Engineering and Safety Partnership Enhances Safety of the Space Shuttle Program (SSP)

Alberto Duarte
National Aeronautics And Space Administration (NASA)
Marshall Space Flight Center (MSFC)
Engineering Directorate
Marshall Safety and Engineering Review Panel
Co-Chair
Alberto.duarte@nasa.gov

ABSTRACT

Project Management must use the risk assessment documents (RADs) as tools to support their decision-making process. Therefore, these documents have to be initiated, developed, and evolved parallel to the life of the project. Technical preparation and safety compliance of these documents require a great deal of resources. Updating these documents after-the-fact not only requires substantial increase in resources – Project Cost –, but this task is also not useful and perhaps an unnecessary expense. Hazard Reports (HRs), Failure Modes and Effects Analysis (FMEAs), Critical Item Lists (CILs), Risk Management process are, among others, within this category.

A positive action resulting from a strong partnership between interested parties is one way to get these documents and related processes and requirements, released and updated in useful time. The Space Shuttle Program (SSP) at the Marshall Space Flight Center has implemented a process which is having positive results and gaining acceptance within the Agency. A hybrid Panel, with equal interest and responsibilities for the two larger organizations, Safety and Engineering, is the focal point of this process. Called the Marshall Safety and Engineering Review Panel (MSERP), its charter (Space Shuttle Program Directive 110F, April 15, 2005), and its Operating Control Plan emphasizes the technical and safety responsibilities over the program risk documents: HRs; FMEA/CILs; Engineering Changes; anomalies/problem resolutions and corrective action implementations, and trend analysis. The MSERP has undertaken its responsibilities with objectivity, assertiveness, dedication, has operated with focus, and has shown significant results and promising perspectives. The MSERP has been deeply involved in propulsion systems and integration, real time technical issues and other relevant reviews, since its conception. These activities have transformed the propulsion MSERP in a truly participative and value added panel, making a difference for the safety of the Space Shuttle Vehicle, its crew, and personnel. Because of the MSERP's valuable contribution to the assessment of safety risk for the SSP, this paper also proposes an enhanced Panel concept that takes this successful partnership concept to a higher level of 'true partnership'. The proposed panel is aimed to be responsible for the review and assessment of all risk relative to Safety for new and future aerospace and related programs.

1.0 INTRODUCTION

Safety related risk assessment tools and documents have been developed and proposed to assist the project manager in the decision-making process. However, due to several circumstances, some projects opt not to use them in managing the project or to develop them at a later date after-the-fact or simply to ignore them. Preparation and compliance with technical and safety standards and requirements sometimes require significant resources. Updating of documents after-the-fact not only requires a substantial increase in resources - seizing manpower from

engineering disciplines doing other activities, hiring contractors, longer and more elaborated reviewing, approval processing, etc. – impacting directly the already tight Project Cost, but it is also not useful and perhaps is an unnecessary expense.

2.0 RISK ASSESSMENT DOCUMENTS

For the purpose of this paper and without undermining any other process or document, Project 'risk assessment documents' (RADs) include:

- Risk management program (RMP).
- Failure Modes and Effect Analysis (FMEA).
- Critical Items List (CIL).
- Hazard Reports (HRs).
- Hardware and Software Discrepancies Reports.

There are few good references to intelligently help in preparing each one of these documents. There are also few good techniques and many deviations and interpretations. There are several computer software aids available for each RAD as well. The purpose of this paper is not to derive a new or innovative technique or method. However, in this regard, it is the intent in this section of the paper to identify and emphasize those key points which, through the years, have been found definitely of relevance and significance while processing these RADs.

2.1. Risk Management

- Prepare with your projects the risk management plan of the project.
- Identify a 'recovery path' for each risk, with specific milestones, off ramps and contingency plans. Use any technique like cascade schedule, etc. Update it monthly, at least, and use it. Manage your projects with it.

2.2. Failure Modes and Effect Analysis

- Use a logic methodology supported by the corresponding system/subsystem design team.
- Define with details a failure mode and its effects. The use of generalized terminology, 'contamination', 'Manufacturing defects', etc, do not provide the thoroughness of the analysis and allow for specific activities within the processes and operations to be overlooked.

2.3. Critical Items List

- Derive the CIL from the FMEA or similar analysis. Do not use 'precious experiences' or brainstorming for identification of causes to be part of the CIL.
- In the retention rationale, provide controls for each requirement and verification methods for each control.

2.4. Hazard Reports

- Start with the Fault Tree Analysis (FTA). Identify the highest potential catastrophic event for all your projects within a Program, and always develop from there down to the level where the controls are applied.
- Define at which level your FTA stops and provide for each cause, requirements, controls and verification methods. For each control, provide corresponding verification methods (analysis, test, inspection) with the corresponding acceptable reference.

2.5. RADs MUST HAVE:

- Consistency: same guidelines to all contractors. Same philosophy, same level of detail. The product may not be the same, but your directions and technical depth ness will be consistent.
- Enforce them. Assign a responsible individual at the level required i.e.: one person for HR; or one person for the whole FMEA; or a team for the RMP of a projects, etc.

• Make RADs deliveries on time. Update them as the project matures in such a way that they become relevant tools in the decision-making process.
• RADs are tools to be used in a daily basis by management (program management; project management; line organizations).
• RADs must be the responsibility of the Project itself, although preparation and implementation is the responsibility of the project through the line organizations and the Chief Engineers or System Engineers. Therefore, it is of a mutual interest to have RADs identified, developed and reviewed with the milestone of the project {System Requirements Review (SRR), Preliminary Design Review (PDR), Critical Design Review (CDR), etc}. An independent entity with adequate supporting background and knowledge should be assigned to assess, monitor and disposition RADs, shoulder to shoulder with the progress of the project. An independent Panel of experts is the right approach, as long as the Panel operates through the duration of the project, from conception to closure or disposal. Assessment of RADs after-the-fact is not as useful. In addition, these later assessments usually require a larger amount of resources than if they had been developed and reviewed with the progress of the project.

3.0. SAFETY PANEL

3.1. Background

Now, relative to the assessment of safety risk, let's look at history and specifically talk about the Space Shuttle Program (SSP). Since early stages, efforts have been made to maintain and establish an official Senior Panel: *"... A Senior Safety Board as a mechanism to periodic review of system and element level hazard resolution activities and for providing management visibility of open and accepted risk hazards"* (January 15, 1981) [1]. At that time, the charter was prepared for a centralized Board, assigning the Board activities under the responsibility of the Johnson Space Center (JSC) Director of Safety Reliability and quality assurance and charter to concentrate its efforts in the review of Space Shuttle Integration, cargo Integration, and Element-level open hazards, and establish actions for hazard resolution, and review and approve of hazard closure rationale. In addition, it was defined as part of the policy that each one of the Board members was responsible for identifying hazards to the Board for their areas of responsibility.
In the following years the charter of the Board was confirmed with minor modifications, such as, addition of interaction and participation of other Agencies (i.e.: Air Force) [2], [3], [4].
After the Challenger accident on January 28, 1986, the National Space Transportation System Safety Review Panel (SSRP) was then established on December 08, 1988. [5], *"...as a mechanism of enhancing the Space Transportation System Safety Management and Engineering through informational interchanges, development of concepts to improve the STS Safety Program, review of safety documentation, review of STS integration and cargo integration, review of STS element-level hazard identification and resolution activities, and recommendations to level II management for Hazards report disposition."* Later (February 2, 2000), in an effort to cover more ground relative to the SSP Safety Risk products, the scope of the SSRP was stretched: *"This scope includes all Space Shuttle flight and ground processing Hazards and critical failure modes that can affect program Safety risk and have criticality 1, 1S, 1R, 2, 2R impact on the Space Shuttle including government furnished equipment."* [6].
Although the intent was right, now including the CILs and the ground and processing equipment and operations, it was resource and time intensive. In addition, at this time the SSRP was chartered to *"...establish and execute risk management techniques to provide identification and*

resolution of potential program risks... " [6], which require additional concentration, dedication and research of individual design, manufacturing, testing, and operations and processes at each Center. Certainly, to properly review Hazard Reports plus CILs plus coming up with innovative risk management strategies and policies for the SSP, more than the SSRP was required. The scope, as defined in the charter, was intentionally right but perhaps too ambitious for the resources allocated.

3.2. Safety Engineering Review Panel (SERP)

Post-Columbia evaluations of Shuttle Program [7} concluded that the existing SSRP function/operation was deficient in providing Program Management with proper insight into program risk. Subsequently, Shuttle Program S&MA Office concluded the following: 1. The Safety Panel should become as proactive as possible without losing independence. 2. Program/project managers must accept all risk. 3. Decrease scope to increase involvement in project decision-making. 4. Engineering should actively participate in the Safety Review Process.

In order to make the Safety Panel more effective and focused, the SSP approved the establishment of the Safety Engineering Review Panel (SERP) [8], on April 15, 2005, in lieu of the SSRP. The SERP, really, is an organization of Panels structured as the SSP is (see Fig. 1). One Panel at each Space Center (JSC, KSC, and MSFC), which constitutes the Level 3 and one management Panel at the Level 2. In addition, an Integration Safety Engineering Review Panel (ISERP) resides at the Level 2 and is responsible for the review of integrated HRs and serves to technically integrate safety products across the program elements.

It was intended to have the SERP as an independent advisor to program and project management for the acceptance of risk. Now its scope emphasizes in reviewing and approving SSP Hazard Reports (HRs) and Critical Item Lists (CILs) based on adequacy of safety analysis, compliance to program requirements, and assessment of risk, of each element or operations by a Center. In addition, a few more tasks were added to the scope which now reaches to perform the assessment of risk to support the project milestones (SRR, PRR, CDR, etc), the assessment of engineering and project changes that may affect HRs and CILs, and 'Problem Report and Corrective Action' (PRACA) having associated criticality of 1 and 1R.

3.3. The Marshall SERP

At the MSFC the SERP concept was very well adopted and immediately implemented. The scope and responsibilities were summarized in a flow diagram (see Fig. 2), to be applied to the MSFC Shuttle Propulsion Elements: External Tank (ET), Redesigned Solid Rocket Motor (RSRM), Solid Rocket Booster (SRB), and Space Shuttle Main Engine (SSME). An innovative approach was taken to enhance the ED participation in the MSERP. The two line organizations ED and S&MA agreed upon the approach giving ED additional participation in the Panel. First of all, the Panel is titled, 'Marshall Safety AND Engineering Review Panel'. Notice the sense of partnership and the level of responsibility bringing the two organizations together in one entity. The ED Senior Rep is the Focal point for engineering needs and he/she is given the title of Co-Chair, having the MSERP Chair from within S&MA, since the Panel directly responds to S&MA upper management. The ED Senior rep is responsible for managing the ED participation and technical expertise required to adequately support the Panel review meetings, technical interchange meetings (TIMs), and safety issue briefing reviews. Also, ED is committed to provide professional expertise required to support MSERP meetings with the Projects and Prime

System Safety Review Panel Charter

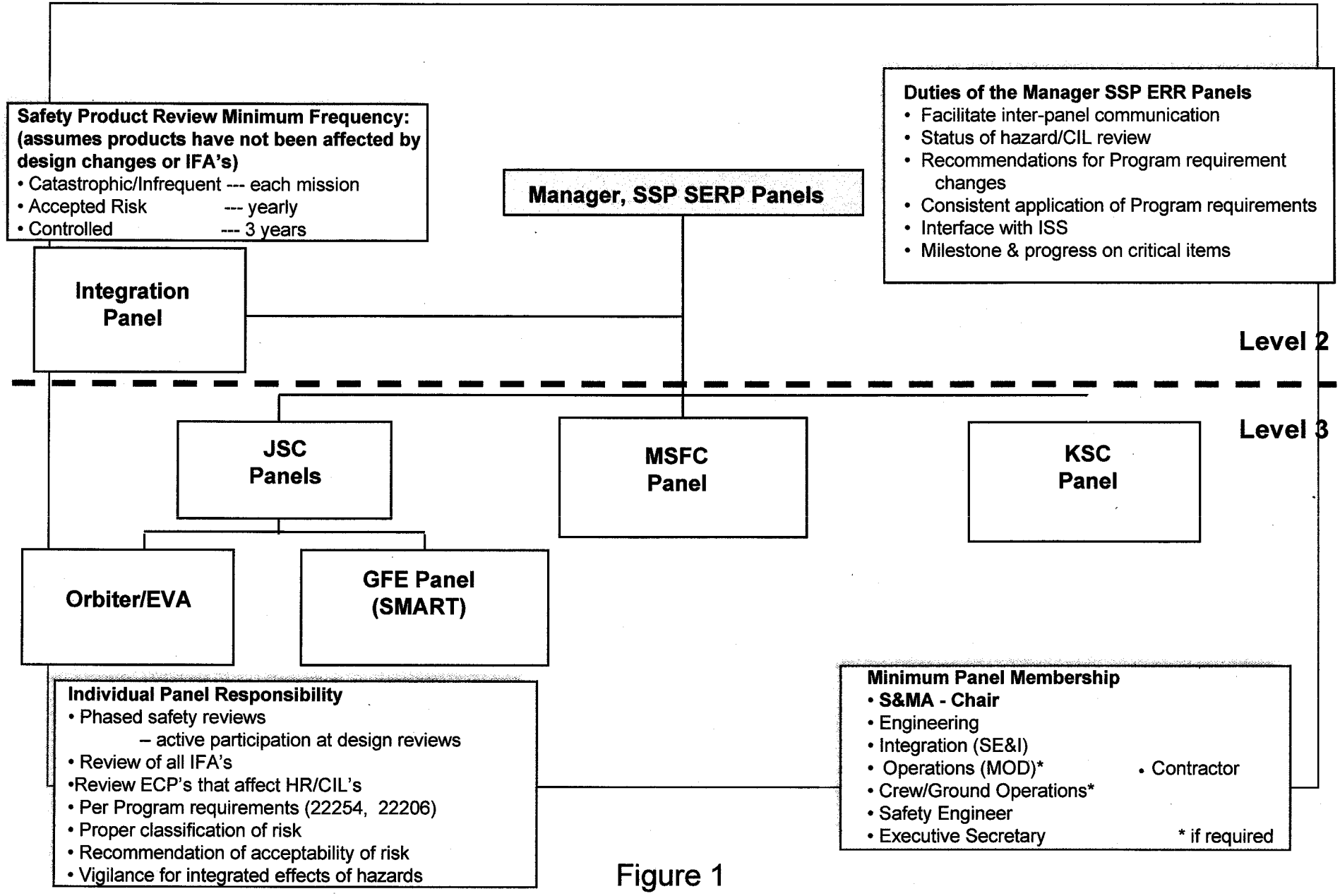

Figure 1

SERP Marshall Implementation

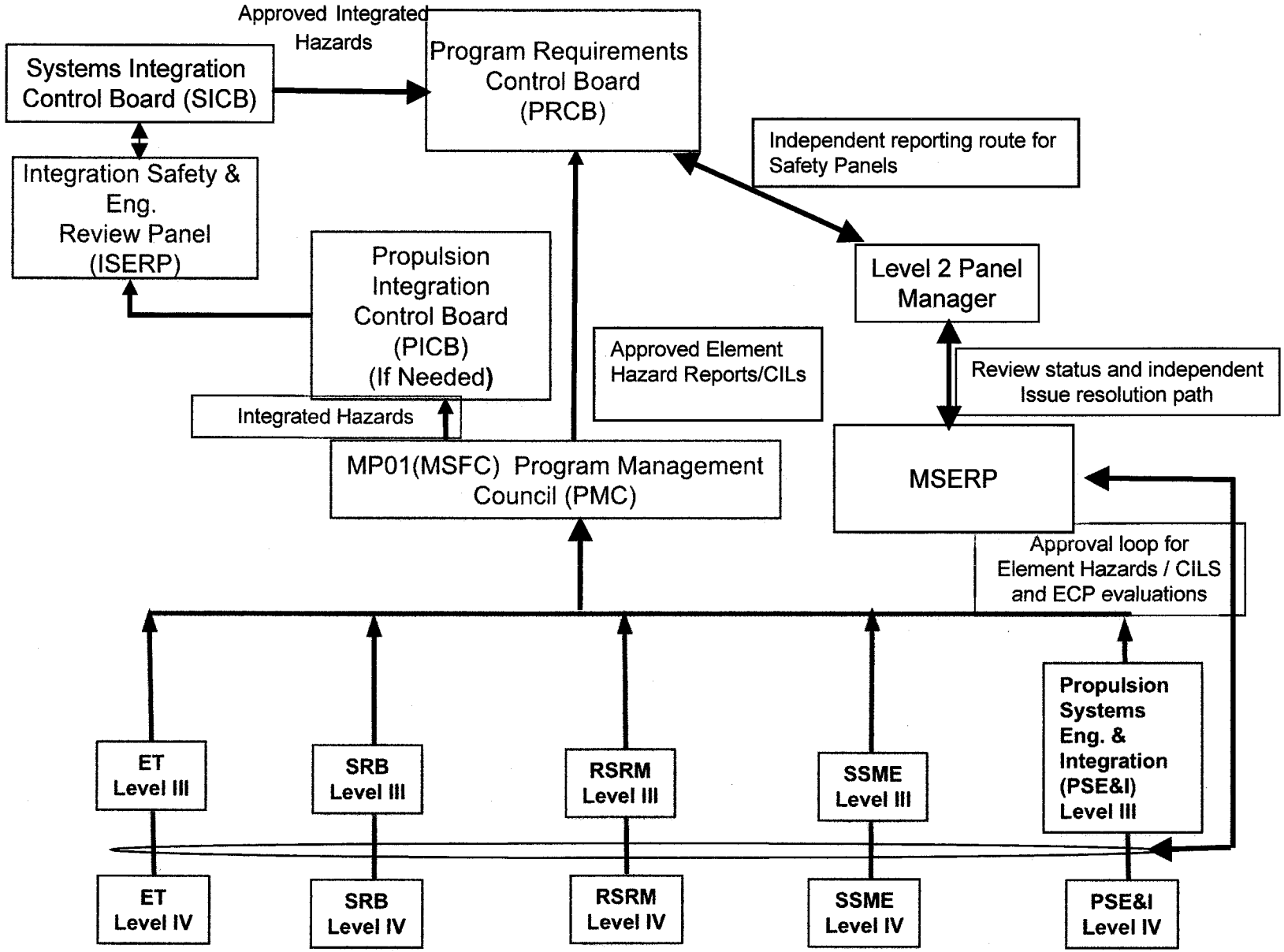

Figure 2

contractors, and any other MSERP activity, as required. ED has agreed to assign ED responsible individuals for the HRs and CILs for each Propulsion Element. The Element Chief Engineers have taken this responsibility. The MSERP has shown, since the SERP implementation, stronger participation in risk assessment and more in-depth analysis and accomplishment of the charter tasks. Its organization and structure has allowed it to penetrate into the current issues and also update those activities that were behind, as far as risk assessment is concerned. MSERP has adopted a database within the MSFC Process Base Mission Assurance (PBMA) system where schedules, meeting minutes, technical and other support presentations, action items and agreements, and closures are stored and available. Any additional MSERP statistical information is stored and available in PBMA and as well as the current issues of required documents (standards, Spec's, requirements, etc.).

In order to dedicate adequate time with all Propulsion Elements, the MSERP schedules monthly meetings, ahead of time, with each one of them. Additional meetings are available as requested. Also, face-to-face meetings at the Contractor's site are held at least once a year. Continuous formal or informal communication is encouraged between the MSERP members and all parties involved in the risk assessment process. Once a week the MSERP meets to review internal matters, establish priorities, and set strategies.

3.3.1. MSERP Membership

PRIMARY PANEL MEMBERS:

Chairperson – from MSFC S&MA
Engineering Directorate Rep – from ED MSFC
Executive Secretary – from MSFC S&MA
Integration Rep – from MSFC S&MA
PSE&I Rep – from MSFC
Astronaut Office
Mission Ops from JSC (as needed)

ADVISORY PANEL MEMBERS:

Project Office Representative
Project/element S&MA Representative
Prime Contractors
KSC Launch/Landing Project Office (as needed)
Reliability/Maintainability for CIL reviews

4.0 PROPOSED PANEL

4.1. The MSERP has accomplished successful goals and achievements and its performance will continue improving towards stronger contribution to the Space Shuttle safety and mission success.

One step forward – beyond those already made by the MSERP – is proposed in this paper to be considered for future and relatively new aerospace and related programs and projects.

The same team that has the background and the trained expertise in this matter must assess any safety concern, issue or risk. With the right team, the right structure, and the required level of expertise, the proposed Panel must be able to accommodate any safety risk assessment within the project. In addition, it would be an independent expert assessment to the benefit of the project manager, as well. This Panel must assure on-time delivery of those RADs and other engineering and project changes, PRACA items, risk management progress, etc., to adequately support the project milestones.

On the other hand, since the risk associated with safety has origins and roots at any point during the life of the project - concept, design, manufacturing, test, operations and flight, recovery, etc. – it is proposed that the safety panel be a true partnership between those organizations involved in the process. Since in some projects there are numerous organizations to be represented in a workable Panel, just select the most significant (three or so) to be represented as members of the Panel. However, when

the term 'true partnership' is used, it means: same level of responsibility and accountability, same level of authority, same level of representation and support, and same level of rights and prerogatives. A true partnership and an independent entity do not have to have ownership in one single organization: it has to be equally and strongly supported by those key organizations that are participating in the safety review process. Sure, it has to be a Chair and a Co-Chair, and it has to operate as a Panel. However, they do not have to be from within S&MA necessarily. Furthermore, as an independent entity it must have its own budget, funded by the Program and it can have dotted line responsibilities to those organizations (ED, S&MA, Operations, etc) that equally support the Panel. Also, there will be in the Panel some representatives supporting only certain tasks, not as permanent members.

4.2. It is desirable and perhaps advantageous that, from the start to the end of a task or project, safety risk associated with its design, manufacturing, test, flight, etc., of a sub-system, system, etc. be assessed by the same entity of risk experts - same entity does not necessarily means same individuals. It provides consistency, continuity, and better utilization of the expertise gained through the process. Furthermore, while tasks required to control or eliminate risk are performed by individuals from the engineering, safety, operations or science organizations, the analysis and assessment of safety risk is preferable to be a joined effort of experts who have gained knowledge of the system and acquired expertise, working as an entity. The risk coming from the project risk management process has to be handled with the same philosophy and similar strategy than any other safety risk. So when safety risk is at stake, it must be understood that it is intended to be relevant to any safety risk originated from any source. So, the safety risk associated with the HRs, CILs, Engineering and project changes, and PRACA items, and that risk associated with the risk management process of a project and any other source, must be treated equally and reviewed and assessed by the same Panel.
For all of the above, while the scope of the SERP is well accepted, it is proposed to create a Panel whose scope includes not only the SERP's but also the task of assessing all safety risks including those from the risk management process of the project and any other source. It will also allow for consistency in safety risk analysis, disposition of risks and risk ranking.

5.0. Conclusions

5.1. RADs must be implemented at the early stages (rather than at the beginning) of a project and must be used as tools in management decision-making. Otherwise, it is advised to utilize those allocated resources in other relevant project activities.

5.2. It is advisable that the safety risk within a project be assessed and reviewed by an independent entity or Panel.

5.3. The MSERP believes in its objective and has undertaken its charter with professionalism, commitment, and accountability.

5.4. The 'True partnership' Panel concept can be applied to any specific task within the project, not solely to Safety risk assessment.

6.0 Recommendations

6.1. The SERP concept for the SSP was a step in the right direction, as far as management of safety risk. This concept must be considered for relatively new and future aerospace and related programs.

6. 2. A well structured 'True Partnership' Safety Panel has been proposed to enhance the performance, responsibility, and accountability of the key organizations participating in the assessment of the project risk associated with safety.

6.3. This Panel shall assess and review safety risk coming from related processes, documents (RADs), and project changes.

6.4. A 'True partnership Safety Panel', as an independent entity, must be equally supported by the key organizations represented. Those organizations have same level of responsibility and accountability as the Panel itself.

6.5. The 'True Partnership Panel' must respond to the key organizations represented in the Panel and at the same level of management. It must also have its own budget funded by the Program.

7.0. REFERENCES

1. *JSC SPACE SHUTTLE PROGRAM DIRECTIVE. SSPM DIRECTIVE NO. 110, January 5, 1981. JSC form 1310 (May 1973), NASA – JSC, CHANGE NO. 46*

2. *JSC SPACE SHUTTLE PROGRAM DIRECTIVE. SSPM DIRECTIVE NO. 110A, September 14, 1981. JSC Form 1310 (Mar 1973), CHANGE NO. 51*

3. *SPACE SHUTTLE PROGRAM DIRECTIVE SSP DIRECTIVE NO. 110B, September 14, 1982. JSC form 1310 (May 1973), NASA – JSC, CHANGE NO. 57*

4. *NATIONAL SPACE TRANSPORTATION SYSTEM DIRECTIVE. NSTS DIRECTIVE NO. 110C, August 13, 1984.*

5 *NATIONAL SPACE TRANSPORTATION SYSTEM DIRECTIVE. NSTS DIRECTIVE NO. 110C, December 08, 1988.*

6. *SPACE SHUTTLE PROGRAM DIRECTIVE SSP DIRECTIVE NO. 110E, February 02, 2000, Volume II, Book 2, Revision D CHANGE NO. 158*

7. *COLUMBIA ACCIDENT INVESTIGATION BOARD, Report Volume 1, August 2003*

8. *SPACE SHUTTLE PROGRAM DIRECTIVE SSP DIRECTIVE NO. 110F, April 15, 2005, Volume II – Book 2, Revision D CHANGE NO. 184*