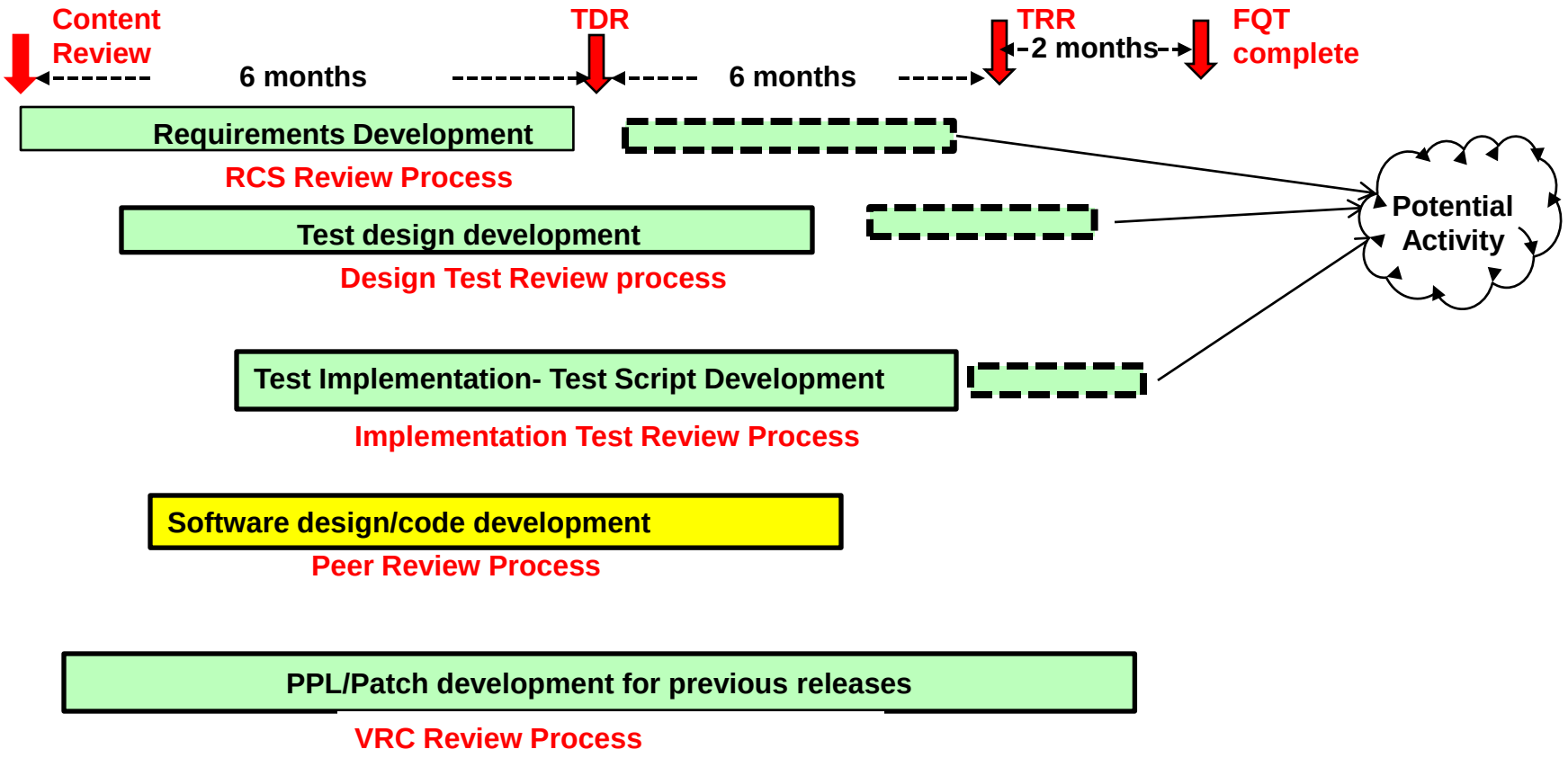
- Program Requirements driving a new development model in sustaining phase
  - New software release every year
  - Limited resources
  - Changes to baseline does not warrant extensive reviews
  - Parallel development activity to cut down total development time

CSCI Life Cycle

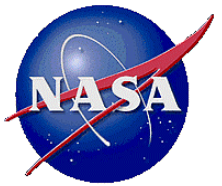


- **Highly parallel activities in sustaining phase**
  - Same team Working on multiple releases development
  - Developing new PPLs and code patches to operational software
  - Operations anomaly investigation
- **For each release the development activities run in parallel**
  - New Requirements development
  - Design/coding/ testing of approved requirements
  - Design of new test cases for new requirements
  - Test script development for designed test cases
  - FQT test dry runs on engineering releases of software
  - IV&V reviews and provides issue feedback as and when review artifacts are available in the above processes.
    - « Very limited review time (<a week) for each review

CSCI Life cycle

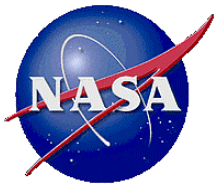


CSCI Life Cycle



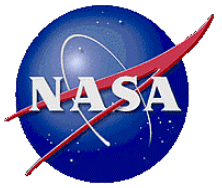
- **Sustaining engineering CSCI development life cycle**
  - **Content review**
    - **SCRs from Problem Database are selected based on:**
      - **Highest priority given by System development community organizations including IV&V**
      - **Eliminating Operational workarounds with code fixes**
      - **Ease of problem fix**
      - **Developer's resources availability**
  - **Technical Design Review (TDR)**
    - **Held after all requirement changes and new designs are complete**
    - **Combines SRR, PDR, and CDR**
    - **Only requirement and design changes from previous release are subject to review**
  - **Parallel FQT development**
    - **IV&V performs test analyses during this time**
  - **Test Readiness Review (TRR)**
    - **Held after all tests complete dryruns and reviews**
  - **Formal Qualification Testing**
    - **IV&V reviews test logs to verify anomalies are properly reported**

CSCI life cycle



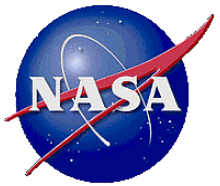
- **Each CSCI release following first release will be an incremental build of previous release**
- **New release content is established after a content review for the CSCI from documented problem reports, which contain:**
  - non-conformances
  - New functionality
  - Product improvements
  - pre-planned changes to match operational system configurations
- **Reviews are targeted to change content only (on Requirements, design, code, and test)**
- **Formal testing is generally a delta FQT where:**
  - **New and modified requirements are verified**
  - **Changes made to code only (without requirement change) are also verified**
  - **Regression tests to exercise each CSCI function is run**
  - **Software is exercised with default PPLs (Pre-Positioned Loads)**

CSCI life cycle



CSCI Example

- CCS R11 is the most recent release. CCS (Command &Control Software) is the largest CSCI (3 times larger than others).
- It provides for System level Commanding, Control , Safing, and Telemetry . It has:
  - 1418 SRS requirements (84 new or changed requirements) plus 408 applicable ICD requirements (23 ICDs)
    - « Many requirements have very large structure containing several sub-requirements
  - 121 SCRs in release content
  - 22 SCRs changed requirements, 28 SCRs changed code, 77 SCRs changed PPLs, 19 SCRs changed S/W parameter database(Standard Out)
  - Full FQT suite will contain 132 Tests containing 1826 test cases
  - Delta FQT suite (changed requirements/code) contains 30 tests containing 412 test cases
  - Regression test suite contains 67 Tests containing 864 test cases.
  - IV&V work load is much higher on test reviews than reviews on requirements and code for new releases



Introduction

CSCI life cycle

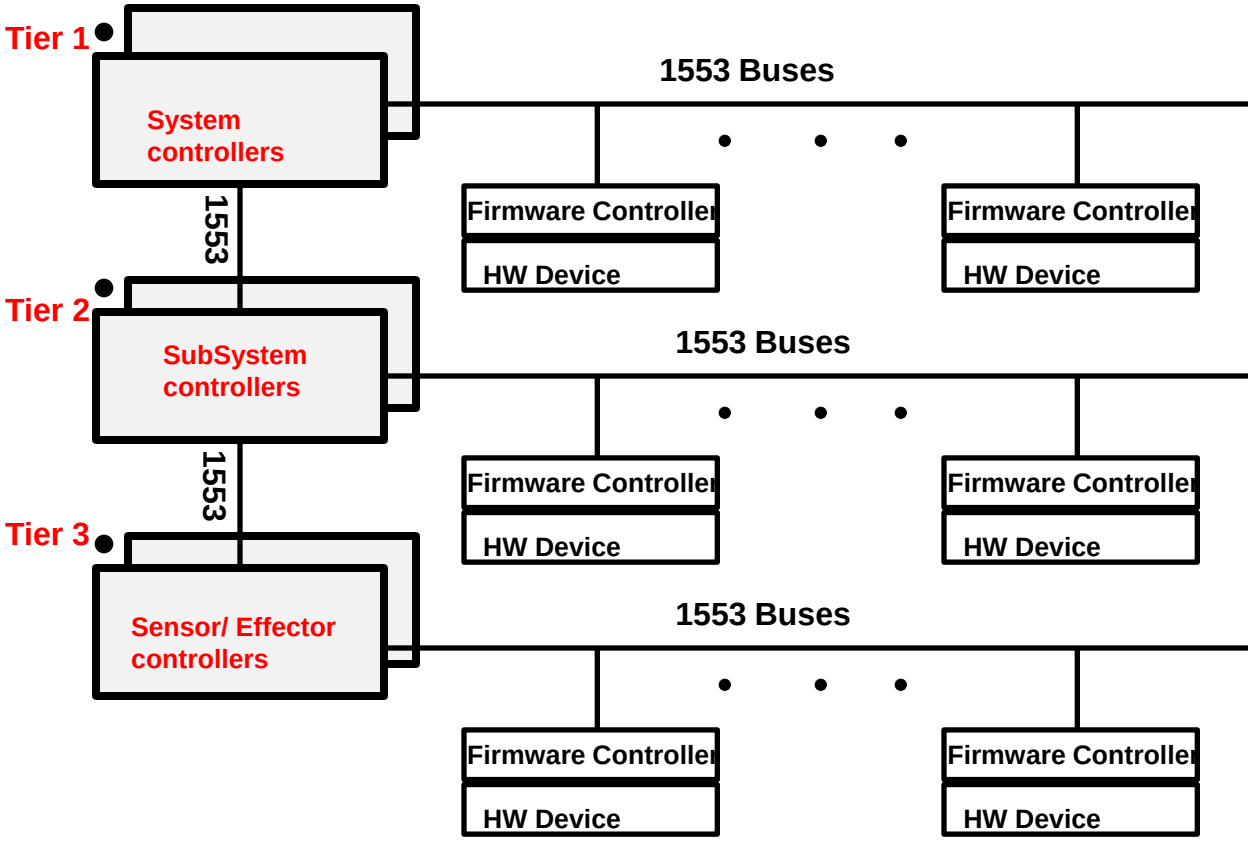
FQT Platform

Test Analysis

Test Review Process

IV&V's Test Review impacts

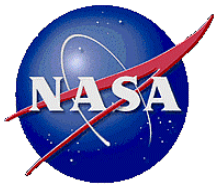
FQT Platform



Coputer System Architecture

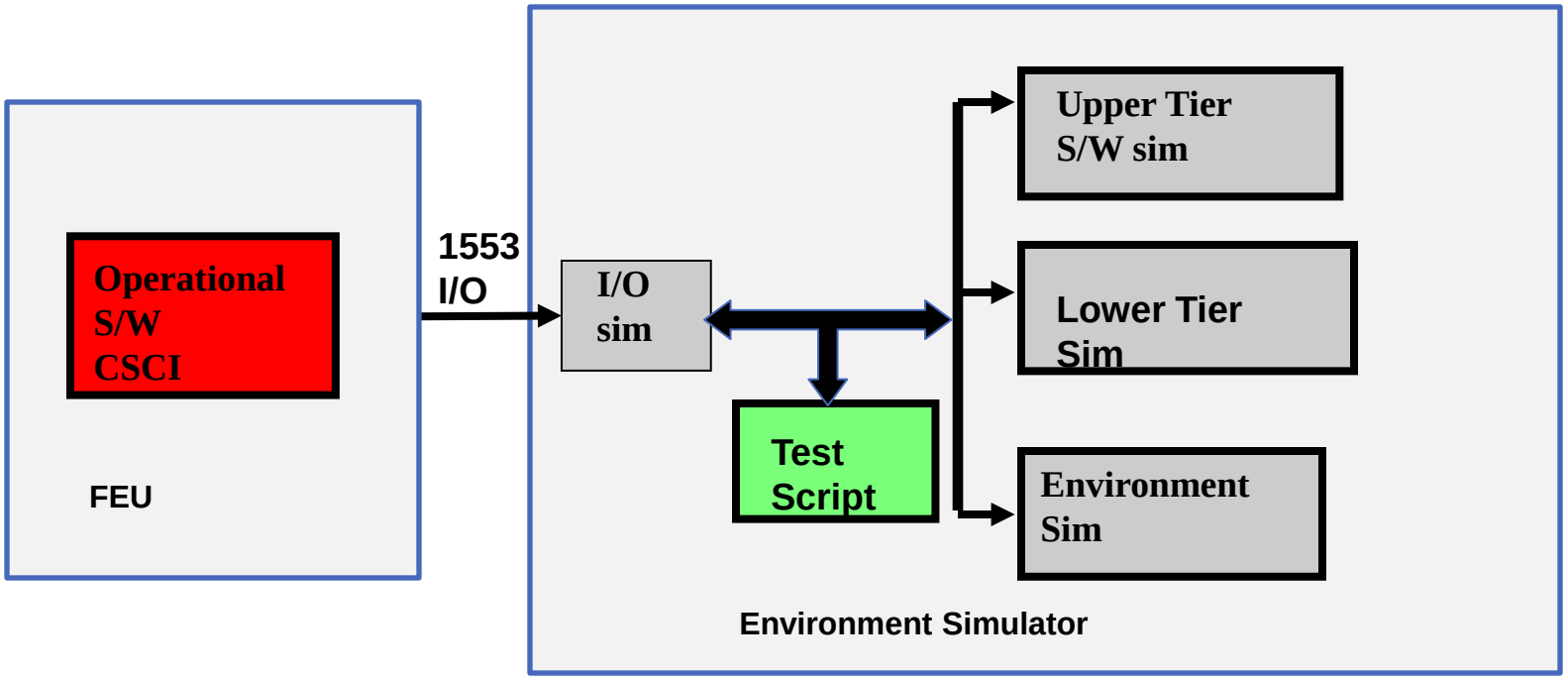
Hardware devices: such as:
- **Valve**
- **Fan**
- **Remote Power Controller**
- **Comunication equipment**
- **Audio equipment**
- **Etc.**

FQT Platform



- Figure shows Hierarchical Distributed connectivity architecture.
- Operational Software runs on Field Equivalent computers
- Top Tier has System level Command and Control Software(CCS)
- Second Tier runs software that control each subsystem: e.g. Guidance and Navigation, Thermal, Power, Environmental Control etc.
- Third Tier computers are grouped into subsystems and each group runs software that controls sensors and effectors for that subsystem
  - Each Controller runs a software CSCI that is designed for that controller
- Firmware controller runs specialized firmware that transmits device data to system controller and routes commands from system controller to the hardware device.
- Each CSCI is formally tested by the CSCI's test organization in FQT.
- After FQTs, CSCIs are tested in an integrated configuration in an operational configuration
- This presentation is focused on formally verifying in FQT that the CSCI meets its requirements

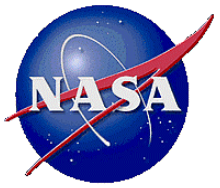
FQT Platform



- Operational S/W runs on Field Equivalent Unit (FEU)
- FQT test Script runs on simulator

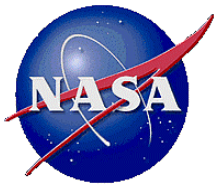
FQT Platform architecture

FQT Platform

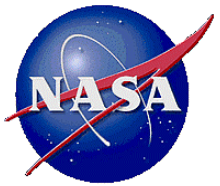


- **The Operational Software runs on Field Equivalent Unit**
- **The Environment simulator runs:**
  - Simulation software which simulates :
    - « Upper tier controller software's basic command/ data communications
    - « Lower tier controller software's basic command/data communications
    - « Low-fidelity simulation of hardware devices with limited closed loop responses for the Devices connected to the 1553 buses
    - « 1553/IO communications to the FEU
- **Simulation software CSCI is tailored to match each operational software CSCI release and is developed in parallel with the operational software development.**
  - Not in IV&V Scope
  - But IV&V analyst needs to be very familiar with the simulation architecture to assess correct requirement verification

FQT Platform



- The Environment Simulator also runs the test script developed by FQT group
- At the beginning of each test, its test script is loaded and executed
- Test script is developed in C and runs all the test cases defined under a test in a sequential order
- The script is implemented as per the test design documented in STD
- The script :
  - generates necessary stimulus signals to the software as per the requirement under test
    - « operator commands,
    - « sensor data
    - « Fault conditions
  - monitors the output of the CSCI (commands and Data) and Verifies that the operational software behavior and outputs match what is required in the SRS requirement
  - The script generates a log containing items such as:
    - « stimulus generation, output verification
    - « Pass/Fail status of each verification step
    - « Unexpected CSCI behavior anomalies
- The log can be examined to confirm that the test is executed as per design and all verification steps passed.



Introduction

CSCI life cycle

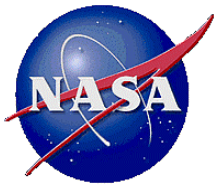
FQT Platform

Test Analysis

Test Review Process

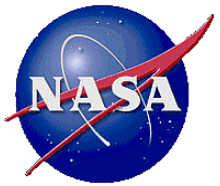
IV&V's Test Review impacts

Test Analysis



What do we do to verify the proposed test is correct and complete to verify the requirement?

Test Analysis



Format of a typical action requirement

If <condition a>

Then

Perform <action a> and

If <condition b>

then

Perform < action b>

Else no action

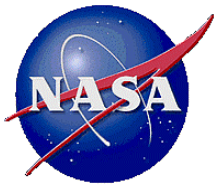
Else no action

- Each requirement can be viewed as a Boolean logic statement although written in plain English
- Each condition is a logical expression of configuration parameters, data parameters and function enable/inhibit states etc.
- The action could be: generate a command, or changing the value in a system parameter or generate a C&W event etc.
- There could be many nested if statements in one requirement

To verify the requirement:

- **There must be a separate verification of action for each predicate in the OR logic**
- **There must be a separate verification of no action if the condition is not met (negative test)**

Test Analysis
Sample Requirement



If any of the following conditions exist

(1) the Device Element Temperature is greater than Maximum Element Temperature for 3 consecutive readings

(2) the Device Baseplate Temperature is greater than Maximum Baseplate Temperature for 3 consecutive readings

(3) the Device Power Supply Temperature is greater than Maximum Device Power Supply Temperature for 3 consecutive readings

the software shall

1. Set the Device Over temperature Indicator to "In Alarm" (Initial value = "Return to Normal") and provide it to the Annunciate Alarms function,

2. If all of the following conditions exist

(1) the Device Overtemp Failure Reconfig is Inhibited

(2) the value of Device Heartbeat Indicator is "Return to Normal"

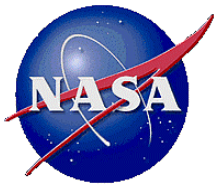
Perform the following

1. Issue the Power Off commands (arm and fire) for the Device

Table Operationally Modifiable Device Parameters

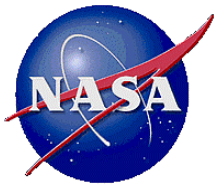
Name	Default Values
Maximum Baseplate Temperature	B max
Maximum Element Temperature	E Max
Maximum Power Supply Temperature	P max
Overvoltage Trip Limit	V max
Device Overtemp Failure Reconfig Flag	Enabled

Test Analysis



- **Analysis Steps**
  - Determine correct initial conditions of CSCI where the requirement would be effective
- **From the Requirement:**
  - Extract Triggers that will cause some action to take place
    - « Triggering parameters
    - « Triggering criteria
  - Extract all input and output parameters
  - Extract the CSCI actions
  - Extract any additional behavior specification such as:
    - « Data persistency checks
    - « Delays
  - Extract adaptation parameters
- **Analyze the test design to ensure all required verifications are present**

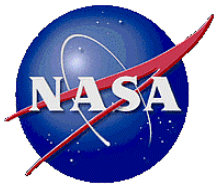
Test Analysis



- **Initial condition verification**
  - Before applying any stimulus to the CSCI, Test must verify:
    - « CSCI is in proper state
    - « Device over temperature alarm is not set i.e. Return to Normal
    - « Loss of Device heartbeat indicator C&W is not set i.e. Return to Normal
- **Two actions specified here:**
  1. Set Device over temperature indicator to Alarm
  2. Issue the Device Power off commands

  Setting alarm
  - Test must verify alarm generation when any of the three listed conditions are met. i.e. 3 separate verifications
    - –Device element temperature greater than Threshold (value specified in PPL)
    - –Device base plate temperature greater than Threshold (value specified in PPL
    - –Device power supply temperature greater than Threshold (value specified in PPL)
  - – Since the threshold value is adaptable and comes from PPL
    - « Test must change this to a new value and verify the alarm 3 more times

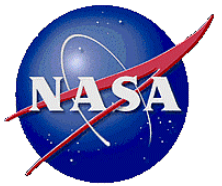
Test Analysis



Persistency verification

- Requirement specifies (3 consecutive data samples > threshold value) criterion for alarm generation.
  - So, for each of the three Device temperature parameters, test must verify
    - « Alarm is set only for 3 consecutive samples exceeding threshold value
  - There must be negative test to ensure that
    - « Alarm is not set when 3 non-consecutive samples exceeding threshold value are received
- It is important to verify that that the test script re-establishes initial conditions as needed before starting next verification step

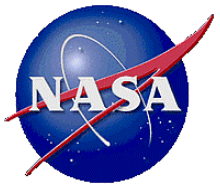
Test Analysis



- **Second software action calls for powering off the Device under alarm condition.**
- **But powering off is conditional as per the Truth Table**

Recon	Heartbeat	Action
Inhibit	Yes	Power off
Inhibit	No	No action
Enabled	yes	No action
Enabled	No	No action

  - **Test must be designed**:
    - « **To control the device heartbeat received by software**
    - « **Change the default Recon flag**
  - **Since the default value for Recon flag is Enabled, the test must verify that no power off commands are sent whether Heartbeat is present or not**
  - **Test must command the software to inhibit recon flag and verify that power off commands are sent when there is Heart beat and no commands are sent when there is no heartbeat.**
- **Overall for complete requirement verification there are 17 individual verification steps and each of them must pass and the test log should indicate that.**



Introduction

CSCI life cycle

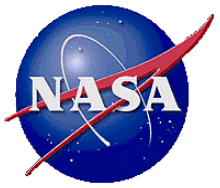
FQT Platform

Test Analysis

Test Review Process ⟹

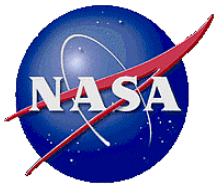
IV&V's Test Review impacts

Test Review Process



- **Assess the scope of delta FQT i.e. what needs to be tested.**
  - Develop a Requirement Database to track requirement changes for each release of the CSCI.
- **For each CSCI requirement the database indicates:**
  - New or modified requirement
  - If new or modified, the SCR that triggered the change and trace to the Requirement Change Sheet(RCS) that implemented the change
  - If requirement is unchanged, pass/fail status in the past release
  - For a failed requirement, the SCR number that described the anomaly
- **The Database is used by IV&V analysts:**
  - To verify creation of new test cases or modification to existing test cases
  - Determine adequacy of the proposed regression tests

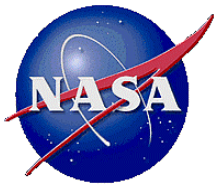
Test Review Process



Code only changes

- Some CSCI changes do not change requirements but change code only
- Such changes must be formally verified in FQT
- Corresponding test cases are documented the same way they are for requirements and go through the review process
  - Separate test case in STD
  - Separate test implementation review for dry run results
- IV&V will verify
  - that the Test script stimulates the software anomaly described in the SCR
  - the corrected software behavior if the problem is fixed

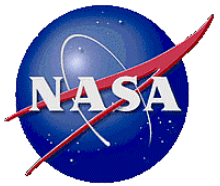
Test Review Process



- **FQT development Process has 3 phases**
  - **Test Design Phase**
    - « Decide on unique Tests for each CSCI function or Sub-function requirements
    - « Decide on the test cases that would verify each requirement or part of a requirement or code only changes
    - « Determine the requirement trace, CSCI inputs, outputs, initial conditions, execution logic flow and verification criteria for each verification step
    - « Document the design in Software Test Descriptions (STD)
    - « There will be several DTR reviews, each review targeted for a group of tests
    - « Test Design (STD) is reviewed against the requirements and code only changes
- **Next chart shows a typical description of a test case in STD**
- **IV&V uses this, before the script is developed, to confirm that the test is designed to fully verify the requirement**

NASA IV&V Facility

Test Review Process
Test Case Format in STD



- **Initial Condition**
  1. CB Channel Switch Inhibit Status = FALSE.
  2. Bus has not been switched within the last 10 seconds.
  3. RT I/O Status for the RT is TRUE.
  4. RT FDIR Inhibit Status for the RT is FALSE.
- **Objective**

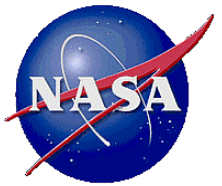
  Show that when CCS detects transaction errors in two non-consecutive status cycles for an RT whose RT FDIR Inhibit Status is FALSE and the CB Channel Switch Inhibit Status is FALSE, CCS performs no fault response.

  1. Confirm the current value of the CB Channel Switch Counter for the bus.
  2. Confirm the current value of the CB Error Counter for the bus.
  3. Confirm the current value of the CB Channel Select Status for the bus.
  4. Create a transaction error in one status cycle.
  5. Verify that the CB Error Counter for the bus increments once.
  6. Wait one status cycle.
  7. Create a transaction error in one status cycle.
  8. Verify that the CB Error Counter for the bus increments once.
  9. Verify that CCS does not switch to the other bus channel by validating the following:
  10. Verify CB Channel Switch Counter has not incremented.
  11. Verify Channel Selected Status has not changed, reflecting the same active bus channel.
- **SRS/SCR Reference and Qualification Method**

  3.2.16.3.a Test

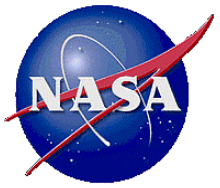
  d. ICD Reference none
- **Assumptions and Constraints**
  - Performed for each FDIR RT defined in the CCS release.
  - This one test case is sufficient to prove that non-consecutive transaction errors do not cause failure responses to occur.

Test Review Process



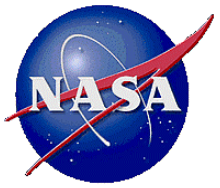
- **Design Test Reviews**
  - **Scheduled when requirement change process for a group of Tests completed and new test designs (including for code only changes) are worked in STD**
  - **IV&V's analysis consists of:**
    - **Review SCRs triggering requirement changes and ensure that requirement change captures the intent of recommendation in SCR**
    - **Ensure that the test case is designed/ or changed only to verify the new requirement or changes made to existing requirement (comparing previous and current STD versions)**
    - **Ensure that negative test cases are specified as per FQT Standards and Guidelines**
      - **i.e. verifying software does not do what it is not supposed to do**
    - **Ensure that requirement is tested at boundary values of input parameters**
    - **For requirements that use adaptation parameters:**
      - **verify that the test inputs new parameters and the software behavior changes due to new parameter**

Test Review Process



- **Test implementation phase**
  - **Starts after Test Design is completed and reviewed for a test**
  - **Test scripts are developed per STD**
  - **Tests are dry run and the software defects found are reported via formal problem reports (SCR)**
  - **ITR for a test will follow DTR regardless of the development of other tests**
  - **Test logs, test scripts , changes to STD, and any latent requirement changes are reviewed at each ITR**

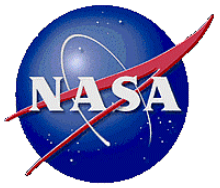
Test Review Process



Implementation Test Reviews

- **IV&V's analysis consists of:**
  - **If Test design changed after last DTR, ensure that Test design changes are correct**
  - **Perform a high level script review and ensure that the script matches design documented in STD**
  - **Ensure that the Input/Output parameters used in the script match the data definitions system database**
  - **Examine log and verify that the test stimulus to CSCI is applied as stated in STD**
  - **Analyze the script and ensure that it matches its STD description.**
  - **Examine log and ensure that there is evidence that verification steps specified in STD are executed**
  - **Examine the log and verify all required individual verification steps passed**
  - **If any verification step did not pass or if there is some other anomaly in log, verify that the problem is referenced to an existing or new SCR**
  - **Read the SCR's problem description and confirm that the anomaly or failure noted in the SCR is adequately described**

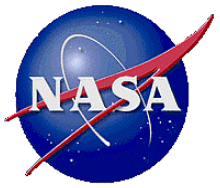
Test Review Process



Regression test analysis

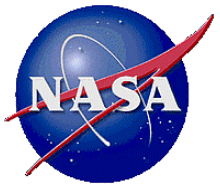
- For each delta FQT, FQT team will propose a set of regression tests
- These tests exercise CSCI's applications that are not covered in the requirement changes
  - CSCI is composed of several individual applications each of which is designed as a separately scheduled function
  - Each regression test will cover a set of critical requirements in an application
- IV&V will review the adequacy of this test suite and recommend additional tests if they do not cover all applications

Test Review Process



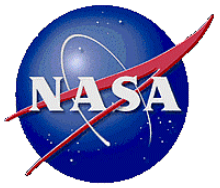
- **Adaptability verification**
  - « **Some input/output parameters in requirements are specified in SRS as adaptable during software operation:**
    - ‹ **Changed by operator commands , Or**
    - ‹ **Changed by loading a new Pre-Positioned Load (PPL)**
    - ‹ **Software is loaded with default PPLs (CCS R11 has 222 default PPLs)**
    - ‹ **New PPLs are generated to suit mission phase and loaded by Operator command when needed**
- **IV&V will verify both in STD and Test Script that where adaptability is specified in the requirement:**
  - **Operational software can take a PPL load for the data set**
  - **The new data set becomes effective in software behavior after the load**

Test Review Process

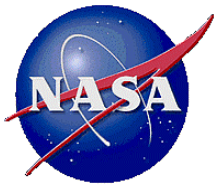


- **Test Readiness Review**
  - **After all tests complete ITR , a Test Readiness Review (TRR) is taken**
  - **Usually, by TRR all test issues are worked and software is ready for FQT immediately following TRR**
  - **At TRR, the test scripts, test logs, and updated STD are presented for review if there are any changes(very rare) after ITR reviews**
- **Formal Test Phase**
  - **Tests are run on configuration controlled FQT rig**
  - **Test runs are witnessed by Software Quality Assurance**
  - **Formal test report is generated after running all tests**
  - **If any new software defects are found (which is very rare), new Problem reports are generated.**
  - **IV&V ‘s role is limited to reviewing additional Problem reports that are generated and reviewing test logs to ensure test anomalies are properly accounted**

Test Review Process



- **Post-FQT test verifications**
  - **New PPLs and code patches will be generated for CSCI operational configuration**
    - « **As needed to correct problems**
    - « **As needed to match changing System hardware configuration**
  - **These will be formally tested both at FQT level and at Integrated CSCI level (Stage Testing) as needed**
  - **IV&V reviews these tests to ensure:**
    - « **Intended new software behavior is verified**
    - « **The change does not produce side effects**
      - ‹ **Verify relevant regression tests are run**



Introduction

CSCI life cycle

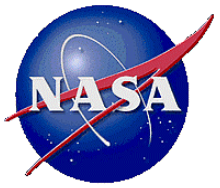
FQT Platform

Test Analysis

Test Review Process

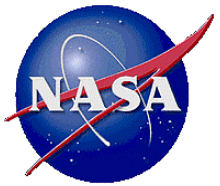
IV&V's Test Review impacts

IV&V's Test Review Impacts



- **Includes both Process and Product impacts**
  - **Major test issue contributor for all reviews.**
    - « **Roughly 30% of issues change scripts before they run in FQT**
      - ‹ **Some of these uncovered operational software problems which resulted in generating an operations note for the current release and code fix in a later release.**
    - « **Remaining issues change STD**
  - **Complete revamp of STD to describing the design of each test case from mere rewrite of requirements**
  - **Adding negative test cases for conditioned requirements**
  - **Convincing the Program to go for full FQT instead of delta FQT when CSCI changes were extensive**
  - **Convinced the Program to develop a CSCI stress test separate from CSCI sizing and Timing test**
    - « **This became necessary as nearly 85% of CPU is being used with occasional task overruns**
  - **Found major testing flaws in Firmware controlled Environmental Control Units developed by vendors**
    - « **Resulted in Enhanced re-testing of those units**

IV&V Test Verification Methodologies in Highly Parallel Development Projects



Questions/Comments