

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 1 of 19	

Review of the Constellation Level II Safety, Reliability, and Quality Assurance (SR&QA) Requirements Documents during Participation in the Constellation Level II SR&QA Forum

August 7, 2008

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 2 of 19	

Approval and Document Revision History

NOTE: This document was approved at the August 7, 2008 NRB. This document was submitted to the NESC Director on September 16, 2008 for configuration control.

Approved:	_____ Original signature on file NESC Director	_____ 9/19/08 Date
-----------	------------------------------------------------------	--------------------------

Version	Description of Revision	Office of Primary Responsibility	Effective Date
1.0	Initial Release	Kenneth D. Cameron, NESC Deputy Director for Safety	8/07/08

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 3 of 19	

NESC Participants

Kenneth D. Cameron, NESC Deputy Director for Safety
 Steven J. Gentz, NESC Principal Engineer
 Robert J. Beil, NESC Systems Engineer
 Nancy J. Currie, JSC NESC Chief Engineer (NCE)
 Stephen A. Minute, KSC NCE
 Steven S. Scott, GSFC NCE
 Michael D. Smiles, SSC NCE
 Charles F. Schafer, MSFC NCE
 Walter Thomas III, GSFC NESC Deputy Chief Engineer (NDCE)
 Cynthia H. Null, NASA Technical Fellow for Human Factors
 P. Michael Bay, NESC Systems Engineering Technical Discipline Team (TDT) Support

Introduction

At the request of the Exploration Systems Mission Directorate (ESMD) and the Constellation Program (CxP) Safety, Reliability, and Quality Assurance (SR&QA) Requirements Director, the NASA Engineering and Safety Center (NESC) participated in the Cx SR&QA Requirements forum. The Requirements Forum was held June 24-26, 2008, at GRC's Plum Brook Facility. The forum's purpose was to gather all stakeholders into a focused meeting to help complete the process of refining the CxP to refine its Level II SR&QA requirements or defining project-specific requirements tailoring. Element prime contractors had raised specific questions about the wording and intent of many requirements in areas they felt were driving costs without adding commensurate value. NESC was asked to provide an independent and thorough review of requirements that contractors believed were driving Program costs, by active participation in the forum.

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 4 of 19	

Overview of Lessons Learned and Recommendations from Forum Splinter Groups¹

Lessons Learned:

- A face-to-face forum discussion between empowered representatives of Program, Project and Element stakeholders should be held as early as possible before Program-level requirements are base-lined.
- Effectiveness and efficiency of the entire safety review process can be enhanced by maintaining consistency in Safety Review Panels’ approach and stability in their membership. This allows expectations to be understood by the design teams and allows the Panels’ technical knowledge to mature along with the design maturity.

Problem Reporting, Analysis and Corrective Action (PRACA) Recommendation

- Because the CxP version of “PRACA” is significantly different from previous programs, the CxP should consider re-naming their nonconformance and corrective action reporting system to avoid potential difficulties or errors in implementation caused by confusion in terms stemming from legacy meanings.

Acceptance Data Package (ADP) Recommendation

- To maximize the overall Program safety and reliability, the CxP should actively seek perspectives from the Cx Projects (who are responsible for hardware design and delivery) on those items of highest potential for maximizing their element’s safety and reliability.

Reliability & Maintainability Recommendations

- To avoid potential confusion between the list of critical items (a product) and the risk evaluation/analysis processes, the CxP SR&QA should change the lexicon of the currently-used "CIL" to distinguish the FMEA-derived List from the data collection/ evaluation/ assessment Process.
- To provide accurate Program risk assessments, CxP SR&QA should maintain FMEA(s) and Critical Items Lists for all items in each subsystem and system.
- To more accurately compare and balance risks across the entire Program, CxP SR&QA should ensure that the risk Likelihood and Consequence (also called Impact or Severity) rankings are applied uniformly across all Projects/Elements and sub tier suppliers.

¹ Splinter Groups with no Recommendations are not included.

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 5 of 19	

General Observations

The forum was very productive and was a major step forward in the on-going SR&QA process of aligning the requirements throughout the Program and reducing the Program costs, compared to the original SR&QA requirements baseline. The face-to-face interaction among involved parties (Program, Projects, Elements, Suppliers, and Independent Observers) resulted in faster communication and a better understanding of the issues. The prime contractors were well represented in all sessions and did a good job identifying cost-drivers prior to the forum, evident by the number of items they had submitted to the discussion matrix. They were candid in the sessions and provided honest discussions of benefits and risks of existing Space Shuttle Program (SSP) and International Space Station (ISS) Safety and Mission Assurance (S&MA) systems. Their openness and team player attitude contributed greatly to a better understanding of the Program's needs and expectations, versus potential costs of meeting those needs and expectations. The NASA Project SR&QA representatives also were fully engaged in the splinter sessions and with Team Zero. In general, the forum provided many effective resolutions of open discussion items and the NESC concurred with the outcomes, unless noted in the following position paper. ***Lesson Learned: A face-to-face forum discussion between empowered representatives of Program, Project, and Element stakeholders should be held as early as possible before Program-level requirements are base-lined.***

The Program-level SR&QA attitude coming into the splinter sessions seemed to be geared toward top-down detail and control, even though the splinter groups were told that CxP is "project centric". The desire for Level II information access without contact with Levels III and IV was a frequently recurring theme. This, in part, was attributed to the reported plan for reduced sustaining engineering at Levels III and IV. It also appeared that review and cross checking of draft documents within Level II, and by Levels III and IV, was still on-going. This was evident by the large number of forum items being readily resolved and the forward work needed to clarify sections of the retained requirements. Significant time was directed towards resolving confusion or conflict in the definition of nomenclature. As an example, protracted discussion detracted from the Process Failure Modes and Effects Analysis (PFMEA) splinter due to interpretation of the terms "special" and "critical" processes. These differences persisted from prior meetings and generally were not resolved at this meeting.

One general finding is that some of the Level II requirements were unclear or too prescriptive in nature. As a guiding principle, Program-level SR&QA requirements should address the desired outcomes while Project-level requirements should address the specifics of implementation. Several examples are described in more detail in subsequent sections of this white paper, including: using a PRACA system as the single problem reporting system versus the desire to have a single compilation of all the elements/projects nonconformance reports; the detailed content of a deliverable's ADP versus the desire to utilize data for higher level trending and

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 6 of 19	

analysis; the frequency of vendor audits versus the desire to have an auditable vendor audit program; and prescribing PFMEA as a requirement versus the desire to implement process control. The forum was successful in providing the dialogue leading to a common understanding of the Program's desired outcomes with appropriate changes to the requirements documents to more clearly define what is expected of the Projects and Elements without prescribing how to implement Level II requirements.

A focus on cost-cutting activities surfaced throughout the review. Cutting unnecessary costs is an admirable goal; however, each individual reduction in activity must be assessed as to its effect on the whole Program. As a balance, the Team Zero reminded the Splinter Groups that, in general, SR&QA does not cost money, it saves money. Injuries, mishaps, quality slips and system problems found late in the schedule are the real cost drivers for the Program. It is important to recognize that a design decision, made to optimize one parameter (such as performance), may also increase overall system vulnerability to quality problems or critical failures. In protecting against these system vulnerabilities, costs seemingly attributable to SR&QA should really be considered part of the total cost of the particular design choice. The forum was very valuable in raising awareness of efficiency in SR&QA activities, without going too far.

Judiciously applying SR&QA effort where it does the most good is necessary to ensure that safety and reliability are adequately addressed across the whole Program. It is hard to create a one size fits all sets of SR&QA requirements at Level II that will guarantee the appropriate result at the hardware and software item elements controlled by Level III and IV requirements. To assure that the Program gets the most "bang for their buck", the requirements at Levels II, III, and below should be tailored to match the chosen system design to attack the risk drivers. Until this is done it will be premature to declare a "pencils down" state for the requirements. In summary, it was necessary and very productive to hold the SR&QA Requirements Forum as a face-to-face meeting (and the choice of remote location also was beneficial) to rapidly clarify and negotiate issues identified in the draft Level II SR&QA documents. Overall, the SR&QA Forum was successful in aligning all stakeholders and facilitating rapid information transfer. NESC participation provided added value in discussions by providing independent expertise and domain knowledge, and by facilitating the removal of any impasse, as needed.

Comments on specific Splinter Group discussions follow.

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 7 of 19	

Discussion of the Problem Reporting, Analysis and Corrective Action (PRACA) Splinter Group:

(NESC POCs: Robert J. Beil, Stephen A. Minute, Michael D. Smiles)

The PRACA splinter group had good cross-functional participation from the prime contractors and Projects. Broad consensus was reached, dealing with 47 comments, 35 of which were unique (non-duplicates), 6 were withdrawn, and 2 were elevated for further deliberation with Team Zero. One of the elevated items was a comment to CxP 70059 (Safety, Reliability and Quality Assurance Requirements) relating to the existence of a Program-level Material Review Board (MRB) function. A second comment was to CxP 70068 (PRACA Requirements, volumes 1-3) relating to PRACA reporting criteria.

The 47 comments were broken into the six categories: *Single System, Reporting Criteria, Processes, Technical, MRB, and Miscellaneous*. Out of the above breakdown, there were 4 primary topics of interest: the first three related to PRACA reporting criteria and the fourth regarding the existence of Program level MRB. The primary topics were as follows:

- Use of a single problem reporting system
 - Whether all data or a limited subset should be entered into PRACA (for instance, SSP and ISS Programs limited contractor reporting to a subset of material review items)
 - When during the lifecycle should the prime contractors data delivery commence (i.e., starting with acceptance testing, post-CDR, etc.)
 - Whether the CxP should have a MRB or delegate this function in its entirety to the Projects
1. Regarding the PRACA reporting criteria, there was little disagreement regarding the use of a single PRACA system. Generally, Ares contractors were in agreement with establishing an interface to their internal nonconformance database(s) given that they are allowed to maintain their records in their internal system and that NASA will pull data on a regular basis into the single NASA PRACA system. Ground, Crew Exploration Vehicle (CEV) and Government-Furnished Equipment (GFE) Projects were also supportive of a single PRACA system. Pulling the data into NASA PRACA will necessitate the development of a ‘filter’ that maps data fields (from each contractor and/or Project nonconformance and corrective action reporting system) into the appropriate Level II PRACA fields. Ideally this will be an electronic interface and will be a one time development for each. This is particularly important as the agreement reached at the Level ‘0’ board is to include all nonconformance data in PRACA, including anything ranging from minor nonconformances to material review items. The prime contractors agreed that since they are already collecting this data electronically, this is not a significant cost impact in terms of the transfer of the data.

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 8 of 19	

2. There are residual concerns regarding transfer of all nonconformance data. These include the cost impacts associated with addressing the same questions, from multiple NASA offices to contractor staff, on problem status and actions (failure to follow the chain of command) and concerns about time spent chasing perceived issues due to uninformed evaluators “second guessing” the contractor’s actions with respect to analysis, causal analysis, corrective actions and other data posted in CxP PRACA. There are also concerns about an “apples to oranges” comparison of different contractors, and that data entered into the system will be used to punish contractors.

3. The third topic of interest regarding PRACA reporting criteria revolves around when the Program should start to collect data and was mostly due to confusing wording in the requirements. These questions were clarified, with the agreement that the start of data collection would be post-CDR for hardware or start of Acceptance Validation and Verification for software.

The resolutions reached during the forum pertaining to the first three topics listed above make the CxP version of PRACA significantly different from previous programs.

Because the CxP version of “PRACA” is significantly different from previous programs, the CxP should consider re-naming their nonconformance and corrective action reporting system to avoid potential difficulties or errors in implementation caused by confusion in terms stemming from legacy meanings.

4. The final major topic discussed was the need for a limited Program level MRB. This is an issue between the Program and the Projects. Other large NASA Programs (in particular SSP and ISS) have Program level MRBs, usually at the hardware integration level, that are put in place to address significant issues that change the level of risk being accepted by the Program with a particular material review. Team Zero assigned an action to further study this item.

**Discussion of the Acceptance Data Package (ADP) Splinter Group:
(NESC POC: Charles F. Schafer, Steven J. Gentz)**

Observations concerning the Cx SR&QA requirements for ADP include:

1. The data required in a Cx ADP were described generally in para. 1.0 of Cx 70146 as *“The ADP provides a complete and verified status, including the as-built configuration, of hardware or software, contains information pertinent to acceptance, identifies information unique to the item, and enables the continuation of required activities by the using organization. The ADP is prepared as part of the hardware or software acceptance/delivery criteria and will be maintained throughout the hardware or software life cycle after government acceptance.”* Given this definition, it seems clear that the

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 9 of 19	

ADPs are provided as part of the contracts that each Project or Element has with the suppliers. Many of these contracts are already in place. Changes to the deliverables under these contracts may be expected to change cost. The discussions in the ADP splinter sessions led to specific language in individual requirements clarifying the role of the Projects in defining the content of the ADPs (for example, ADP-B-7 and ADP-B-6).

2. There was a mismatch between the Levels III and IV understandings of an ADP versus the Level II desired concept of ADP. A typical ADP as viewed by Levels III and IV is a discrete static data set deliverable applicable to a subcomponent, component, element, and/or system. The Level II concept was to use ADP as an online system able to archive, retrieve, compare, trend, and report data from a variety of like items. Cx 70146 does not try to define implementation requirements for an electronic Cx required ADPs. Paragraph 1.2 (page 8) explains that this will be done in a separate document. In spite of this, there was a great deal of discussion initially in the ADP splinter session about the need to connect the implementation requirements with the product to be delivered. One source of debate was the requirement for electronic signatures. The suppliers saw this as an additional requirement over their contractual requirements. Ultimately it was agreed that the Cx SR&QA requirement would be satisfied by a scanned document (pdf format).
3. The use of the terms “ADP report” and “query” also generated extensive discussion. These terms apparently implied to the suppliers that additional deliveries of data were being required over which they had planned and were contracted by the Project/Elements to provide. In these cases, the issue was primarily that repeated deliveries of data already ADP deliverable seemed to be implied. Para. 4.1 requires that *“ADP providers shall not deliver duplicate acceptance data when that information already exists in other CxP databases, which are under CxP configuration management [CxP-SRQA-ADP-0012].”* These issues generally were ultimately resolved consistent with this requirement (no duplication of delivery).
4. The issue of what documentation must be text searchable versus what is only desirable was not completely resolved. This is an open issue to be resolved per the following: *“Develop table of mandatory text-searchable data elements. Also conduct ADP Face-to-Face with appropriate project representation, including data providers and end-users of the acceptance data (e.g., Engineering).”* Cost impacts of this are pending completion of this “Tiger Team” activity. The charge to the supplier team (in developing data which will be used in the face-to-face activity) is to assess their data elements to determine which of three categories they fall under:
 - Data that can be provided in a text-searchable native format.
 - Data which is typed and can be scanned using Optical Character Recognition (OCR) software.

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 10 of 19	

- Data which is handwritten and is, therefore, more complicated to convert into a text-searchable format (i.e., data has complex character recognition challenges if OCR software is used to convert it). Although additional work is required for resolution, the establishment of the “Tiger Team” and the data categorization process should provide a rational means for determining additional data requirements (if any) and their cost impacts.

5. During the discussions of ADP Requirements, a specific illustrative example was presented in side discussions with the First Stage Project Manager. In this system, knowledge of the propellant grain integrity, insulation integrity, and the integrity of bond lines between propellant and insulation strongly affects the ability to understand the safety and reliability of a solid rocket motor. Radiography is used to detect voids and open un-bonds for propellant and insulation in solid motors. Radiographic coverage of the redesigned solid rocket motor (RSRM) has historically been about 30 percent, however, coverage of 100 percent is possible, desirable, and represents industry best practice. As pointed out by the First Stage Project Manager, combining 100 percent radiographic coverage with a move to digital imaging could reduce costs to the Project. Additionally, other methods exist to observe cracks or un-bonds that are not open (no void exists). Application of one of these methods (i.e., an acoustic method) to characterization of the solid motor propellant and insulation integrity could further assure that a given motor is safe to fly. As this SRM example suggests, the teams closest to the design and delivery of the hardware are often in the best position to consider relative added value for test data (per unit cost). ***To maximize the overall Program safety and reliability, the CxP should actively seek perspectives from the Cx Projects (who are responsible for hardware design and delivery) on those items of highest potential for maximizing their element’s safety and reliability.***

**Discussion of the Software Assurance Plan (SAP) (CxP 70128, Baseline, Release Date: August 23, 2007) Splinter Group:
(NESC POC: Steven S. Scott)**

The CxP SAP was reviewed independently outside the participation of the forum. Observations concerning the SAP include:

1. The document is written at a very high-level and contains numerous generalities and “boiler plate” statements. However, it is generally acceptable for a high-level assurance plan. The Software Assurance life cycle plans also seem reasonable enough, but they are largely motherhood. In particular, the SAP does not address any automated tools that Software Assurance will use to accomplish its work. It is not clear whether there is any standardization in this area.

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 11 of 19	

2. Section 1.2, first paragraph, third sentence, page 5 of 42 says this plan applies to computer programs for “Complex Electronics.” This ambiguous term is not generally nor widely accepted. Software Assurance has used it as a term for programmable logic hardware devices that are not computer software like Field Programmable Gate-Arrays (FPGAs), Application-Specific Integrated Circuits (ASICs), etc. If this term is intended in this use to mean software that runs on embedded processors that are instantiated (i.e., implemented, physically realized) on programmable logic devices, then it makes sense for software assurance to be responsible for monitoring it. If it refers to the functional programming of the hardware devices themselves, then this would be the responsibility of digital logic designers and hardware assurance engineers as software assurance principles have limited application in this area. Similarly, the term “firmware” has become so ambiguous that the IEEE Glossary of Software Engineering Terms advises against its use. It is used to mean software code or data stored on a programmable device, which could be changed. Now it can mean almost anything.

3. The Glossary of Terms, Section A2.0, page 34 of 42, does not include the terms “Complex Electronics” nor “firmware. This is probably because of the ambiguity and confusion surrounding these terms. (It does, however, include such minor terms as “Oversight,” on which it places great emphasis.)

4. Many sections of the SAP contain statements that say “The Provider Software Assurance Manager will...” These statements are “pseudo” requirements. Requirements do not belong in a SAP but in a requirements document or specification. It is not clear that anyone will actually look in the SAP for requirements or even acknowledge that they are contractually obligated to follow “will” statements in a SAP. These are basically requirements that have no power of enforcement. They are requirements masquerading as implementation details.

5. Section 4.2.3, Software Reliability, page 18 of 42: Most of this section consists of the same thought repeated over several pages. It is clear that NASA does not have a very clear idea of what should be done and what will be acceptable in this area. Much of this is an attempt to extrapolate the well-developed principles of hardware reliability into the realm of software without much guidance or direction on how exactly to do this. Some specifics are:
 - Page 18 of 42, Section 4.2.3, first paragraph, sentence two states: “The emphasis for Software Reliability is a qualitative measure.” This seems somewhat self-contradictory but it illustrates a weakness that NASA is not very good at quantifying software reliability.

 - Page 19 of 42, Section 4.2.3.1, item g says: the Acquirer Software Assurance

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 12 of 19	

Manager will “summarize and elevate software reliability issues and findings to the CxP SR&QA Director”, but doesn’t give any indication of what these kinds of things might be or how they will recognize a software reliability issue. The entire section is filled with such vagaries and generalities.

- Page 20 of 42, Section 4.2.3.1, item h enumerates a whole list of things the Provider Software Assurance Manager will provide. There are no details or guidance on what NASA expects for items 2, 3, 4, 5, 6. These are terms from the hardware reliability discipline and it is not evident that NASA knows any specifics about what it wants or expects in the area of reliability modeling for software, reliability allocations for software, reliability predictions for software, etc. Will Software Assurance Managers recognize these things when they see them?
6. Page 30 of 42, Section 6.0, Software Assurance Program Metrics: This entire section is very vague. Almost anything satisfies it. There are very few specific examples (four, to be exact) of what NASA is expecting in the way of metrics. Since only four are “specified” (remember, this is not a requirements document), then those four are probably the only ones NASA will get. In some cases, the Acquirer Software Assurance Manager is obligated to prepare metrics from data it has not specifically requested and may not get from the Provider Software Assurance Manager (see page 30 of 42, paragraph 2, items a through e).

In conclusion, the CxP SAP is generally acceptable for a high-level assurance plan.

**Discussion of the Reliability & Maintainability Splinter Group:
(NESC POCs: Cynthia Null, Walter Thomas III)**

Specific observations and recommendations concerning the Reliability and Maintainability Splinter Group include the following:

Most of the Reliability and Maintainability Splinter Group discussion centered on relationships between Hazard Reports and other SR&QA products, especially FMEA/CILs. The following five fundamental questions were covered at various times during the extended sessions:

- Terminology differences between products and processes, stemming from past usage in legacy programs
- The value of retaining two independent processes with differing approaches, top-down and bottom-up, to ensure all hazards are recognized and evaluated
- Completeness in applying risk assessment processes and the consequent danger of reducing the set of items considered – that is, “ground-ruling out” some items

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 13 of 19	

- The need for accurate likelihood of occurrence quantification by including reliability-engineering expertise in assessment teams
- The importance of integrating risk assessments across the entire Program and supply chain, to provide consistent data for risk mitigation activities

While progress was made during the forum, a follow-up "Tiger Team" has been assigned to review and resolve the "FMEA/CIL" and Hazard Report/Analysis Level II requirements issues identified at the forum in both splinter group and Team Zero discussions.

1. Throughout the splinter meeting, there was continuous discussion centered on differing interpretations of the term "CIL." These interpretations derive from historical usage in past programs. In that heritage context, "CIL" has two meanings: (a) a list of critical items (derived from the FMEA and having Crit 1 or 2 severity/criticality); and (b) the process to research and provide rationale for using these Crit 1 and 2 items in spaceflight applications. Shuttle-derived usage of "CILs" means gathering, compiling, and assessing all relevant data for detailed analyses concerning a "CIL-listed-item." A first step to clarify these differing interpretations is to divorce "CIL" (the Critical Item List) from the subsequent assessment/analysis process, and rename the process to, for example, "Critical Item Safety Analysis". This will distinguish the list from the process. By renaming the process, another distinction is made from the former Shuttle process. This will be especially important if the process used to produce the CxP "Critical Item Safety Report" is implemented using a method different than the existing Shuttle method. ***To avoid potential confusion between the list of critical items (a product) and the risk evaluation/analysis processes, the CxP SR&QA should change the lexicon of the currently-used "CIL" to distinguish the FMEA-derived List from the data collection/evaluation/assessment Process.***
2. Considerable discussion ensued about the overlap between "doing a CIL" (the "process," see above) and generating a Hazard Report, and whether these processes are duplicative tasks. FMEA is a "bottoms up" and Hazard Report a "top down" approach. Each provides the Projects with an *independent* risk assessment for the same critical item(s) or element(s), from different points of view. Thus they are checks - one against the other.

The two analyses currently are performed by separate groups or organizations. (In one Team Zero presentation it was stated there were "FMEA/CIL empires" and "Hazard empires" – the words used by one senior manager). Some splinter participants stated that performing both is duplicative. One contractor proposed performing either one or the other (i.e., Critical item evaluation or Hazard Report) to reduce costs. Other inputs suggested these analyses currently are executed by "re-labeling" the corresponding analysis' cover sheet. This latter *practice* defeats the reason for performing both –

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 14 of 19	

independent analyses of the same critical item(s) to assure identified risk(s) have been assessed accurately.

Collaboratively involving those persons responsible for each analysis – particularly in the “research” or “data collection” phases for the corresponding analyses – could provide potential efficiencies for the Program. The same “basis information” would be applied for both the “bottoms-up” (Critical item evaluation) and “top-down” (Hazard Report). Researching these data collaboratively could reduce expended effort versus performing this data gathering independently. Furthermore, the collaborative approach would serve as a “real time” check and balance which would avoid subsequent dissention regarding the basis data. The two analytical techniques are then applied to the given item/subsystem being evaluated. A subsequent collaborative comparison of respective results will verify whether the risk ranks for the two analyses correspond. That is, if the bottoms-up and top-down analyses reach the same conclusion regarding mission risk impact(s), the analyses and the assigned risk are credible. If not, both analyses need to be reconciled to determine why equivalent “risk rankings” were not obtained.

These “concurrently engineered” Critical item evaluation and Hazard Reports would be performed at the lowest indenture level deemed appropriate by Level III requirements. This bottoms-up and top-down approach to evaluating and ranking the risks for human spaceflight systems provides the “checks” mentioned above. Once the Level III independent assessments are deemed credible, the data from the two analyses (for each item) can then be combined into one document (or other applicable data structure) with a summary page or paragraph (“Cover sheet”). Then, this would become the basis data for higher level risk assessments and integration (that is, at Level III/Project and then to Level II/Program). This enables the Projects and Program to integrate and assess all mission critical risks. Another potential advantage of this collaborative assessment process is that the risk Likelihood and Consequence (also called Impact or Severity) rankings can be more uniformly applied across all Projects and sub tier suppliers so the “risk roll-ups” at both Project and Program levels are accurate and not an “apples to oranges” comparison.

3. A lengthy debate about the depth of applying “FMEA/CILs” occurred. Contractors supported limiting some items to be included in FMEAs, e.g. structures. Also, there was discussion about “ground-ruling out” certain items off the FMEA. The splinter group eventually reached consensus that it was appropriate for an FMEA to be a complete listing of all hardware items with their respective criticality/severity categories enumerated. However, there may be pressure to relax the requirement for completeness, since the CEV redesign increased the projected percentage of “Crit 1 and 2” items from about 40 to 90 percent of their total hardware items. In the main, it is the change to a single string design that increases the percentage of items in an FMEA. Arbitrarily

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 15 of 19	

reducing the number, by limiting or “ground-ruling out” FMEA items, is not consistent with reliable systems design. If some items are to be analyzed by other means or “ground-ruled out”, then those facts should be recorded in the remarks section of the FMEA to so indicate. At the conclusion of the meeting, there was agreement that both FMEAs and Critical Items Lists (CILs) are needed. ***To provide accurate Program risk assessments, CxP SR&QA should maintain FMEA(s) and Critical Items Lists for all items in each subsystem and system.***

4. It was observed that reliability engineering expertise was not initially included as part of the planned FMEA/CIL – Hazard Report “Tiger Team”. That is, the stated resolution team make-up did not call for reliability engineering participation. Risk likelihood (probability) quantification will play an important role in discussing these outstanding Level II issues. FMEA/CILs, Critical Item Evaluations, and Hazard Reports all are performed to support CxP risk assessments and require understanding risk likelihoods (probabilities) and the associated methodologies for deriving them; this can be provided by reliability engineering. A recommendation to include quantitative reliability participation in the Tiger Team was made and acknowledged as appropriate by the splinter group.
5. With multiple teams and suppliers creating FMEAs, Critical Item Evaluations, and Hazards Reports, the task of integrating Program-level risks and the processes of identification/assessment/management will be challenging. FMEAs and Hazard Reports need to be integrated vertically along the supply chain and horizontally across the various FMEA/CIL, Critical Item Evaluation, Hazard Report, and PRA analyses. These analyses need to be consistent among each other and reinforce each other to provide a Programmatic risk profile that assesses and resolves risk drivers using a coordinated approach. ***To more accurately compare and balance risks across the entire Program, CxP SR&QA should ensure that the risk Likelihood and Consequence (also called Impact or Severity) rankings are applied uniformly across all Projects/Elements and sub tier suppliers.***

**Discussion of the Surveillance Splinter Group:
(NESC POCs: Michael D. Smiles, Steve J. Gentz, Stephen A. Minute)**

The results of the Surveillance splinter group session were good, but limited, as the surveillance activity was not fully developed. There is a Level II vision to develop a Surveillance Plan based on a three-prong approach consisting of audits, Government Mandatory Inspection Points (GMIP), and surveillance. Only an incomplete draft of the surveillance prong was presented. The audit and GMIP aspects have not been developed. This splinter group was not able to outbrief Team Zero due to time constraints at Plum Brook, but did present their results at a meeting on July 2, 2008.

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 16 of 19	

Most issues were worked out without a lot of extensive debate. One example of requirements clarifications was the agreement to remove the 24-month vendor audit period. This was replaced with a Level II requirement for the generation of a Level III Project/Element specific vendor audit plan which would identify explicit review periods.

Much of the surveillance process has been under development by a CxP Government Surveillance Working Group. As part of this effort, a NESCS member participated in a CxP Surveillance Strategy meeting at JSC the last week of May 2008, which resulted in the establishment of the CxP Government Surveillance Working Group. The working group is trying to implement the philosophy adopted from the strategy meeting. The CxP Surveillance Government Working Group and associated splinter groups appear to be working towards the development of the proposed Surveillance Plan. The schedule associated with finalizing the Surveillance Plan was not discussed at the Plum Brook meeting, but requires coordination with the CxP SR&QA community to ensure timely and coordinated review and approval.

One concern discussed during the splinter group session was for the Level II requirement to have an electronic closed loop tracking system for GMIP. The CxP has developed a system to record GMIPs and has provided it to the Government personnel performing inspections for evaluation. This developmental system is a database distinctly separate from the contractor build records of the flight hardware and software. The population of this system is envisioned to be a NASA responsibility utilizing Government inspection resources. The inherent risks and costs associated with this concept, including potential contractor costs and risks, may not yet be recognized and could require extensive programmatic trades.

This splinter group session represented the lowest maturity level of the forum topics covered with only the partial development of the proposed Surveillance Plan. The CxP Government Surveillance Working Group appears to recognize the significant challenges necessary to complete this effort.

**Discussion of the Process Control Splinter Group:
(NESCS POCs: Stephen A. Minute, Steven J. Gentz)**

There were two areas of contention for the Process Control splinter group. The splinter group could not converge on the definition of critical process, and there were concerns that the Program was being too prescriptive in requiring PFMEAs for critical processes at the project and contractor level. The splinter group understood and agreed on the intent of the requirement, but disagreed on the stipulation of a specific process to be used. PFMEA is a particular methodology for assessing potential failure points within a process. There are other tools and methods for doing similar assessments. As an example, Statistical Process Control (SPC) is also another best practice manufacturing tool, but like PFMEA should not be imposed. The contractors are already

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 17 of 19	

using variants in their current programs. Re-scoping the requirement to more succinctly capture the “what” is intended, and removing the “how” language is preferred. Allowing tailoring by the Projects would also be valuable.

The splinter group also discussed an apparent attempt in the requirements to augment the “how to” requirement with a threshold of “when to” apply to Level IV processes. This was attempted by the introduction of a CxP 70055 unique definition of “critical” processes. No consensus could be reached due to the diversity of prior program experiences using varying definitions for “special” and “critical” processes.

**Discussion of the Contamination Splinter Group:
(NESC POC: Stephen A. Minute)**

Although the Contamination splinter group was small, there was very good discussion. It was obvious that the majority involved had discussed the issues before this meeting and were already in the process of revising the document with redlines received and agreed to by the splinter group. The splinter group was missing one of the industry partners in the initial splinter group meeting due to conflicting splinter sessions. However, the splinter group was able to tag-up with that team member and resolve the inputs to everyone’s satisfaction.

There were no significant issues. The greatest discussion centered around concerns where requirements were too prescriptive. In particular, requirements to double-bag and seal clean hardware (in clean rooms) and lighting and distance requirements for Visual Clean (VC) inspections. The language was adjusted to allow appropriate flexibility without sacrificing technical intent. Most of the inputs were addressed by clarification of the requirements via notes to better explain intent.

**Discussion of the Hazard Analysis Methodology Splinter Group:
(NESC POC: Nancy J. Currie)**

The Hazard Analysis Methodology splinter group was relatively small with representation from the Program Office, NASA SR&QA organizations supporting Constellation, and Contractor representatives. One of the most significant discussions centered on the relationship between hazard reports and other SR&QA products, especially FMEA/CILs. These discussions have been captured in the Reliability & Maintainability Splinter portion of this report.

Other significant issues that were discussed include level of failure tolerance and definition of design for minimum risk (DFMR), inclusion of descriptions of planned survival methods in hazard reports, and the phasing and timing of safety reviews.

1. **Failure Tolerance:** The current requirement for failure tolerance reads: “The level of failure tolerance should be commensurate with the severity of the hazard and the

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 18 of 19	

likelihood of occurrence.” Most of the discussions of this topic involved the potential ambiguity of this major design requirement. Both NASA SR&QA and contractor systems safety personnel were concerned that the ambiguous wording of the requirement might lead to various interpretations of this requirement by CSERP members and chairpersons. Further, some in attendance interpreted the wording of this requirement to mean that failure tolerance should be increased until the risk is at Low or Very Low. After much discussion and debate, there was no resolution reached and was elevated to a Team Zero discussion.

The Team Zero discussion revolved around the single failure tolerance requirement captured in the CARD. This question misinterprets the intent of the Human Rating Requirements Revision B that stipulates a minimum of 1 failure tolerance. The intent of the Human Rating Requirements was for the Level II team to look at the whole program and have the design team (e.g. Projects and Elements) provide the rationale for why their system is acceptable. The onus is on the design team (e.g. Projects and Elements) and not the Program SR&QA to decide where failure tolerance is necessary. An integrated risk assessment should be done at the Program level. Designers should always design for minimum system risk. A two failure tolerance is just one way of minimizing risk. A complex failure tolerance solution could unintentionally increase risk over a simpler and safer solution.

2. Planned Crew Survival Methods: The initial requirement stated: *“At a minimum, the planned crew survival methods: Abort, Escape, Emergency Egress, Safe Haven, Rescue, Emergency Medical, or None; should be identified, description provided if not evident by the survival method identified, and reference provided to documentation or analysis that validates the availability of the survival method identified.”* The concern expressed with this wording was that the CSERP may interpret this to mean that a detailed description of every instance of crew survival mode must be included in every hazard report, which would require significant labor hours. Following detailed discussion, this requirement was modified to alleviate the requirement to provide a detailed description if the survival method is evident. Further, in cases where crew survival methods are not available, additional scrutiny will be placed on the robustness and reliability of identified hazard controls.

3. Timing of Safety Reviews: The initial requirement stated: *“The Program shall conduct phased system safety and mission success reviews prior to each Project and Program milestone reviews (PDR, CDR, SAR).”* Safety Review Panel personnel participating during Project and Element design reviews, as a concurrent engineering practice, minimizes adverse schedule and cost impacts over the Program’s life cycle. The requirement was modified so that safety and mission success reviews are conducted in parallel with Project and Program milestone reviews. Further, qualifiers were added to

	NASA Engineering and Safety Center Report	Document #: RP-08-86	Version: 1.0
Title: Review of the Constellation Level II SR&QA Requirements Documents during Participation in the Constellation Level II SR&QA Forum		Page #: 19 of 19	

state that holding the phased safety review during or after the Projects and Elements milestone reviews may create some additional schedule and cost risks to the Program.

Lesson Learned: Effectiveness and efficiency of the entire safety review process can be enhanced by maintaining consistency in Safety Review Panels' approach and stability in their membership. This allows expectations to be understood by the design teams and allows the Panels' technical knowledge to mature along with the design maturity.

**Discussion of the Probabilistic Risk Assessment (PRA) Splinter Group:
(NESC POC: Nancy J. Currie)**

The CxP assembled a Probabilistic Risk Management splinter group that includes experts with significant prior experience in Program-level risk management and PRA. The group is leveraging lessons learned from prior human spaceflight programs while also advancing and improving PRA methodologies and practices. The CxP appears to have a sound and reasonable approach to development, configuration management, and implementation of PRA across all Program elements. This will greatly assist the CxP and Project Managers in determining their risk posture throughout the Program's life cycle. In general, there was concurrence on the methodology, process, and requirements associated with PRA. Comments withdrawn did not reflect technical content or methodology issues, but rather internal Orion Project management and roles/responsibilities between NASA and the contractor community.