Downloaded from http://www.everyspec.com

AEROSPACE REPORT NO.
TOR-2009(8546)-8604, Rev. A

Reuse of Hardware and Software Products

January 27, 2010

Rosalind Lewis[1] and Dana J. Speece[2]

[1]Acquisition and Planning Subdivision, Systems Engineering Division
[2]Product and Process Assurance Department, Mission Assurance Subdivision

Prepared for:

National Reconnaissance Office
14675 Lee Road
Chantilly, VA 20151-1715

Contract No. FA8802-09-C-0001

Authorized by: National Systems Group

Approved for public release; distribution unlimited.

AEROSPACE
Assuring Space Mission Success

Downloaded from http://www.everyspec.com

AEROSPACE REPORT NO.
TOR-2009(8546)-8604, Rev. A

Reuse of Hardware and Software Products

January 27, 2010

Rosalind Lewis[1] and Dana J. Speece[2]

[1]Acquisition and Planning Subdivision, Systems Engineering Division
[2]Product and Process Assurance Department, Mission Assurance Subdivision

Prepared for:

National Reconnaissance Office
14675 Lee Road
Chantilly, VA 20151-1715

Contract No. FA8802-09-C-0001

Authorized by: National Systems Group

Approved for public release; distribution unlimited.

AEROSPACE
Assuring Space Mission Success

Downloaded from http://www.everyspec.com

Reuse of Hardware and Software Products

Approved by:

Jacqueline K. Unitis, Systems Director
Foundational Mission Assurance
Mission Assurance Subdivision
Systems Engineering and Ground Division
National Systems Group

William F. Tosney, General Manager
Corporate Chief Engineering Office
Systems Planning and Engineering

Downloaded from http://www.everyspec.com

Preface

This document has been revised to reflect one small but significant change in content. This revision, Revision A, supersedes any previous versions of TOR-2009(8546)-8604. Distribution remains the same.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Acknowledgement

The authors would like to express their deep appreciation to the National Security Space Mission Assurance Improvement Workshop *Reuse of Heritage HW and SW* working group members for sharing their experiences and insights on this subject. The working group included Ed Schwabecher (LMSSC) as Co-Lead, Dave Pinkley (Ball Aerospace & Technologies), Chahriar Assad and Roger Shaw (Boeing), Norm Brown (MDA), Bill McMullen (NGST), Tyrus Coman (Raytheon), John McBride (General Dynamics), Steven Miller (Orbital Sciences) and Dave Bart, Joe Meltzer and John Brownell (The Aerospace Corporation). This document represents the collative understanding of the team members listed above, and is intended for use by the space industry.

The processes and tools described herein to enhance the assessment of heritage products (subsequently referred to as “reuse products”) represent a mutually agreed upon conceptual approach. This concept is expected to evolve as actual implementation and execution of the processes defined here occur. Recently, additional insight has been gained by the authors during discussion and review with several programs actually attempting to implement this process. This has resulted in clarifications that the authors expect to incorporate in a future revision.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Contents

Downloaded from http://www.everyspec.com

Figures

Tables

Downloaded from http://www.everyspec.com

1. Introduction

1.1 Background

Heritage and legacy designs are supposed to cost less, work better, and be more reliable! But increasingly these assumptions have proven invalid. Use of heritage or legacy elements specifically designed for multiple applications (i.e. commodity products) and reuse of heritage or legacy elements in applications that were not anticipated at the time of the original design have produced unintended consequences ranging from program cost and schedule impact to mission affecting failure. Proposals tout the value of heritage and legacy, but program schedules and budgets expand to accommodate subtle differences in application, design, mission environment, and late arriving failure data (pop-ups). Mission failures are often attributed to erroneous assumptions about the applicability of the requirements, configurations, performance, and reliability of heritage and legacy elements.

This has led to situations where industry and government have been surprised when a previously designed and developed product did not work as intended in a follow-on effort, or in a new application and/or mission. When assumptions and decisions regarding the reuse of products (hardware and software items) are not adequately supported, this can lead to several undesired conditions such as:

- Aggressive assumptions about the cost and schedule benefits of re-use frequently result in short-cuts in test and misplaced confidence, occasionally with disastrous results.
- Lack of close examination regarding the applicability of each requirement of a heritage system specification to a different application leads to requirement/design modifications and associated changes in verification methods.
- Introduction of re-qualification, delta qualification, or pseudo-qualification testing of heritage/legacy designs after contract is viewed as “scope creep”, and the impacts are usually not adequately evaluated.
- Multiple command and telemetry interfaces to accommodate the various heritage elements resulting in complex harnesses, data systems, flight software, and mission operations.
- Choosing a commodity design from a product line of options usually requires a “model step” to an option that can greatly exceed the requirement, but usually at a cost of complexity, size, weight, and power. Inversely, constraining an option can result in a reduction of system performance.
- Commodity products are usually better specified, but they reduce system design flexibility and increase complexity by driving other mission elements to accommodate them. Force fitting multiple commodities or re-used systems usually results in interface adapters, mission operations constraints, or other work-arounds.
- Late arriving “pop-up” reliability information can cause tear-down and repair of many systems that do not demonstrate any anomalous performance, and/or require expensive analysis to support “use-as-is” disposition, which is rarely anticipated in program budgets or schedules.
- Poor configuration control at lower tiers of the supplier chain have frequently resulted in subtle but fatal changes in performance that are not discovered by a reduced set of acceptance tests. Misidentification of Class II changes has caused mission affecting failure.
- Inaccurate assumptions or poor documentation about the behaviors of heritage and legacy designs causing interface problems, performance impacts, and operations errors.

There are benefits to heritage and legacy systems, but realizing those benefits requires rigorous evaluation of the proposed reuse product capability against the new applications requirements. The

Downloaded from http://www.everyspec.com

reuse benefits cannot be achieved by assuming "plug-and-play" or "drop-in solution". Supply chain managers need to oversee the configuration management systems of suppliers. Systems engineers need to take great care in applying heritage or legacy designs. Test engineering needs to test the design and the assumptions. Program managers need to anticipate the impacts of system complexity and late pop-up data. Customers need to understand the challenges faced by system integrators. And users need to accommodate the subtle difference in using follow-on designs.

Leverage of a product reuse decision decreases as each key milestone or program gate passes. Viable fall-back options that exist at the earliest program stages generally become less attractive with time. Familiar scenarios in which cost and schedule dictate a marginal design result from inadequate early-stage delta-design reviews, poor oversight from senior engineering staff cognizant of the heritage application's qualification limits, and inattention to system engineering detail.

1.2 Applicability/Scope

This document defines a reuse review and decision process that can be applied to all programs/projects that plan to reuse products to execute their program/project mission objectives. This process is performed whenever reuse is being considered throughout the program lifecycle; however the benefits are greatest when used in the early program phases. It is important to know as much as possible, as early as practical, about the feasibility, benefits and risks of reusing products. The response to the RFP/proposal is an early opportunity for the customer/government buyer to obtain detailed information about proposed reuse and potential program execution risks. Adequate information must be provided in order to allow an informed acquisition and development decision. An Independent Review Board (IRB[1]) is essential to ensure that the reuse decisions depicted in Fig 1 are not unduly influenced by programmatics, but are based on sound and unbiased technical assessments. This process culminates with a decision to reuse "as is," "with product modifications," "with revised program requirements," or with "reject reuse." Requirements and/or product changes[i] that may occur after the initial evaluation will necessitate revisiting the reuse assessment decision.

A program may sometimes benefit from an approach that uses a heritage product as a platform on which to base an extensive redesign. Heritage products undergoing modifications must be redesigned, fabricated and tested according to the same standards as completely new designs, because modifications within designs tend to interact with existing features in unpredictable ways that can escape high-fidelity analytical methods. Even if the escape rate is small, the totality of such escapes on a program leads to significant risk in the absence of a systematic reuse decision process for products undergoing modifications.

This reuse process can apply from the board/module level (e.g. a single board computer / software CSU), to an assembly level, (e.g. electronics box, mechanism. software CSC) and potentially to a subsystem level (power distribution, command and data handling, software CSCI), government furnished equipment or customer furnished equipment and even non-operational units[ii].

System functions and requirements must still be proven, even if the capability is provided by a reuse product. Neither this decision process, nor the application of a reuse product, obviates or reduces the need for a verification and validation (V&V) process[iii]. The approach to V&V may leverage the analysis and rationale collected as a part of this decision process. However, it is not the intent of this guidance to suggest how V&V of reused products (or systems that employ them) should be accomplished.

---

[1] Contractors may have existing boards, such as a Qualification Review Board (QRB) that would have responsibility for the review board functions discussed in this document.

Downloaded from http://www.everyspec.com

1.3 Document Content

Reuse Decision Process

The reuse decision process is used to assess a potential reuse product's capability to meet a target program requirements. A process flowchart outlines the decision steps involved in the reuse product usability assessment, which is supported with text that describes each decision point in detail. Additional information on each decision point is also captured in a table that includes the entry and exit conditions, potential assessment risks, and a listing of the expertise required to support each decision point.

Reuse Evaluation Considerations

This document includes a listing of evaluation considerations, in checklist format, that are gleaned from industry best practices and lessons learned but are not all encompassing. They serve as guidelines for consistent application of the reuse process and the identification of sources of risk. They are to be used as examples and do not relieve an evaluator from technical due diligence to determine reusability.

Hardware and software considerations are provided in Appendices A and B respectively. They are applicable to the tasks of determining the suitability of a product for reuse and of identifying categories of potential risk that may emerge as a reuse plan develops. Multiple sections of this report leverage the considerations for decision support, reuse planning, and risk evaluation with the objective of ensuring that reuse risks are identified and managed.

Reuse Decision Process Implementation Example

Appendix C describes how the reuse decision process could be implemented by a contractor's organization. The example contains detailed information regarding the roles and responsibilities of the different participants involved in the reuse decision assessment.

Endpoints

The Endpoints section is a collection of real industry examples of products that were reused without the benefit of a sufficiently thorough assessment process.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

2. Reuse Decision Process Flow

The reuse decision process is used to determine what is known (or can be known) about the potential reuse product, assess whether the potential reuse product is compatible with the target program's requirements, and evaluate the risk/impact of proceeding with a potential reuse product that is not compatible (as-is) with the target program requirements.

The process describes six major decision gates[2] for assuring mission compatibility when reusing products. These decisions gates incrementally build upon each other and are structured to systematically explore the risks associated with making a product reuse decision. A key part of exploring the risk is the treatment of a series of considerations found in Appendices A and B of this document. These considerations represent a collective set of lessons learned or best practices associated with product reuse. All of the considerations are important and may be applicable at different times throughout the decision process. It is incumbent upon those involved in the decision process to ascertain that each of the considerations are adequately addressed when appropriate, or that an explanation for not addressing a consideration is provided.

Each decision gate has entry/exit criteria, risks (an undesirable condition or consequence of a decision), and a recognized set of participants. Depending on the decision gate, the participants will include the Independent Review Board, Program Management, speciality engineering, etc. The exit criteria include identifying the risks associated with that decision and should be captured in the reuse plan for subsequent handling and management by the program. A brief overview of each decision gate with the suggested decision participants is found in Table 1 with a more detailed explanation of the decision in the text following Figure 1.

All options for product reuse will require the development of a reuse plan. The reuse plan defines the criteria and supporting artifacts that captures the rationale and assumptions for the reuse decisions made with respect to Figure 1. Once the plan is established it must be revisited throughout the program to ensure that program changes or reuse product differences do not invalidate the original decision. Each decision gate has a minimal set of criteria, which must be considered as described in the matrix and text below. The reuse plan also serves as a construct to identify and track risks associated with the reuse decision.

[2] The six gates are designed primarily to focus on a hardware reuse product decision. For software there are primarily three primary gates: Compatible, Program Baseline Change and Product Modification.

Downloaded from http://www.everyspec.com

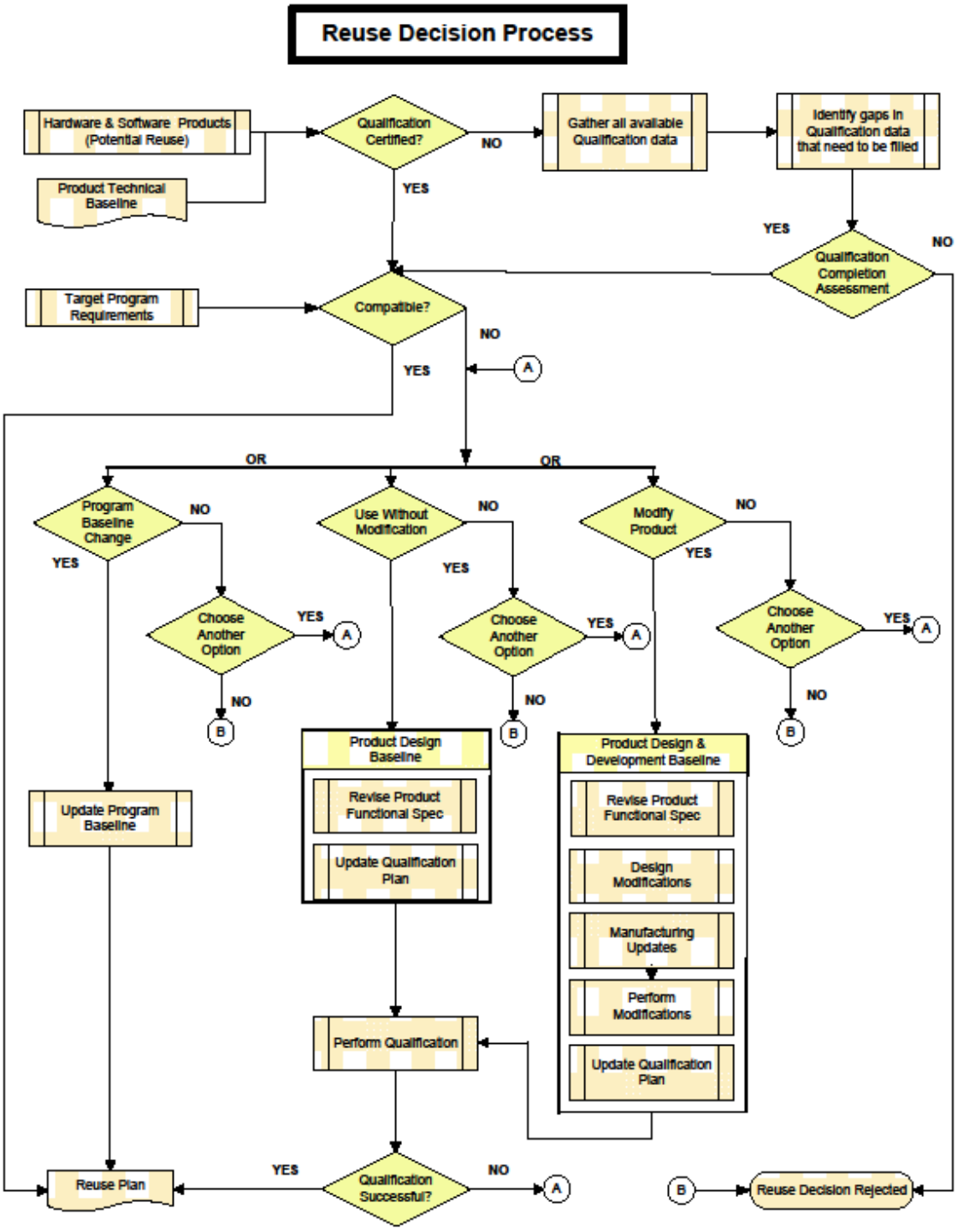

Figure 1. Reuse decision process flow.

Downloaded from http://www.everyspec.com

2.1 Qualification Certified

Qualification certified is a ***status decision point***, designed to determine if sufficient information is known about the potential reuse product. This decision point relies on and requires the following entry conditions:

- the qualification data, which is a collection of technical and performance information that describes and documents demonstrated capability and behavior of the reuse product. This information is noted as H/W & S/W Products (Potential Reuse) in Figure 1.
- the *state* of the qualification data which is either certified (complete, valid, etc) or not. Certified qualification data will enable direct transition to the Compatibility decision, while lack of certification, requires additional effort to understand the cost/benefit of achieving certification.

The major risk for this decision point is the extent to which the generation, collection and maintenance of the qualification information, represents a true and accurate accounting of the product's design[iv], composition[v], configuration[vi], and performance (poor data integrity). Rigorous QA and CM can help reduce the amount of inaccuracy. Therefore attention should be given to understanding the information flow and data handling processes. Additionally, Technology Readiness Levels (TRL) are used as indicators of product maturity. Products with a higher TRL are likely to have more thorough historical data. However TRL alone is not sufficient to justify reuse, but may be considered in the overall reuse decision.

Completion of this decision point should be accompanied by documenting the rationale for the decision, along with the qualification data risk assessment observations/findings as described above. In either case (a yes or no decision), this information must be retained for inclusion in the reuse plan, if the product is ultimately selected for reuse.

2.2 Qualification Completion Assessment

Qualification Completion Assessment is a ***resource decision point***, designed to determine if the effort, both in time and dollars, required to complete the qualification of the potential reuse product is beneficial to the program. This decision point relies on and requires the following entry conditions:

- a predefined set of certification requirements and method for evaluation
- a collection of qualification related data which may include
  - existing but not certified formal qualification data
  - data about the product that may reside in informal sources such as program, team and/or individual databases, files and notes.
- a comparison of the collected data versus the certification requirements. This comparison, the gap analysis, articulates what additional information must be acquired and includes the corresponding cost and schedule to do so.

The major risks for this decision point are (1) poor data integrity (as described above for the Qualification Certified Decision); (2) lowered expectations for certification; and (3) cost/schedule estimates that are not credible. If the requirements for certification exceed the available or "found" data, caution should be exercised to avoid disregarding certification requirements that have not been addressed. This situation can be mitigated somewhat by defining the certification requirements well in advance of the data collection activity. Poor credibility of the cost/schedule necessary to complete

Downloaded from http://www.everyspec.com

certification can be reduced by comparison of the estimates to actual cost/schedule for similar activities.

Completion of this decision point should be accompanied by the documented cost/benefit decision, along with the risk assessment observations/findings as described above. When the Cost/Schedule Acceptable decision is "yes" (leads to the compatible decision point), this information should be retained for inclusion in the reuse plan, if applicable.

2.3 Compatible

Compatible is a ***planning decision point***, designed to determine if a potential reuse product is the correct choice for providing a capability required by the target program. This decision point relies on and requires the following entry conditions:

- certified qualification data[3]
- the *program (target) baseline* which is a collection of technical and performance information that describes and documents required capability and behavior of the target program to include safety, reliability, part quality, materials and processes, etc.
- operations and maintenance data

The considerations (Appendices A and B) for hardware and software are the basis of the gap analysis; a comparison of potential reuse product performance against target program requirements. The assessment of these considerations supports the decision to proceed along one of the following paths:

- Yes …Use-As-Is
- No …but consider alternative option
  - Program Baseline Change
  - Use W/O Modification
  - Product Modification
- No Reuse-not-possible

The major risks for this decision point are (1) poor data integrity (as described above for the Qualification Certified Decision) including operational/maintenance data; (2) inadequate treatment of the compatibility considerations[vii]; and (3) a poorly formed or immature program target baseline[viii].

When the applicable considerations are not or cannot be sufficiently evaluated, this increases the possibility of making a poorly informed decision by overlooking or discounting information not available. Similarly, a not-well-defined target baseline may also adversely impact the evaluation of the considerations, additionally adversely impacting the decision quality.

Completion of this decision point should document the decision rationale to include a relative ranking of the possible next paths based on technical risk. The technical risk, as well as, any capability/performance shortfalls should be exposed (and captured in the reuse plan) during evaluation of the considerations. The decision risks described above should also be independently (of the target program) assessed and captured as part of the reuse plan. When the Compatible decision is "yes", this means that the reuse product can be used without further assessment or modification and the supporting artifacts accompanying this conclusion should be captured in the reuse plan.

---

[3] For software a collection of design, architecture and test artifacts, and the product itself compose the necessary historical information. These are explicitly called out as considerations in Appendix 2.

Downloaded from http://www.everyspec.com

2.4 Program Baseline Change

This is a ***feasibility assessment decision point***, designed to determine if the target program requirements can be descoped (changed) to match the capability and performance of the potential reuse product. This decision point relies on and requires the following entry conditions:

- technical risk assessment from the Compatibility decision point that supports the baseline change
- traceability of the descoped target program requirements to other parts of the system as well as the concept of operations

The major risk for this decision point is that unintended consequences to the system behavior or operational utility could result from the descope decision. To minimize this possibility, effort should be undertaken to (1) articulate the impact of changes on total system (and interface) performance; and (2) assess the effect of these changes on mission performance and/or operations. Traceability of the impacted target program requirements will support this analysis.

Completion of this decision point should document the decision rationale along with the decision risk assessment observations/findings as described above. If a program baseline change is not possible, then this decision point should also reconsider the remaining options (ranked during the compatibility decision point) and provide any objective update to those ranking. The decisions and findings, along with supporting artifacts should be captured in the reuse plan.

2.5 Use Without Modification

This is a ***feasibility assessment decision point***, designed to determine if the reuse product can be qualified to the target program requirements.[ix] This decision point relies on and requires the following entry conditions:

- technical risk assessment from the Compatibility decision point that supports the use without modification option
- identification of capability/performance gap that will be assessed in the qualification (identified as a shortfall from the Compatibility decision point)

The major risk for this decision point is that the product may fail qualification. Minimizing this risk begins with selecting products that have a reasonable likelihood of achieving qualification. However a recovery plan that describes the alternate course of action (technology, cost, and schedule) if qualification fails, should be prepared. This recovery plan, if exercised, will consume resources in addition to the qualification effort, and therefore must be adequately programmed.

Completion of this decision point should document the decision rationale along with the decision risk assessment observations/findings as described above. The decisions and findings, along with supporting artifacts should be captured in the reuse plan.

2.6 Product Design Baseline

This set of activities is used to prepare for qualification that will determine if the reuse product can satisfy the target program requirements. The activities include the following:

Downloaded from http://www.everyspec.com

1. Revise Product Functional Spec – Update the reuse product specification to match the requirements of the target program
2. Update Qualification Plan -
   a. Revise the qualification plan, which defines the test, analyses, inspection, and demonstration necessary to verify the target program requirements
   b. Present data (including analysis and test results) which demonstrate that the qualification approach (full, delta, incremental, etc.) will result in meeting the target program requirements
   c. IRB assessment and approval of the revised qualification plan

2.7 Modify Product

Product modification is a ***feasibility assessment decision point***, designed to determine if the reuse product can be changed to satisfy the target program requirements.

This decision point relies on and requires the following entry conditions:

- technical risk assessment from the Compatibility decision point that supports the modification option
- identification of capability/performance gap that will be assessed in the qualification (identified as a shortfall from the Compatibility decision point)

The major risk for this decision point is that the product modification and/or qualification may fail. Minimizing this risk begins with selecting products that have a reasonable likelihood of being successfully modified and subsequently achieving qualification. However a recovery plan that describes the alternate course of action (technology, cost, and schedule) if modification and/or qualification fails, should be prepared. This recovery plan, if exercised, will consume resources in addition to the modification/qualification effort, and therefore must be adequately programmed.

An additional risk is that the modification may cause unintended consequences to the system behavior or operational utility due to new and unforeseen product/component interactions. To minimize this possibility, effort should be undertaken to (1) articulate the impact of modification on total system (and interface) performance; and (2) assess the effect of these changes on mission performance and/or operations. Traceability of the target program requirements affected by the modification will support this analysis.

Completion of this decision point should document the decision rationale along with the decision risk assessment observations/findings as described above. The decisions and findings, along with supporting artifacts should be captured in the reuse plan.

2.8 Product Design & Development Baseline

This set of activities is used to prepare for qualification that will determine if the reuse product, as modified, can satisfy the target program requirements. The activities include the following:

1. Revise Product Functional Spec – Update the reuse product specification to match the requirements of the target program
2. Design Modification – Determine the architectural changes necessary to meet the target program requirements
3. Manufacturing Updates – Revise the manufacturing planning (parts, materials, processes, equipment, etc) to execute the design changes

Downloaded from http://www.everyspec.com

4. Perform Modifications – Implement the design changes
5. Update Qualification Plan
   a. Revise the qualification plan, which defines the test, analyses, inspection, and demonstration necessary to verify the target program requirements
   b. Programs should present data (including analysis and test results) which demonstrate that the qualification approach (full, delta, incremental, etc) will successfully expose any unforeseen interactions that result from modifying the reuse product
   c. IRB assessment and approval of the revised qualification plan

2.9 Qualification Successful

This is an IRB ***decision point***, which determines if the qualification process has succeeded in extending the qualification envelope or modifying the product to satisfy the target requirements. This decision point relies on and requires the following entry condition:

- results of the qualification test and analyses.

1. If the IRB determines that the qualification was successful,
   a. The assessment conclusions along with any associated risk observations/findings should be captured in the reuse plan
   b. Qualification information may be used to revise the existing verification plan (see TOR 2004 (3901) 3242)
2. If the IRB determines that the qualification was unsuccessful
   a. Another option for pursuing the reuse product must be selected, or
   b. Reuse product not viable, other alternatives that do not rely on the reuse product must be considered

Downloaded from http://www.everyspec.com

Table 1. Reuse Decision Gates Summary

	Entry and Exit Conditions	**Risk Assessment**	**Decision Participants**
Qualification Certified	Entry: Qualification data and state Exit: Rationale for the decision and risk assessment	1) Poor data integrity => mitigate by use of strong QA, MA and CM processes	IRB or equivalent[4] to include at least the following: System Engr Design Engr Manfacturing, PM&P Mission Assurance
Qualification Completion Assessment	Entry: Certification Requirements, Qualification data, Gap Analysis Exit: Rationale for the decision and risk assessment findings	1) Poor data integrity 2) Lowered certification requirements => mitigate by a prior certification requirement and method 3) Low credibility of cost/schedule estimates	Program Mgmt System Engr
Compatible	Entry: certified qualification data, program (target) baseline Exit: Rationale for the decision, relative ranking of the possible next paths, capability and performance shortfall, and decision risk assessment findings	1) Poor data integrity 2) Inadequate treatment of considerations 3) Target Program Baseline Immaturity	IRB or equivalent to include at least the following:System Engr Design Engr Software Engr, etc.
Program Baseline Change	Entry: technical risk assessment, and traceability of the descoped target program requirements Exit: Rationale for the decision, and decision risk assessment findings	1) Unintended consequences to the system behavior or operational utility	Customer Program Mgmt System Engr Mission Assurance
Use W/O Modification	Entry: technical risk assessment, and capability/ performance shortfall Exit: Rationale for the decision, and decision risk assessment findings	1) Product may fail qualification	IRB or equivalent to include at least the following: PM&P Test Engr
Modify Product	Entry: technical risk assessment, capability/ performance shortfall, traceability of the target program requirements affected by the modification Exit: Rationale for the decision, and decision risk assessment findings	1) Product modification and/or qualification may fail 2) Modification may cause unintended consequences to the system behavior or operational utility 3)	IRB or equivalent to include at least the following: Program Mgmt SE, MA Design Engr Manufacturing, PM&P Mission Assurance (MA)

[4] An equivalent construct for the IRB in some organizations may be a Qualification Review Board (QRB).

Downloaded from http://www.everyspec.com

3. Definitions

Component-Based Software Engineering – The concept of designing and building a system from smaller, existing, proven stand-alone software elements, including COTS, GOTS, and artifact reuse.

COTS Hardware: COTS (Commercial-Off-The-Shelf) products are designed for broad based commercial usage and tailoring of performance requirements or the product by the procurer is not allowed.

COTS Software : COTS (Commercial-Off-The-Shelf) software artifacts are those that are procured commercially, usually as libraries and applications. They are often maintained by the vendor and the procurer has limited control over the final product.

Heritage Hardware: Hardware products (i.e. complex part, unit, assembly, subsystem or system) that has previously undergone qualification and utilization.

Legacy Software: Software previously utilized on a predecessor system.

Qualification: Test, analyses, inspection, demonstration conducted to demonstrate satisfaction of design requirements including margin and product robustness for designs that have no demonstrated history. A full qualification validates the planned acceptance program, in-process stress screens, and retest environmental stresses resulting from failure and rework.

Qualification Certified: A decision based on the completeness and applicability of the qualification data associated with hardware being considered for reuse.

Qualification by Similarity: An approach to apply the qualification history (test, analysis, inspection, demonstration) of a previously used hardware item to meet the qualification requirements for reusing that hardware on a different system or mission.

Reuse: The utilization of a previously developed product. Typically the intent of reuse is to avoid duplication of development, tooling or qualification test (i.e. costs and schedule) by the application of existing hardware or software products that have been previously used.

Review: A review is a forum and a process to provide assurance that the most satisfactory approach, plan, or design has been selected, that a configuration item has been produced to meet the specified requirements, or that a configuration item is ready. Reviews communicate an approach, demonstrate an ability to meet requirements, or establish status.

Service Life: The service life of an item starts at the completion of fabrication and continues through all acceptance testing, handling, storage, transportation, prelaunch testing, all phases of launch, orbital operations, disposal, reentry or recovery from orbit, refurbishment, retesting, and reuse that may be required or specified.

Use-As-Is: A determination based on review of all qualification data and analyses, new system performance requirements and environments, usage history, manufacturing capability, and other relevant information that the product being considered for reuse is acceptable without any additional test, analysis or modifications.

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

4. Acronym List

BIT – Built in Test
BITE – Built in Test Equipment
CPU – Central Processing Unit
CCB – Change Control Board
CM – Configuration Management
COTS – Commercial-Off-The-Shelf
CVM – Condensable Volatile Material
CRD – Critical Design Review
ESD – Electrostatic Discharge
E3 – Electromagnetic Environmental Effects
ECR – Engineering Change Request
ELDRS – Enhanced Low Dose Rate Sensitivity
EQM – Engineering Qualification Model
EMI/EMC – Electromagnetic Interference/Electromagnetic Compatibility
FMECA – Failure Modes, Effects and Criticality Analysis
FTA – Fault Tree Analysis
FFA – Functional Failure Analysis
FQT – Functional Qualification Testing
GEO – Geosynchronous
GIDEP – Government-Industry Data Exchange Program
GSE – Ground Support Equipment
H/W – Hardware
IPT – Integrated Product Team
ICD – Interface-Control Drawing
IRB – Independent Review Board
I/O – Input/Output
LEO – Low Earth Orbit
LRU – Line Replaceable Unit
MA – Mission Assurance
MIUL – Materials Identification and Usage List
MTBF – Mean-Time Before Failure
MTTR – Mean-Time-to-Repair
MMOD – Micrometeoroid Orbital Debris

Downloaded from http://www.everyspec.com

PSA – Parts Stress Analysis
PDR – Preliminary Design Review
PA – Product Assurance
PM – Protoflight Model
QA – Quality Assurance
QRB – Qualification Review Board
RF – Radio Frequency
RRB – Reuse Review Board
SEE – Single Event Effect
SEU – Single Event Upset
SEL – Single Event Latch-up
SPF – Single Point Failure
STE – Special Test Equipment
SSPA – Solid State Power Amplifier
SRR – System Requirements Review
TRL – Technology Readiness Levels
TID – Total Ionizing Dose
TML – Total Mass Loss
TWTA – Traveling Wave Tube Amplifier
TTI – Time to Irreversibility
TTCE – Time to Critical Effect
WCA – Worst-Case Analysis

Downloaded from http://www.everyspec.com

5. References

1. Incorporating Reusable Software Products, MIL-STD-498, Appendix B, 5 December 1994
2. IEEE Standard for Information Technology – Software Life Cycle Processes – Reuse Processes, 25 March 2004
3. NASA Software Safety Guidebook, NASA-GB-8710.13, 31 March 2004
4. Software Acquisition Gold Practice™ – Assess Reuse Risks and Costs, www.goldpractices.com/practices/arrc/index.php
5. Test Requirements for Launch, Upper-Stage, and Space Vehicles, Vol II: Applications Guidelines, MIL-HDBK-340, 01 April 1999
6. Space System Verification Program and Management Process, Aerospace TOR-2006(8506)-4732, 30 June 2006

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

6. Endnotes

i. Several programs developed designs based on a commodity reaction wheel assembly (RWA) with significant flight heritage. After procurement had begun, flight anomalies were noted, ultimately resulting in the total loss of one mission. Due to program schedule and budget pressures, the programs continued with the baseline design, but monitored the developments of the heritage hardware. As failures and anomalous performance were noted in other programs, a root cause was tentatively identified related to the configuration since all of the failed units were mounted in configurations that corresponded to the theory. Follow on programs responded to this information accordingly. Two years later another failure theory emerged, blaming the failures primarily on the installation processes and hardware design. Further investigation revealed that the programs using these RWAs (now very close to launch) were built slightly differently than the failed units and that there were other very significant differences in the evolution of the heritage designs.

ii. Program F had been developing an evolving family of mission solutions for a government customer going back decades. In each successive generation some hardware is redesigned to improve performance, address new requirements, and leverage new technologies while other hardware is "built to print". An engineering model is built for each generation to be used to validate the design and troubleshoot problems discovered in the flight hardware. The EM, like the flight hardware, is a mix of new and heritage hardware and legacy software. In one case a proposed design change was evaluated on the EM and judged to be beneficial to the mission. However when the flight hardware was built the expected performance improvement was actually a degradation of key parametric performance. Investigation revealed that the EM was built with "representative" hardware, not flight identical hardware. This difference was judged to be insignificant by the original designer over 10 years earlier, however the engineer that inherited the EM did not know about the difference. Since the design evaluation was based on qualitative functional data it did not reveal the quantitative degradation in performance. Significant and expensive rework mitigated some of the problem, but the customer ultimately accepted the system with some residual degradation.

iii. On September 8, 2004 the Genesis sample return capsule drogue parachute did not deploy during entry, descent, and landing operations over the Utah Test and Training Range. The drogue parachute was intended to slow the capsule and provide stability during transonic flight. After the point of expected drogue deployment, the sample return capsule began to tumble and impacted the Test Range. Genesis Management and Systems Engineering and the Genesis Red Team made a number of errors because of their belief that the G-switch sensor circuitry was a heritage design. Further, the prevalent view that heritage designs required less scrutiny and were inherently more reliable than new designs led to the mishap. It is likely that the design error would not have occurred or would have been discovered during verification had the same standards as those applied to new hardware been applied to the heritage product.

iv. Program XYZ proposed re-use of heritage interface electronics boards for a very similar application. The design was judged to be "plug and play" based on the component specification, and the program was planned and baselined with short development times and few engineering hours. However it was discovered that the inherited designs were full of red-line changes that made the designs unusable by the inheriting program. The redesign resulted in severe cost and schedule impacts to the program.

v. Four parallel programs purchased communication transmitters from a vendor with a long history of reliable performance. One of the programs noted a subtle change in performance in Space Vehicle level TVAC. Disassembly of the transmitter revealed a cracked semi-rigid cable, but the Failure Analysis Lab also noted the presence of pure tin coated feedthrough capacitors. Upon investigation

Downloaded from http://www.everyspec.com

it was discovered that a 3rd tier supplier had replaced tin-lead coated parts with pure tin coated parts, and delivered over 3000 parts to the 2nd tier vendor. All 4 parallel programs were de-integrated and reworked to conformal coat the pure tin coated parts, and to evaluate the cracking semi-rigid cables. In several cases the rework caused other problems that resulted in further delays.

vi. IFT-10 failed when the Missile Defense exoatmospheric kill vehicle (EKV) did not separate from its booster rocket. The problem was created when a pin broke that should have activated a laser to release the boost vehicle's restraining units, causing the boost vehicle to remain with the EKV. The pin came apart from excessive vibrations related to the removal of a piece of insulating foam by the subcontractor to make monitoring the system easier. The change was characterized as Class II by the subcontractor, and was not reviewed by the prime contractor or customer.

vii. Program X proposed a Computing and Data Handling (C&DH) solution that was based on a previous mission. Because of the heritage assumption the program was proposed with a fraction of the engineering hours of the predecessor program. However because of functional and interface differences the Program X team actually spent more hours than the predecessor program, overrunning the program. The overruns were not incurred until late in the program causing delayed delivery of the subsystem, required numerous modifications to interfacing hardware, dramatic re-design of the legacy software, and ultimately reduced performance.

viii. Several spacecraft used legacy flight software (FSW) derived from a baseline mission. After a second generation program adopted the baseline FSW, the original program discovered that a fault protection routine identified "dead tasks" but did not execute any mitigation or recovery steps (i.e. reboot or safemode). A fix was developed and implemented for the first generation mission, but two second generation missions were not notified. Another second generation mission adopted the FSW from the first generation after the fix had been incorporated. Third generation missions that adopted the FSW from the later second generation mission (with the fix) were similarly protected. Third generation programs that adopted FSW from the missions without the fix were informally notified of the fix on the first generation mission, and incorporated their own versions of the fix. Ultimately 2 of 7 missions were deployed without the necessary fix, resulting in one "near miss" that almost ended the mission.

ix. In some instances, requirements on the new application may deviate from the heritage qualification only incrementally (typically—and only in the case of hardware—due to the launch or orbital environments). A TWTA may not have been qualified to operate through critical pressure; ELDRS analyses may not exist for certain electronic components; the spacecraft acoustic environment may have increased, over a range of frequencies, beyond the qualification test environment of the heritage program(s); an antenna may experience temperatures below those enveloped by its qualification limit. Each of these issues could be addressed by analysis (e.g., in the ELDRS case) and/or tests without the need to modify a design given that the required margin is inherent to the existing product.

Downloaded from http://www.everyspec.com

Appendix A. Hardware Considerations

General Description

These considerations are intended to help determine whether existing hardware (H/W) products are correctly matched to project requirements in support of subsystem and component design reuse. The considerations are intended for use throughout the project life cycle and at each product life cycle gate to ensure that the design is ready to proceed to the next phase. The level of detail (system, subsystem, or component level) for completion of these considerations, are determined by the phase, complexity and other factors.

Table 2. is a potential tool to status the reuse consideration evaluation for hardware products.

- Disposition Status (example entries)
  - N/A
  - Yes - Fully Compliant
  - No - Non-Compliant
  - Under Evaluation
- Comments/Rationale/Resolution/Future Action
  - Document the design rationale with the appropriate justification.
  - Add future action plans.
- Verification Approach/Objective Evidence
- Top-level verification approach and objective evidence.
- Verification Status

Table 2. Hardware Considerations

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
DEVELOPMENT/PROJECT MANAGEMENT & STANDARDS					
1	Have all differences in the standards followed in the development of the reusable component been evaluated?				
2	Has a change management process for the component being reused been defined?				
3	Do all original design data and analyses exist?				
4	Are the engineering tools used to develop the reuse component still available?				
5	Have all design notes, revision notes, and other component history documentation been reviewed?				
6	Is there a current problem report list detailing existing latent bugs and has it been reviewed?				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
7	Is an original development team member included in the Integrated Product Team (IPT) or available to provide support to the IPT?				
8	Is any specialized training/education needed to implement the reuse of the component?				
9	Has an evaluation of sparing been done?				
10	Has an evaluation of the reuse component's life cycle cost been done?				
11	Has an evaluation of schedule impact and long lead activities been done?				
12	Has an evaluation of changes in certification/accreditation been done?				
REQUIREMENTS-GENERAL					
13	Do requirements documents exist and have they been evaluated?				
REQUIREMENTS-FUNCTIONAL/PERFORMANCE					
14	Has the impact against false alarm rate/spurious signal mitigation requirements been evaluated?				
15	Has the applicability against measure and command/telemetry list requirements been evaluated?				
16	Have all changes to Built in Test (BIT)/Built in Test Equipment (BITE) and other diagnostics been evaluated?				
17	Has consistency with latency and other TTI/TTCE timelines been evaluated?				
REQUIREMENTS-ENVIRONMENTAL/THREATS					
18	Have all differences in lightning requirements for susceptibility (launch site, vehicle, or probabilities used in the prior analysis) been evaluated?				
19	Has an evaluation of the impact of any changes needed due to natural environments (e.g., radiation, MMOD) been done?				
20	Has an evaluation of the impact of any changes needed due to human-induced environments/threats been done?				
REQUIREMENTS-RELIABILITY/MAINTAINABILITY					
21	Have all changes to applicable reliability requirement metric (e.g., Mean-Time Before Failure (MTBF), inherent availability, failure/fault tolerance level.) been evaluated?				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
22	Have all changes to applicable maintainability requirement metric (e.g., Mean-Time-to-Repair (MTTR), failure/fault diagnostic coverage) been evaluated?				
23	Have all changes to life (e.g., duration, duty cycle, life limiting parameters) been evaluated?				
DESIGN/ARCHITECTURE-GENERAL					
24	Has the architecture been evaluated for interface compatibility and sizing of data systems (e.g., through-put, storage) versus software (S/W) requirements?				
25	Have all functional differences between the reusable component and the requirements been evaluated?				
26	Have all differences in algorithm, data flow structures, interface structures, or data formats been evaluated?				
27	Can the component being reused be acceptably modified?				
28	Is the reuse component design mature (i.e. TRL) and flight proven?				
29	Have all changes in margin-related parameters (e.g., derating, operating temperature/stressing conditions) been evaluated?				
30	Has the component failure/defect history been reviewed?				
31	Are all possible failure modes/effects still bounded by previous Failure Modes and Effects Criticality Analysis (FMECA)/Functional Failure Analysis (FFA)?				
32	Have all changes related to common cause failure potential (e.g., spatial proximity, like type versus dissimilar redundancy) been evaluated?				
33	Have all changes that affect human operator interface been evaluated?				
34	Have all changes that affect maintenance approach (e.g., LRU, repair) been evaluated?				
35	Has the user interface been evaluated for applicability?				
36	Has the component been evaluated for any personnel access/line of sight issues?				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
37	Has the component been evaluated for any issues interfacing tools and equipment?				
38	Has an evaluation of radiated/conducted emissions and susceptibility, including any change of standards as applicable, been done?				
39	Has an evaluation of operational Electrostatic Discharge (ESD) (spacecraft charging or triboelectric effects) susceptibility, including any change of standards as applicable, been done?				
40	Has an evaluation of the adequacy of grounding, bonding, and shielding for intended use been done?				
41	Has an evaluation of the effect of parts substitutions that might affect unit Electromagnetic Environmental Effects (E3) performance or signal integrity attributes been done?				
42	Has an evaluation of the impact of any changes needed due to changes to external interfaces (e.g., protective features, shielding, vulnerable pathways) been done?				
43	Has an evaluation of security policies for compliance to any potentially new policies and standards that now apply been done?				
44	Has an evaluation of any changes in vulnerability been done?				
45	Has an evaluation of any changes in countermeasure strategy been done?				
46	Has an evaluation of the reuse components packing criteria been done?				
47	Has an evaluation of the reuse components handling criteria been done?				
48	Has an evaluation of the reuse components storage criteria been done?				
49	Has an evaluation of the reuse components transportation criteria been done?				
DESIGN/ARCHITECTURE- PARTS AND MATERIALS					
50	Has an evaluation of the reuse component piece parts been done with respect to obsolescence and have acceptable alternative parts been identified?				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
51	Has an evaluation of the effect of parts substitutions that might affect unit survivability performance attributes been done?				
52	Has an evaluation of the piece part components with respect to changes in environmental stresses (e.g., thermal, electrical) been done?				
53	Has an evaluation of the piece part components with respect to changes in margin (e.g., derating) been done?				
54	Has an evaluation of the piece part components with respect to changes in duration, duty cycle, and life limiting parameters been done?				
55	Has an evaluation of the piece part components with respect to failure history/supplier defects been done?				
56	Has an evaluation of the piece part components with respect to quality factors associated with production line, change of vendors, or change of personnel been done?				
57	Has an evaluation of the impact of any material changes been done?				
58	Has an evaluation on whether specified materials are appropriate for intended use been done?				
MANUFACTURING					
59	Has an evaluation of the impact of any process changes been done?				
60	Has an evaluation on whether the process is appropriate for the intended use been done?				
TEST					
61	Do all test documents exist and have they been evaluated?				
62	Is the reuse component Special Test Equipment (STE) still available?				
63	Have all external interfaces related to Ground Support Equipment (GSE), STE, or fixturing been evaluated?				
64	Have all changes related to infant mortality screens/burn-in/run-in been evaluated?				
65	Have all changes related to lot sampling/other reliability statistical quality factors been evaluated?				

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Appendix B. Software Evaluation Considerations

General Description

These considerations are intended to help determine whether existing software (S/W) products are correctly matched to project requirements in support of subsystem and component design reuse. The considerations are intended for use throughout the project life cycle and at each product life cycle gate to ensure that the design is ready to proceed to the next phase. The level of detail (system, subsystem, or component level) for completion of these considerations, are determined by the phase, complexity and other factors.

Consideration Instructions

Table 3. is a potential tool to status the reuse consideration evaluation for software products.

- Disposition Status (example entries)
  - N/A
  - Yes - Fully Compliant
  - No - Non-Compliant
  - Under Evaluation
  - Comments/Rationale/Resolution/Future Action
  - Document the design rationale with the appropriate justification.
  - Add future action plans.
- Verification Approach/Objective Evidence
  - Top-level verification approach and objective evidence.
- Verification Status

Table 3. Software Considerations

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
LEGAL & SOURCE CODE					
1	Have all legal and/or licensing issues for use (and modification) been reviewed and resolved?				
2	Has the source code for the reusable component been made available for analysis and retention?				
ENVIRONMENT					
3	Have any differences between the original and reuse target environment been identified and evaluated, (e.g., hardware (H/W); Central Processing Unit (CPU); operating system, etc).?				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
4	Have any differences between the original and target operating environment been identified and evaluated? (e.g., interoperability with other systems and system-external elements; service layers; Application Program Interfaces (APIs); etc.)				
STANDARDS & PROCESSES					
5	Have any relevant differences between standards applicable to the original and reused environments been identified and evaluated?				
6	Have any differences in development processes between the original process and current reuse processes been identified and evaluated?				
REQUIREMENTS					
7	Do requirements documents exist for both the software component under reuse (i.e., “original role”) and its proposed new reuse role?				
8	Are the requirements for the proposed reuse software the same as the requirements for the original development? If not, have the differences been identified and evaluated?				
9	Have all relevant requirement differences regarding performance envelope, dimensions, timing aspects, interlocks, etc. explicitly been identified and evaluated for needed additional review and change?				
10	Have any differences in safety, security, and privacy protection requirements been identified and evaluated?				
FUNCTIONAL DIFFERENCES					
11	Have any functional differences between the reusable component (from #2) and the present requirements been evaluated, i.e., the reuse S/W provides the required capabilities and meets the required constraints?				
ARCHITECTURE					
12	Do architectural exist for both the s/w component under reuse and its proposed new reuse role, ?				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
13	Have all relevant architectural differences (between original and reuse) explicitly been identified and evaluated for needed additional review and change?				
DESIGN					
14	Do design documents exist for both the s/w component under reuse and its proposed new reuse role				
15	Have all relevant design differences regarding performance envelope, dimensions, timing aspects, interlocks, etc. between original and reuse been identified and evaluated?				
16	Have all relevant differences in algorithms, data structures, or data formats between the original and reuse been identified and evaluated?				
17	Have any differences in performance envelope, dimensions, timing aspects, interlocks, etc. between the original and reuse been identified and evaluated?				
TEST					
19	Have all relevant test differences between original and reuse been explicitly identified and evaluated?				
20	Has an automated test suite for the reusable component been evaluated?				
21	Are original test procedures, data and results available for regression test comparisons?				
22	Does a current problem report list for the reuse component show acceptable problems due to latent bugs; i.e., is the reuse software reliable and mature?				
23	Does documentation exist describing the nature and extent of testing achieved on the original reuse software component exist? If so, is the testing achieved sufficient for the reuse purposes?				
24	Does the reuse component have associated metrics indicating				
CHANGE MANAGEMENT					
25	Has the change management process for the reusable component been evaluated? Have all recommended changes been implemented				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
PROGRAMMING ENVIRONMENT					
26	Have all differences in the programming language of the reusable component been evaluated?				
IMPLEMENTATION					
27	Do implementation documents exist and have they been evaluated?				
FEASABILITY ANALYSIS					
28	In the event that modifications to the reuse software component are necessary, has the feasibility of accomplishing those changes been assessed?				
ALTERNATIVES EVALUATION					
29	Has an alternative to the proposed reuse strategy (in the event that the reuse becomes infeasible) been identified?				
30	Does the alternative to the reuse strategy include completed cost, resource, and schedule impacts?				
ORGANIZATIONAL EVALUATION					
31	Has the organization which produced the reusable component been evaluated for consistency of fielding successful products?				
32	Has the consumer organization been evaluated?				
TRADE STUDIES					
33	Have technical, cost, and schedule risk assessment and trade studies, to include prototyping, been conducted to assess the reuse benefit?				
DOMAIN KNOWLEDGE					
34	Have original development team members been included in the Integrated Product Team (IPT) or to provide support to the IPT, i.e., is domain knowledge available?				
MAINTENANCE APPROACH					
35	Has a maintenance approach been defined to support maintenance issues discovered by both the producer and the consumer?				

Downloaded from http://www.everyspec.com

Item #	Item Description	Disposition Status	Comments/Rationale/ Resolution/Future Action	Verification Approach/ Objective Evidence	Verification Status
QUALITY ASSESSMENT					
36	Has a quality assessment of the reuse component been performed, and has the reusable component been evaluated at an acceptable quality level?				
37	Have reuse component service history and error rates been evaluated?				
38	Has the reuse component been evaluated as acceptable based on having a large user base and longevity in operation?				
39	Have measures of performance margin and key performance metrics been collected to validate component performance?				
40	REWORK EVALUATION: Has an evaluation of any needed additions or other changes to the s/w proposed for reuse been made?				
REWORK					
41	REWORK EVALUATION: Has a rework effort, cost, and schedule estimate been completed and validated based upon any identified additions or other changes to the s/w proposed for reuse?				
RISK ANALYSIS					
42	Have the obsolescence risks including any custom h/w required, vendor support and end-of-life re-host alternatives been considered?				

Downloaded from http://www.everyspec.com

Downloaded from http://www.everyspec.com

Appendix C. Reuse Decision Process Implementation Example

This example demonstrates the underlying tasks that enable the reuse decision process discussed in Section 2/Figure 1. Figure 2 below identifies four core elements of this process; (1) a formal review process, (2) evaluation criteria tied to the previous (Section 2) decisions, (3) continuous risk evaluation, and (4) life-cycle verification. Each of these four elements is discussed in this appendix as organized in Figure 2.

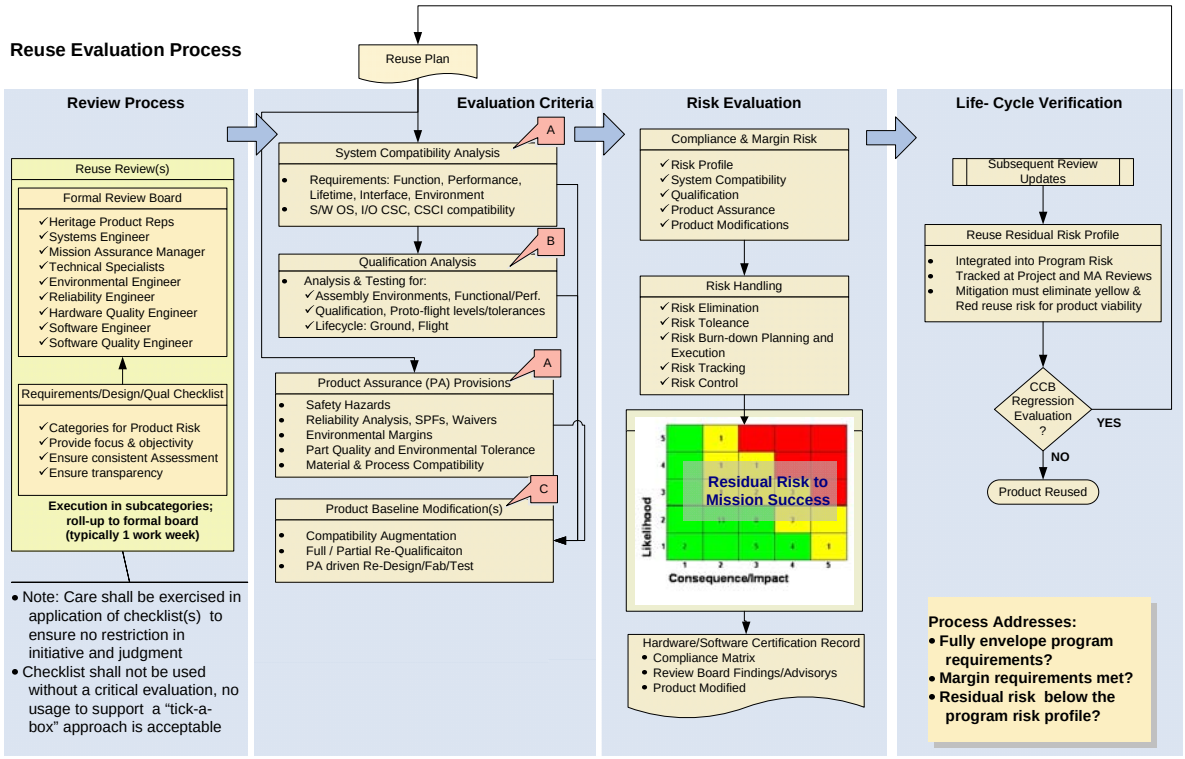

Figure 2. Reuse verification and implementation process flow.

The review process shall include the establishment of a formal independent review board, and the collection of findings, directives, action items, and advisories as products of the board. Objectives of the review board include implementing the evaluation criteria and risk evaluation processes shown in Figure 2.

Review Board Membership and Scope

Reuse review board membership should include members from many disciplines and if possible heritage product expertise. A sample list of board membership is identified in Figure 2. This membership shall provide the expertise to effectively review reuse decisions. The role of this independent non-advocate board is to clearly identify the risk of reuse. The board makes recommendations regarding product reuse but does not have the authority to make actual decisions regarding reuse implementation. Discipline expertise may include, but need not be limited to, Systems Engineering, Design Engineering, Manufacturing Engineering, Mission Assurance, Material and Process Engineering, Component Engineering, and Environmental Engineering (stress, dynamics, thermal, and survivability analysis). Each board member should have responsibilities, accountabilities

Downloaded from http://www.everyspec.com

and authority defined. Every effort should be made to retain the same review board membership throughout the development lifecycle of the product, which sometimes may take years. Board members should understand and review media applicable at least one level of integration lower than the integrated reuse product. In addition, any high-risk or long-lead items necessary to produce the reuse product should be identified and their availability, producibility, and reliability discussed, from a technical perspective, during the review board meetings.

A member of the board, either the product responsible engineer for in-house developments, or the subcontractor engineer for outside product should be assigned the primary responsibility of assessing and providing sufficient documentation for the reuse product and demonstrate its applicability on the program.

The board must have program management and non-advocate representation which conjunctly provide the authorization to proceed based on the product's review demonstrating that the product fully envelopes the program requirements with sufficient margins or can be tailored to meet the requirements within the risk profile of the program. Nominally the program management that is incorporating the reuse product must make the final decision on reuse based on the review board identified risks. The program's decision should be a collaborative effort making the best risk balanced decision for the program. The review board should have the authority to raise objections though an independent path if they feel that the reuse is violating the risk profile of the program.

It is essential that the execution of the review process is carried out in topic categories with evaluation by domain experts and the results of their assessment rolled up to the formal review board for evaluation and integration of the product reuse total risk posture.

Review Board Objectives

The objectives of the review board identified under evaluation criteria and risk evaluation in Figure 2 include:

a) An evaluation of product compatibility with requirements flowed to it from appropriate parent specifications. This will include evaluation of requirements for functions and performance, lifetime, interface, and environment.

b) Evaluation of the life cycle flow of the product to validate its qualification against program qualification requirements including margins and durations.

c) Identify and assess risks associated with the use of the product.

d) Identify and assess risks associated with build-to-print manufacturing or recoding for this application.

e) Identify additional work, modifications, analysis and/or testing required in order to accept the inherited product.

f) Verify that program requirements are correct.

Additional considerations that should be evaluated to support the above objectives can be found in appendices A-1 and A-2.

Downloaded from http://www.everyspec.com

Review Board Success Criteria

Reuse Review Board success will be based on the board's ability to effectively evaluate how the reuse product envelopes the requirements of the program and identify any residual risk associated with the new application. Success criteria include:

a) Reuse product history is adequately established with objective evidence.

b) The reuse product meets the requirements, constraints, and risk policy of the program.

c) Where the existing product does not meet program requirements, the work necessary to bring the product into compliance is defined, does not violate the product reuse baseline, is compatible with program resources and schedule, and does not exceed the risk profile of the program.

d) If a redesign is required, the difference in performance, form, fit, and function, and reliability is known and consistent with the program's baseline for use of the product.

e) For software reuse products, the availability of support documentation and appropriate compilers is clearly understood.

Requirements, Design, and Qualification Support

Supporting the review process are evaluation considerations, in the form of checklists, provided in Appendixes A-1 for hardware reuse and A-2 for software reuse. These considerations are provided as aids for identifying categories of risk in evaluating the product for reuse. The lists should be used to bring focus and objectivity to the evaluation process and ensure consistency across programs. The considerations highlight common driving factors for reuse across industry without invoking individual company propriety processes.

Caution must also be exercised to ensure that use of these checklists does not restrict engineering initiative or judgment. A thorough evaluation must still be performed to ensure no critical factors are eliminated from consideration due to unique requirements and/or constraints of the program. Under no circumstances should such lists ever be used in support of a "tick-a-box" approach.

Evaluation Criteria

Supporting the review boards objectives are specific evaluation criteria that can be classified into the four categories shown in Figure 2. These are:

- System Compatibility Analysis
- Qualification Analysis
- Product Assurance Provision Assessment
- Product Baseline Modifications

Each of these reuse evaluation categories provides insight into the product reuse risk for the program. Each of the evaluation categories serve as the entry point for the reuse decision gate discussed in Section 2 and Figure 1. Each of these categories is examined below within the context of reuse risks.

Downloaded from http://www.everyspec.com

Appendices A-1 and A-2 provide specific hardware and software considerations to aid in execution of these criteria.

A recommend way to capture the following assessments is through the use of a compliance matrix. The compliance matrix tabulates the comparison between the new program requirements and the product technical baseline, including the products characteristics and capabilities. In addition, the compliance matrix should specify the margin between the new program requirements and the product's capability and identify any issues resulting from assessment of margins.

System Compatibility Analysis

System compatibility analysis is the first step in comparing the product pedigree with the new program requirements. Tools for performing the system compatibility analysis include system and block diagrams, detail requirements evaluations, and interface-control drawings (ICDs). Block diagrams illustrate the electrical, mechanical, thermal, optical, and RF interfaces which link the reuse product to other elements comprising its parent subsystem. ICDs in turn provide detailed requirements for each interface appearing in the block diagram. Unit-level requirements must precisely agree with those in the ICDs thus ensuring that the reuse product, once integrated with the rest of the subsystem, will function as intended. The process of decomposing interfaces between units into a block diagram, documenting these in an ICD, and then flowing all requirements to relevant unit specifications immediately identifies interface incompatibilities of the reuse product. Requirements evaluations also consider the functional, performance, lifetime, and environmental capabilities of reuse products in the context of programmatic requirements. Programs must complete requirements flow downs by PDR to determine the extent to which reuse products comply with their new applications. Detailed requirements versus capabilities matrix comparing reuse-product capabilities and qualifications against system requirements should address all of the items in the following list:

a) Functional requirements should include consideration of program mission profile (mission type, total lifetime, cycling environment) and performance requirements including accuracy, precision, and tolerances. The product's capability with respect to mission life operations must be assessed. A focus on the product's heritage verification and validation plan will provide insight into the product's compliance with any new or more demanding functional requirements, and detailed components derating analyses will ensure that reuse hardware will not fail unexpectedly

b) Interface requirements compatibility evaluates physical and functional demands that are levied onto or by the product so that overall system functionality is met.

- Physical interfaces may refer to inertial properties, volume, mass, dimensional and tolerance requirements (e.g., clearances), thermal, fields of view, dynamic properties, and materials compatibility.

- Electromagnetic interference and compatibility considerations (EMI/EMC) lead to specifications including levels and regulation of power, and requirements on voltage, frequency, current, and transients, grounding, shielding, etc.

- Functional signal interface demands will include timing, frequency, duty cycle, rise/fall times, accuracy, voltage levels, transients, RF signal quality, bit-error rate, etc.

Downloaded from http://www.everyspec.com

c) Environmental requirements compatibility assesses all the physical conditions that the reuse product will be exposed to during program development and throughout the mission. This will include fabrication, tests, ground handling and transportation, and operations elements.

- Physical environments can include temperature, pressure including vacuum, humidity, vibration, shock, acoustics, static loads, meteoroids, and radiation conditions.

d) Software product compatibility must assess all interfaces including the operating system in both operational and simulator environments. Functional compatibility will include I/O frequency, compatibility with other software and processes being executed, other subsystem interfaces, etc.

Qualification Analysis

The previous System Compatibility Analysis focused on a comparison of the program baseline against the new program requirements. Qualification analysis focuses on how compliance to those requirements was demonstrated during the product's heritage qualification, proto-flight, and acceptance testing procedures. This should include an evaluation of the expected operational environment and analyses of design margins.

Ultimately, environmental qualification must demonstrate in-specification product performance and required margins relative to the expected operational environments detailed in the System Compatibility Analysis. The assessment of heritage qualification data should include the environmental verification methods (i.e., test and/or analysis, etc.), actual test durations and levels, and the test and/or analysis results. This product baseline information should be compared against the new program environmental approach, as specified in the program's environmental requirements document.

While flight heritage leads to confidence in a product for new space applications, it does not by itself qualify the product for those new applications. Reuse decisions based on flight heritage must always include detailed reviews of the heritage qualification envelopes and requirement-versus capability comparisons.

Product Assurance Provisions

The Product Assurance (PA) product reuse analysis should be performed in parallel with the System Compatibility Analysis and focus on the product's assurance controls and measures. Product Assurance should provide objective evidence that it has positively impacted previous programs and discuss any process modifications required to guarantee mission success for the new program. The assurance controls and measures of interest include:

- System Safety
- Reliability Assurance
- EEE Parts
- Quality Assurance
- Materials and Processes & Contamination Control
- Configuration Control

Each of these disciplines is briefly examined below for their contribution to risk of product reuse.

Downloaded from http://www.everyspec.com

a) System Safety: Previous identified safety hazards and the corresponding safety-inhibit features of the reuse product should be evaluated relative to the new program's application. Initially the focus should be if the hazards and inhibit features still apply in the new application and second their effectiveness in meeting the new requirements. Third will be and evaluation of any new hazards or inhibit feature requirements resulting from the new program application.

b) Reliability Assurance: Comparison of the product's reliability assurance program should consist of:

- Single Point Failure (SPF) design philosophy, internal and external to the product (e.g., requirements levied on the design through system-level SPF concerns, and requirements due to product-level SPFs)
- Extent of reliability analysis performed and their findings
- Anomaly and failure history
- Waivers required on prior applications of the product

Reuse assessment of previous reliability analysis should examine the completeness of the analysis and the corresponding documentation. Analyses could include: Worst-Case Analysis (WCA); Failure Modes, Effects and Criticality Analysis (FMECA); Fault Tree Analysis (FTA); Parts Stress Analysis (PSA); Structural/Dynamical Analysis; Thermal Analysis; Producibility; and Total Ionizing Dose (TID), ELDRS, Single Event Effect (SEE) analysis.

Review of anomalies and failure from previous product application should evaluate both the failure reporting system during the product development as well as the reportable failures. Evaluation of the products reporting system should look at both what events were considered reportable, when the anomaly and failure reporting effort began, and how that compares with the new program requirements. Finally an assessment of the risk rating used and residual risk identified should be assessed.

c) EEE Parts: EEE parts should compare the following items with the new program parts requirements:

- Parts qualification level
- Parts lists availability from the product baseline
- Parts obsolescence and proposed replacements
- Parts specifications used for qualification and screening
- NSPARs and/or waivers documented use of non-standard parts and waiver of parts requirements
- Parts derating requirements
- Parts failure reports
- Total Dose and Single Event Upset (SEU)/Single Event Latch-up (SEL) requirements
- Parts-related GIDEP and internal (i.e., proprietary) alerts
- Other parts control requirements

d) Quality Assurance: Hardware and software quality assurance should include a review of the product procurements for acceptability by comparing QA system requirements and workmanship standards against the new program requirements. Evaluation criteria should include condition, qualification status, possible effects from shelf-life aging and/or handling,

Downloaded from http://www.everyspec.com

adequacy of fabrication and inspection records, and the completeness of the end-item data package.

e) Material and Processes & Contamination Control: Material and process items that should be addressed during the reuse review include:
   - Approved Materials Identification and Usage List (MIUL) including the quantity of metallic and non-metallic materials and the processing specifications for those materials.
   - The total mass loss (TML) and Condensable Volatile Material (CVM) for non-metallic materials.
   - Non-standard materials and fracture-critical applications (welds)
   - Applicable material-related GIDEP and internal alerts
   - Non-standard fasteners
   - Prohibited materials

   Contamination control reuse evaluation should assess the reuse product's contamination control plan requirements and their subsequent verification and validation. Also the MIUL should be evaluated for the molecular contamination sources.

f) Configuration Control: Configuration control aspects that should be evaluated including ensuring the products technical baseline drawings have been archived and reflect the as-built configuration; all approved drawing changes have been incorporated; and the approved engineering change requests (ECRs) and waivers that impact product baseline has been incorporated into the baseline documentation.

Product Baseline Modifications

Design changes incorporated at various states of product development can dramatically affect product reliability, so a key task in the evaluation of product reuse is the starting point for relevant operating experience.

Product baseline modifications required due to exceptions meeting program requirements should be carefully evaluated in determining the applicability of prior operating experience. For instance, minor packaging changes that would not impact product operating characteristics may have no significant bearing on the applicability of prior operating experience. On the other hand, internal modifications required to the product that change its performance requirements may invalidate the applicability of previous qualification and flight heritage. Extreme care must be taken in the application of the above evaluation criteria because even a minor packaging change--for instance, a different surface finish--could significantly affect the assembly's thermal performance.

Compliance matrix comparisons developed in the three Evaluation Criteria subsets discussed above and shown in Figure 2 should be developed into a list of differences and the proposed handling of them with their impact on the planned use of the reuse product. These product baseline modifications will drive the assessment of requirement augmentations and product impact, full or partial qualification, and product assurance driven re-design and analysis.

Risk Evaluation

During execution of this reuse evaluation process, risks to the program will be identified as each of the Evaluation Criteria topics are covered and captured in a reuse risk list. The review board must

Downloaded from http://www.everyspec.com

examine this risk list periodically during the process to ensure that all risks are pertinent and understood. The risks must be evaluated relative to their criticality for acceptance of the reuse product into the program flow.

Initially the reuse program's risk profile must be established. That is the mximum level of risk that is tolerable given the program's mission success criteria. For instance does the program allow single point failures, what level of piece part quality is specified, what is the qualification margins required against the mission environment, etc? This profile establishes the risk tolerance commensurate with program requirements allowing a comparison to be made between the program's needs and the risk of reuse.

Next the reuse product risk will be assessed against the program risk profile to evaluate if the products risk fits within the cost, schedule, risk management baseline and/or the residual risk to mission success is below the risk profile floor for the program.

Each risk source must be assessed and a plan for mitigation proposed. Possible mitigation approaches include reallocating requirements among various subsystem units to reduce the burden previously carried by the reuse product. Alternatively, the program may decide to baseline reduced system performance or may propose different mission environments. When reallocation or specification relief is not an option and the noncompliance requires mitigation, the associated actions should be carried forward as part of the program's normal risk-tracking process. This process must estimate the likelihood of success, any consequences and trades associated with the mitigation approach, and include burn-down plans for risk during subsequent program execution.

The output of this risk evaluation process should be a hardware and/or software certification record that captures the latest compliance matrix for the reuse product, review boards findings and advisories with their closure status, and progress on any required product modifications.

Risk evaluation for product reuse should be enveloped by the programs/companies nominal risk process so that the reuse will have the risk assessment breadth and depth, thorough risk mitigation planning, and full lifecycle risk management commensurate with the program that is committing to the reuse.

In summary core risk criteria for reuse include:

- Since reuse is based on early design decisions during the proposal phase and planning requirements definition phase of the program, ensure that reuse baseline plan assumptions and required product modifications continue to support the program's resource availability.
- Continually assess the reuse product or products for their impact not only on implementation risk during the program but on the aggregate mission success risk profile.
- Focus on cost, schedule, and technical risks for continued validity of the reuse product technical baseline throughout integration and test including verification and validation activities.
- Identify any additional risk that result from closeout of reuse review team action items

Life Cycle Verification

The reuse plan baseline established for a given product must integrate the product into the programs life-cycle flow from the assembly-level to the system level (or for software from individual modules to an integrated build). The plan should include pertinent milestones such as acceptance/performance

Downloaded from http://www.everyspec.com

and applicable qualification testing (including stress and life testing), applicable inspection points, reviews, and opportunities to accumulate operational hours.

The process discussed in the previous Evaluation Criteria sections should be implemented during the planning phase of a program, initially during the proposal phase and updated during assembly level requirements definition where product level requirements are fully defined. However, during the subsequent design phase trade studies will likely be conducted to better balance system resources such mass, power, cost, schedule, and technical risk to meet key program requirements. This may affect the design architecture of the system and hence impact the previous reuse baseline. These changes require evaluation by the program Change Control Board (CCB). The outcome of this evaluation should be ramifications to reuse products including amount of regression evaluation the product most go through for updating its reuse plan.

An integral part of the life cycle verification will be the continual update of the reuse risk profile coming from the Risk Evaluation discussed above and shown in Figure 2. This profile should be integrated with the programs risk list, discussed key program milestones, and the mitigation plans established must be evaluated ensuring that subsequent reuse product risks are reduced to low or green likelihood and impact during program execution.

Downloaded from http://www.everyspec.com