

Suggested Checklist to Improve Test Performance in the System Test Equipment Area

21 May 2009

John C. Cantrell¹, David Gianetto², Robert Atkinson³, Marcia Edwards⁴,
Michael McKeown⁵

¹Software Architecture and Engineering Department, Software Engineering Subdivision,

²Raytheon Corporation, ³Northrop Grumman Corporation, ⁴Lockheed Martin Corporation,

⁵Ball Aerospace and Technologies Corporation

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

Developed in conjunction with Government and Industry contributions as part of the
U.S. Space Programs Mission Assurance Improvement workshop.

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

Suggested Checklist to Improve Test Performance in the System Test Equipment Area

21 May 2009

John C. Cantrell¹, David Gianetto², Robert Atkinson³, Marcia Edwards⁴,
Michael McKeown⁵

¹Software Architecture and Engineering Department, Software Engineering Subdivision,

²Raytheon Corporation, ³Northrop Grumman Corporation, ⁴Lockheed Martin Corporation,

⁵Ball Aerospace and Technologies Corporation

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Space Systems Group

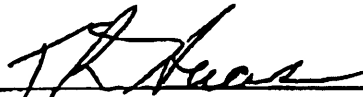
Developed in conjunction with Government and Industry contributions as part of the
U.S. Space Programs Mission Assurance Improvement workshop.

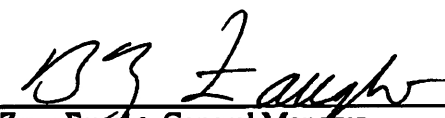
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AEROSPACE REPORT NO.
TOR-2009(8591)-12

Suggested Checklist to Improve Test Performance in the System Test Equipment Area

Approved by:


Thurman Haas, Principal Director
Office of Mission Assurance and
Program Execution
National Systems Group


B. Zane Faught, General Manager
Computers and Software Division
Engineering and Technology Group

Contents

1.	Introduction	1
1.1	Background.....	1
1.2	Definition of Terms for the Checklist and This Document	4
1.3	Anticipated Uses of the Team Products.....	4
2.	Explanation of Checklist	7
2.1	Safety.....	7
2.1.1	Safety Provisions.....	7
2.1.2	Emergency Procedure	7
2.1.3	Capable and Able	7
2.1.4	Safety Features.....	7
2.2	Test Preparation.....	7
2.2.1	Validation of Changes.....	8
2.2.2	Certifications.....	8
2.2.3	Understanding of Test Configuration	8
2.2.4	Understanding of Test History.....	8
2.2.5	Executability	9
2.3	Alert, Alarm Management.....	9
2.3.1	Understanding Alarm Logic	9
2.3.2	Alert/Alarm & Anomaly Actions.....	9
2.3.3	Expected Out-Of-Limits.....	10
2.4	Test Configuration Management.....	10
2.4.1	Knowledge of Initial/End State.....	10
2.4.2	End-To-End Check of Test Configuration	10
2.4.3	Verification of Change Process.....	10
2.4.4	Test Flow Workarounds.....	10
2.5	Special Actions.....	11
2.5.1	Unsafe Commands/Actions	11
2.5.2	Undefined/Anomalous States	11
2.5.3	Special Test Operations	11
2.5.4	Transitional Conditions.....	12
3.	Checklist Tailoring Suggestions.....	13
4.	Areas for Future Work.....	15
5.	Appendix (Checklist).....	17

Acknowledgment

This document was created by multiple authors throughout the government and the aerospace industry. For their content contributions, we thank the following contributing authors for making this collaborative effort possible:

Reena Byrne—The Boeing Company

Mike McKeown—Ball Aerospace

Robert Atkinson—Northrop Grumman Aerospace Systems

Marcia Edwards—Lockheed Martin

A special thank you for co-leading this team and efforts to ensure completeness and quality of this document goes to:

John Cantrell—The Aerospace Corporation

Dave Gianetto—Raytheon

1. Introduction

1.1 Background

The Steering Committee for the Mission Assurance Improvement Workshop for 2009 selected topics that it believed would contribute to the overall goal of mission assurance. One of that topics that the committee felt should be investigated was test equipment/test procedures. At the kick-off meeting in October, 2008, representatives from several organizations, both contractors and government, were given the opportunity to join this topic team. The authors of this paper formed the core team members working on this topic.

The starting point for the work of the “Test Equipment/Test Procedure Team” was a master’s thesis by Annalisa L. Weigel titled “Spacecraft System-level Integration and Test Discrepancies: Characterizing Distributions and Costs.” (MS, Department of Aeronautics and Astronautics, Massachusetts Institute of Technology, June 2000.) After reviewing this document, it was evident that the greatest number of system-level test discrepancies was written against test equipment (approximately 30%). This narrowed the team's primary focus to test equipment with procedures being a secondary contributing factor.

As test equipment was a very broad topic, the team first discussed areas to attack with the intention of providing something that would be of immediate help to the engineers running system tests currently. The team did not originally narrow the field of consideration for this. Instead, we intentionally left everything wide open, to be discussed by the team and either included or not. An initial brainstorming session of the team focused on test equipment issues resulting in a list of nine common problems that team members had encountered. These were, in no particular order:

1. Fragility/past end-of-life issues for the test systems,
2. Operator error,
3. Documentation of the test system,
4. Robustness of the test system (i.e., it meets requirements, but just barely),
5. Data dropout or loss,
6. Configuration control errors,
7. Software coding errors,
8. Unexpected behavior of the test system (again, it meets requirements, but has quirks), and
9. Initialization/shutdown issues.

Using this list, an informal survey was conducted with test subject matter experts (SMEs) from different contractors. They were asked to rank the issues in order of occurrence. In addition, they were asked to incorporate any other problems that were missing. While no new items were added, the ranking came in with the top three listed above as being most problematic. This brought more focus to the information with a finer resolution than that provided by Weigel's paper. The sample size of SMEs for this survey was small (8 total, 5 from Northrop Grumman, 3 from Raytheon) but the fact that agreement was almost universal on what caused the most trouble helped the team focus on fewer areas. Although the remaining items in the list were considered important, the time allotted for this work did not allow for thorough investigations of all the ideas proposed. Instead, these items were captured and are discussed later in this paper.

With these results, the team narrowed the approach to look more closely at the top three issues of the list. When considering the fragility/past end of life issues, the team theorized that the design area had less potential for study at the system test level due to the fact that the test systems are usually capitally owned by the corporation. Generally, a corporation wants to maximize the use of a test set before investing in new equipment, and suggesting that corporations invest in new test sets for each program would not be well received. Next, the team looked at the documentation problem. Those systems lacking documentation would not benefit significantly in the near term from a recommendation in this area, as the SMEs are the most knowledgeable and would lack the time to write documentation. Also, imposing enhanced documentation requirements on new test systems, while a worthwhile activity, would have little impact at the system level as most test equipment is a capital asset reused from program to program. In view of these considerations, the team focused on the operator error category as the one that would bring the most benefit. Operator errors (or interaction errors), though individually may not amount to a high impact, overall, have a high total impact on a test program.

It is important to note that the category “Operator Error” encompasses all interaction-based errors with operators and test systems, irrespective of cause. It is not passing judgment on the operator by the notion of an “operator induced error.” To help clarify this point, the following events should be considered within the scope of this operator error category:

1. During the performance of a test, the technician failed to perform a given command causing failure to trigger a response. Analysis of the failure indicated a significant amount of technician interaction and repetitive motion (turn switch / press button) leading to the technician losing track of the sequence of events. While this clearly was an operator error, a better solution would have been improved test equipment design reducing manual intervention and developing a more automated approach.
2. In 2004 during ambient pre-thermal vacuum testing, a persistent out-of-limits condition occurred on an electronics box, which resulted in near-overstress of hardware. This resulted in a mandatory test stoppage of several weeks, impacting program schedule.
3. During the early integration phase in 2003, a system test was executed with a special configuration of the unit under test. Operators were unaware of the consequences of this configuration would have on the test results. Extensive troubleshooting caused the loss of several days of test time.

After focusing on the operator error issue, it was apparent that the work product in consideration should be a practical tool for the test operator on the floor, rather than a guidance document or other scholarly work. To this end, a checklist that focuses on reducing discrepancies due to interaction issues of operators and equipment (operator error) should be developed.

The checklist represents a generic tool that a contractor could tailor to individual circumstances, and contains the key things the operator and test team members should be cognizant of during test operations.

The checklist will focus on the following areas:

- Safety (operator and hardware)

- Test preparation
- Alert and alarm management
- Test configuration management
- Special actions

1.2 Definition of Terms for the Checklist and This Document

COTS	Commercial off-the-shelf
GSE	Ground support equipment
HW	Hardware
ID	Identifier, identification
OCP	Overcurrent protection
OOL	Out of Limits
Operator	See Tester
OVP	Overvoltage protection
PM	Preventive maintenance
QA	Quality Assurance (department)
STE	System test equipment
STR	Special Test Request, written change to a test procedure, to be executed for some out-of-sequence testing.
Subject Matter Expert (SME)	Person familiar with a particular subsystem, for example, a star tracker, or the attitude determination and control system
SW	Software
TE log book	Test Equipment log book, record containing all changes and anomalies of any type occurring during testing
Test conductor (TC)	Person in supervisory role charged with testing, usually during one shift
Test director (TD)	See Test conductor
Test Engineer	See Tester
Test lead	See Test conductor
Tester	Person actually conducting the test
TV, TVAC	Thermal Vacuum {chamber, testing}
UUT	Unit Under Test

1.3 Anticipated Uses of the Team Products

The goal of the team was to create a checklist that could be used as an immediate tool to enable the test lead, and the testing team members to think about what needs to be done before actually touching any equipment. Over the course of our discussions, the team realized that different contractors use different terminology and have different processes, but the checklist and description document focused on the general course of events that all contractors had (or should have) in common. As work progressed, the team realized that the checklist was not just something to be used on the day of the test. Rather, it could be used as an aid in several other test and planning activities more far-reaching than just the actual test process itself.

The team's first thought was that the checklist would be used whenever there was a change in the configuration of the test system environment. Such changes would of course include additions or modifications of the test equipment or cabling. Furthermore, they also encompass any changes to the makeup of the testing team itself. In addition, whenever a new member joins the team, whether just new to this particular project or new to system testing in general, the checklist should be applied to ensure that the new member is familiar with test equipment particulars such as emergency procedures or any STE peccadilloes that may be of concern to test operations.

The checklist may also be applied at a change of shift. Usually there are meetings when the two shifts overlap so that the outgoing shift can brief the incoming shift of any anomalies or off-nominal conditions that may have arisen during the outgoing shift. While the test logbook should contain any testing anomalies, it might not contain special test requests that were performed and that might have a lingering effect on the test configuration. It is true that the special test requests provide traceability, but they may be overlooked at the end of a shift.

What's more, the checklist can also be used for checking the validation of the STE itself, which must be performed as part of the test system change-management process.

When reviewing the testing procedures to be used, the checklist can be used to ensure that the procedures contain provisions against operator error. In addition, if there are deviations from the written procedures, due to some subsystem not being ready for testing, the checklist will call to mind the test steps that need to be omitted or the extra steps that need to be inserted. Such preparation makes dry-runs of the procedures much smoother.

Finally, the checklist can actually be used during the planning phase for the design reviews of the GSE/STE. Even as early as the make/buy decision, the checklist can help clarify what might be termed "hidden costs" at such an early stage of the project. For example, if an existing system is being considered, how much effort will be required to validate the STE for this project? Such considerations may be overlooked in the rush to claim corporate assets that are about to be discarded by an ending project.

With these considerations, the field of application of this checklist is expanded greatly, spanning from initial planning stages to test operations and test system change management.

2. Explanation of Checklist

2.1 Safety

2.1.1 Safety Provisions

Has the operator read the safety provisions outlined in the test procedure?

If the safety provisions are not understood within the current procedure sequence then mistakes may be made that endanger the test article, such as hazardous situations encountered during test execution. Confirmation that the operator understands the safety aspects of the procedure is imperative to reduce the risk of critical errors. A check should be performed prior to test execution that the operator has reviewed and confirmed knowledge of safety provisions.

2.1.2 Emergency Procedure

Has the operator demonstrated understanding of the emergency safing procedure content?

An emergency procedure should be available at all times to test team members. If the emergency procedure location and contents are not known or understood, unacceptable or unsafe delays may occur in the execution of the procedure should emergency conditions exist, subjecting the test article to more stress than desired. Operators should acknowledge that the emergency information is known and understood. Quick and smooth access to the emergency procedure is expected.

2.1.3 Capable and Able

Is the operator capable and able to effectively perform the subsequent test sequence as described?

This step confirms that the test sequence in question is executable by the operator. For a variety of reasons the operator may not be able to execute the test sequence as prescribed, including time sensitive operations, coordination required with other personnel, or physical limitations.

2.1.4 Safety Features

Have protective (automatic and manual) features been validated appropriately and demonstrated prior to first use?

The functional verification of protective features (such as over-voltage and over-current protection) should be executed prior to test system first use, and the evidence of this verification should be captured in the test system validation procedure. As this feature is safety critical, the test operator should be cognizant of the protective feature verification status, which may include a visual check of the test-system-validation procedure.

2.2 Test Preparation

This section provides four specific steps that can be taken prior to testing to help reduce the probability of test operator errors.

2.2.1 Validation of Changes

Have all test equipment changes been validated?

Ensure all test equipment modifications have been validated. This step ensures that all modifications to either hardware or software elements have been completely tested and are well understood and documented. Operators should understand any change in expected results and/or functionality based on the changes. If not well understood, the operator has a greater potential to accept functionality that may be marginal or even erroneous. Or worse, if the software has a “new look,” errors might be induced by the operator pressing unfamiliar “soft keys” without understanding the results. These changes should be well documented in a log book or some document that is reviewed by the operator. This step reduces the risk associated with the functionality of test equipment.

2.2.2 Certifications

Do operators have all required certifications to run test (program-specific certifications)?

Valid certifications ensure that the test operator has received and passed all prescribed training to successfully run the planned test. The certification training should include information on safeguarding personnel and equipment, including dry run of emergency procedure(s). In the data entry section for this step of the checklist, the operator should list their applicable certifications and dates of expiration. Only operators with the necessary and valid certifications should be allowed to run planned tests to safeguard personnel and equipment.

2.2.3 Understanding of Test Configuration

Does the operator understand how the test equipment interacts with the product being tested, including a basic understanding of the test configuration?

Having a good understanding of the system being tested reduces the chance of making operator test errors, which potentially could damage the products being tested, the test equipment or test personnel. It is strongly recommended that prior to running a test sequence, the operator should “dry run” the steps with an experienced and knowledgeable test mentor (or supervisor) to increase test operator knowledge of what to expect during the test, including any expected anomalies and alarms. Both the name of the test operator and the person certifying that the operator has all the required knowledge should be written in the data entry section for this step.

2.2.4 Understanding of Test History

Has operator reviewed recent (e.g., 24-hours, last shift, last time test was run) test events? *Example of things to review: event log book, shift handoff, anomaly reports, lessons learned, watch lists.*

Prior to running a test, the operator should review the test-set log book to review if recent tests with the test equipment and UUT have been completed successfully and learn if any unexpected events or

anomalies occurred. The test operator should write down the date of the latest entry from the test set log book in the data entry section for this step. By reviewing the log book, the test operator can be made aware of recent activities using the test equipment and gain an understanding of any unusual or anomalous conditions that occurred.

Provide a methodology or requirement to preview upcoming events to ensure the operator is aware of critical operations that will occur. This step will improve the operators understanding of these critical operations, and bring out any interpretation issues prior to the critical step.

2.2.5 Executability

Can the test sequence be reasonably performed before preventative maintenance (or calibration) is required?

Information regarding the status of preventive maintenance provides a known state of the test equipment by demonstrating prior to use that all components and total test console and/or equipment are functioning as required. This does not mean that components can not fail in the process, but does allow the operator to begin the process with confidence in the functionality of the equipment. Visual evidence of calibration dates verifies the ability to begin testing without concerns of equipment “going out of specification” during the test. Both of these activities reduce the risk of failures attributed to test equipment. Use of a log book is recommended for easy access to status.

2.3 Alert, Alarm Management

2.3.1 Understanding Alarm Logic

Is the operator knowledgeable of audio/visual alert/alarms, indicator logic for this test configuration?

A detailed explanation of visual queues and human/machine interface alerts/alarm features are often not captured within individual test procedures, but within user manuals and standard operating procedures that are used as reference material. This step confirms that the operator is familiar with the safety-related features outlined in this external documentation.

2.3.2 Alert/Alarm and Anomaly Actions

Has the operator demonstrated knowledge of the appropriate action(s) to take to out-of-limit conditions (or anomalies encountered) in the upcoming test sequence?

This particular step should also apply to the environment beyond the UUT and the STE such as a fire alarm or any condition requiring a quick exit from the building while testing is being performed. Prompt recognition of critical failures or other emergency conditions allows shutdown of the test before damaging the UUT. Here, the review is intended to identify signs of critical failures so that operators can quickly recognize them and react properly. Also, this should verify that the procedure has been fully tested prior to UUT testing. This review should reduce the risk of damaging equipment. Feedback from operators may result in better and more consistent failure reporting from the STE.

2.3.3 Expected Out-Of-Limits

Is the operator knowledgeable of expected out-of-limit conditions in upcoming test sequence?

Some instances of out-of-limit (OOL) conditions may be planned for tests. Explicit identification of these conditions prepares the operator to differentiate between planned and unplanned OOL conditions. This should eliminate the necessity of aborting the test when such conditions are expected due to the state of the unit under test. Here, the test conductor and test team should identify planned OOL conditions and provide preparation for the operator in documented form. Such preparation reduces the chance of continuing a test under dangerous conditions and provides for efficient (schedule and cost) testing with planned OOL conditions that do not result in unnecessary test stoppages.

2.4 Test Configuration Management

2.4.1 Knowledge of Initial/End State

Is the operator aware of the beginning and end state of the unit under test and test equipment during the test sequence?

Before starting a test sequence, the beginning and ending state is key to managing the test configuration and prerequisites for the following test. If an anomaly occurs and procedures are unclear on how to proceed, the operator can attempt to put the system back in the original state or final state of the test sequence which limits the operator's options and improves decision making clarity.

2.4.2 End-To-End Check of Test Configuration

Have the test configuration items (e.g., STE, SW, HW, databases, cables, auxiliary equipment) been integrated and validated as a system prior to the test sequence?

It is important to completely wring out a test configuration with all configuration items present in as realistic an environment as possible prior to for-record test operations. These dry runs will improve confidence of the test team in the test configuration and expose systematic issues that could affect subsequent for-record test operations.

2.4.3 Verification of Change Process

Have all test system changes been reviewed, approved, documented, and communicated to the operator by the responsible engineer?

This step ensures that the operator is aware of test system changes in process, which helps to avert any misunderstandings as to the current test system state of change during test execution.

2.4.4 Test Flow Workarounds

Have all test flow workarounds been communicated to the operator?

It is important to have a comprehensive understanding of issues addressed by workarounds. This step ensures all participants in the test process understand any out of sequence or out of position activity that may have occurred during the test process and the effect it may have on the test. For example, because activity is not being performed in the predicted order, any “side effects” must be well understood by all to ensure adequate testing is being accomplished. The focus of this activity ensures that documentation exists explaining the workarounds and any additional steps that must occur. This reduces the risk when working outside the “normal” process.

2.5 Special Actions

One item that should not usually present a problem is the state of understanding of the test equipment by the operators. However, this is often not the case, especially when a new factor is introduced. This factor might be a new member of the test team, a new piece of equipment (either in the unit under test or in the test equipment itself) or a new procedure. The intent of this portion of the checklist is to make the test director think about various issues that may not be a problem if addressed early but that could cause schedule delays if not.

2.5.1 Unsafe Commands and/or Actions

Is the operator aware of all invalid or unsafe actions or commands that would negatively affect the current test configuration?

Often, the system test equipment (STE) is qualified as a stand-alone item. When combined with other equipment in new configurations, its performance may change and other equipment may fulfill functions previously accomplished by this STE. This step is to remind the integration and test team that the procedures should be reviewed to identify and restrict critical commands for the equipment in this configuration. Restricting or identifying critical commands reduces the risk of issuing commands that can damage the item under test.

2.5.2 Undefined and/or Anomalous States

Are there any undefined and/or anomalous states expected in the upcoming test sequence?

When anomalous states are expected in a test sequence, including things like telemetry dropouts and out-of-limits, the operator should be knowledgeable of these states up front such that they are taken in stride and test continues in a smooth manner.

2.5.3 Special Test Operations

Is the operator instructed on what to do for any out-of-sequence or special operations (e.g., who to contact, resources needed)?

Damage to the unit under test often results when the operator goes off the test script either in redlining the procedure or for troubleshooting purposes. Deviation from the test script may also be due to some portion of the unit under test being unavailable at this particular time. Such situation may require the operator to specifically skip steps in the procedure. To ensure that this situation does not cause problems, the test director should identify the SME to the operator, assure that the configuration

controlled procedure is followed, and ensure that all proposed changes to the procedure are appropriately reviewed prior to execution. This will reduce the risk of damage to the unit under test and promote communication between the SME and the operator providing a better understanding of the risks and test objectives.

2.5.4 Transitional Conditions

Is the operator knowledgeable of expected transitional conditions, alarms, states in the upcoming test sequence (e.g., TVAC plateau changes)?

Explicitly identifying state changes prior to testing prepares the operator to issue only appropriate commands related to that state. Reviewing the expected conditions promotes communication between the TC and operators. This step reminds the TC to identify the expected states and sequences and the appropriate actions when these states are encountered for all members of the testing team. Recognition that the equipment is not in the expected state, as specified during the state review before the test, will be a red flag to proceed with caution or to shut down and reinitiate the test. This review also anticipates questions to SME regarding states which might occur when the SME is unavailable.

3. Checklist Tailoring Suggestions

During the initial session by the team, it became obvious that different contractors have different terminology. For example, the title used to designate the person in charge of overall testing during one shift might be “Test Director” at one contractor but “Test Conductor” at another. Then, the “Test Conductor” at a contractor would be the “Test Engineer” or “Tester” at another. In addition, the development or testing practices followed by different contractors sometimes overlap and sometimes not. Once this came out, it became clear that having only one checklist would have a difficult time satisfying the internal terminology requirements for each contractor who might use the checklist.

With this in mind, the team wanted to ensure that terms that might cause confusion were defined well enough here to mitigate any consequences. Providing the checklist in a flexible format would also allow individual contractor testing teams to change those terms that might be misunderstood into contractor-specific terms.

While the team has attempted to be consistent throughout this document and the checklist, any suggestions for improvement are greatly appreciated.

4. Areas for Future Work

This section serves as an area where the team could collect ideas that were considered and then dropped for the current project. This was mainly due to the limited scope and schedule available, not to any shortcoming in the ideas themselves. The team wanted to capture all the thoughts that went into the initial approach and present them as possible topics for further study.

(a) GSE/STE design review process

Successful review of any design stems from careful inspection of the proposed design against the stated performance requirements. This implies that the requirements are well defined, traceable to higher system level requirements, and documented in a configuration management system. At a minimum, a critical design review for GSE/STE should be conducted prior to the construction of the item with stakeholder participation from the integration and test team, as well as System engineers from the project. During the critical design review (CDR), the document and revision status of the equipment's requirements that drive the design should be explicitly stated. The CDR should include explicit definition of the requirements that are not covered or requirements that are not achieved in the design.

Additionally a Failure Mode and Effect analysis should be conducted prior to use of the equipment with high value assets. Lastly there should be a test readiness review including HW and SW quality assurance prior to use with high value assets. Evidence of verification of all requirements must be presented and reviewed at the test readiness review.

(b) Root causes for other discrepancies outside of operator error

Possible causes are poorly defined requirements, inadequate verification that equipment meets defined requirements, lack of a well-integrated plan for all support equipment, lack of configuration control (HW, SW, Firmware, scripts, and procedures), poorly executed failure modes and effects analysis, and failure of limited life items used in the design.

(c) Integration process improvements

Support equipment or STE integration follows the same process as flight equipment. Typically flight or high value equipment requires a verification plan be documented. Often STE is treated much less formally and the integration is left to the designer. Consider whether a separate individual or organization should be responsible for STE verification. The STE integration plan should be a significant part of both the STE preliminary design review and CDR. Test should include traceability to appropriate requirements and the TRR should include evidence that all requirements were verified.

(d) How to make GSE/STE more of a priority (not an afterthought)

Consider elevating an integrated support equipment organization to the same level as systems engineering to plan and to coordinate all levels of test of the flight system. Emphasis should be put on proper allocation of flight system requirements at the most cost-effective level. Reuse of STE designs at multiple levels is highly encouraged. An alternate approach would be the establishment of a Support equipment engineering group within the systems engineering organization. It is critical that appropriate, experienced support equipment systems engineers be involved in proposals and that costing is based on actual final numbers from previous similar programs.

(e) Risk tradeoffs of new design compared to legacy reuse

One of Ariane 5's first and most critical failures was from reuse of an existing design. There is an assumption that reuse of design reduces risk. Although this is somewhat appropriate, reuse brings the burden of reviewing the original equipment requirements against the reuse mission requirements. Although it is tempting to assume that no new verification is required, careful evaluation of the previous verification (including assuring that the previous and current setups and/or use is the same) must be completed before waiving additional verification. Even then the engineer that makes this decision must still realize that the responsibility is his rather than the previous verifier.

(f) GSE and/or STE design driven by tradeoffs of design and/or development risks compared to operational risks

Often the designers of STE are not the users. Therefore their risk list is driven by meeting initial delivery to the documented requirements. A concept of operations should be in place before the start of STE development (ideally even during the proposal stage). End users should participate in the PDR for the equipment and should take an active role in defining operational risks.

(g) WBS structure of programs product based or function based? How does test equipment fit in as a true sub-system?

This item is somewhat related to item (d) above. In addition to giving greater visibility to STE by elevating them in the organization of the project, a separate work breakdown structure helps to capture all the STE costs. This provides for more accurate future proposals. Often time STE fails due to corners cut due to inadequate budget.

(h) Overtest compared to undertest? How a verification and validation program can maximize test coverage while minimizing test-induced risks.

This item is related to item (c) above. Appropriate, cost-effective verification is a result of the good planning of verification in the STE requirement document. The first step is to separate one time design verification testing from tests that must be conducted on every build of the STE or repeated tests required for certification of the equipment at various point in system integration and test. This methodology should be pursued at lower levels of the STE design. By tracing lower level requirements and their verification to the higher system level requirements and verification, risk and cost can be reduced by verifying requirements at a lower level and repeating only an easily executed subset at higher STE build levels. Of course, fewer custom or new designs, as well as appropriate re-use of previously qualified COTS or custom design items, also aids in the effectiveness of the overall test program.

5. Appendix (Checklist)

Step Number	Step Name	Step Description	Data Entry
Safety			
1	Safety Provisions	Has the operator read the safety provisions outlined in the test procedure?	Procedure and Page No. of safety provisions Provide name of person who certifies this knowledge.
2	Emergency Procedure	Has the operator demonstrated understanding of the emergency safing procedure content?	Procedure ID for emergency procedure Provide name of person who certifies this knowledge.
3	Capable and able	Is the operator capable and able to effectively perform the subsequent test sequence as described?	Confirmation by Operator
4	Safety Features	Have protective (automatic and manual) features been validated appropriately and demonstrated prior to first use?	Provide page number for completed step in Test Procedure
Test Preparation			
5	Validation of changes	Have all test equipment changes been validated?	Provide date of validation from TE log book
6	Certifications	Do operators have all required certifications to run test (program-specific certifications)?	Provide list of appropriate operator certifications, and expiration dates.
7	Understanding of Test Configuration	Does the operator understand how the test equipment interacts with the product being tested, including a basic understanding of the test configuration?	Provide name of person who certifies this knowledge, and have them initial the entry certifying the operator has been trained in the system being tested.
8	Understanding Test History	Has operator reviewed recent (e.g., 24-hours, last shift, last time test was run) test events? <i>Example of things to review: event log book, shift handoff, anomaly reports, lessons learned, watch lists?</i>	Provide date of last TE log book entry.
9	Executability	Can the test sequence be reasonably performed before preventative maintenance (or calibration) is required?	Provide date of next scheduled PM or calibration and source (TE log book, QA records)
Alert, Alarm Management			
10	Understanding Alarm Logic	Is operator knowledgeable of audio/visual alert/alarms, indicator logic for this test configuration?	Location in procedure where OOL actions are to be found Operator certifies knowledge of any/all expected OOLs and actions required

11	Alert/Alarm & Anomaly Actions	Has the operator demonstrated knowledge of the appropriate action(s) to take to out-of-limit conditions (or anomalies encountered) in the upcoming test sequence?	Operator certifies knowledge of any/all expected OOLs and actions required by specifying location in procedure where OOL actions are to be found
12	Expected Out-of-limits	Is the operator knowledgeable of expected out-of-limit conditions in upcoming test sequence?	Operator certifies knowledge of expected OOL conditions with approximate procedure step, specification of limit exceedance, etc.
Test Configuration Management			
13	Knowledge of initial/end state	Is the operator aware of the beginning & end state of unit under test and test equipment during test sequence?	Provide write-up of states expected, and TC review with operators for any expected states. Also ensure that test procedures have been dry run and that operators are trained on the use of TE.
14	End-to-end check of test configuration	Have the test configuration items (e.g., STE, SW, HW, databases, cables, aux equipment) been integrated and validated as a system prior to the test sequence?	Provide indication of validation records
15	Verification of change process	Have all changes been reviewed, approved, documented, and communicated to the operator by the responsible engineer?	Confirmation by operator
16	Test Flow workarounds	Have any/all test flow workarounds been communicated to the operator?	Provide/review the planning steps that are directing the workaround(s)
Special Actions			
17	Unsafe commands/actions	Is the operator aware of any/all invalid/unsafe actions/commands that would negatively impact in the current test configuration?	Provide reference to restricted commands/actions list for this configuration and/or certification of operator's knowledge by appropriate individual. TC performs a procedure briefing to identify critical commands for each operator
18	Undefined/Anomalous States	Are there any undefined/anomalous states expected in the upcoming test sequence?	Provide write-up of states expected, and TC review with operators for any expected states.
19	Special test operations	Is operator instructed on what to do for any out-of-sequence or special operations (e.g., who to contact, resources needed)	Provide written changes to test procedure and SME contact information.
20	Transitional conditions	Is operator knowledgeable on expected transitional conditions, alarms, states in the upcoming test sequence (e.g., TVAC plateau changes)?	Provide write-up of expected states, alarms, etc. including approximate procedure step.