

MWI 1700.2

REVISION B

EFFECTIVE DATE: June 7, 2004

EXPIRATION DATE: June 7, 2009

MARSHALL WORK INSTRUCTION

QD01

SYSTEM SAFETY PROGRAM

CHECK THE MASTER LIST at
<https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

| | | |
|---|---------------------------|---------------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 2 of 10 |

DOCUMENT HISTORY LOG

| Status (Baseline/ Revision/ Canceled) | Document Revision | Effective Date | Description |
|--|----------------------|-------------------|---|
| Baseline | | 12/13/99 | |
| Revision | A | 3/26/01 | Revised to replace NHB 1700.1 (1V-B) with NPG 8715.3. Added Reference 4.1. Renumbered the sections to format specified in MPG 1410.2. Spelled out acronym for ISS in section 6.4. |
| Revision | B | 6/7/2004 | Revised to omit references to Payload Safety Readiness Review Board and related MWI 1700.1. Several paragraphs added to the Instructions Section to better identify functions and processes. Changed "NPG" to "NPR" throughout the document. Added NPD 8070.6 to the Applicable Documents list. |

CHECK THE MASTER LIST at <https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

| | | |
|--|--------------------|--------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 3 of 10 |

1. PURPOSE

This Instruction defines the essential elements of a System Safety Program at Marshall Space Flight Center (MSFC) for implementing the requirements in Chapter 3 of NPR 8715.3 and additional functions deemed key to successful System Safety Programs.

2. APPLICABILITY

This Directive defines MSFC system safety functions and is applicable to all organizational levels within the Center, including on-site and off-site contractors. MSFC system safety is concerned with the safety aspects of aerospace flight and flight demonstration systems, related support and test equipment/facilities, computer software, and personnel during research, development, design, integration, test, flight, post-landing, recovery, and refurbishment whether for manned or unmanned systems. System Safety is to be emphasized throughout the life cycle of program flight systems, from inception until project completion, and includes an evaluation of all identified hazards.

3. APPLICABLE DOCUMENTS

- 3.1 NPR 8715.3, "NASA Safety Manual"
- 3.2 MWI 7120.6, "Program/Project Risk Management"
- 3.3 NPD 8710.3, "NASA Policy for Limiting Orbital Debris Generation"
- 3.4 NPD 8070.6B, "Technical Standards"
- 3.5 NASA FAR Supplement (NFS), Subpart 1823.70
- 3.6 MWI 8050.1, "Verification of Hardware, Software, and Ground Support Equipment for MSFC Projects"

4. REFERENCES

- 4.1 QD10-SS-011, "Procedures for Performing Hazard Analysis"
- 4.2 NASA Safety and Engineering Center Charter, August 1, 2003

CHECK THE MASTER LIST at <https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

| | | |
|-----------------------------------|--------------------|--------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 4 of 10 |

5. DEFINITIONS

5.1 Hazard. Existing or potential condition that can result in or contribute to a mishap.

5.2 Safety Analysis. Generic term for a family of analyses, which includes but is not limited to: preliminary hazard analysis, system hazard analysis, operating hazard analysis, software hazard analysis, fault tree, sneak circuit, and other safety assessment tools.

5.3 Safety Risk. The combination of (1) the probability (qualitative or quantitative) that a program or project will experience an undesired event that impacts program safety requirements (for example, preservation of life and program physical resources) and (2) severity of the undesired event were it to occur.

5.4 System Safety. Application of engineering and management principles, criteria, and techniques to optimize safety and reduce risks with the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle.

5.5 System Safety Plan. A document that describes the safety assurance tasks and products to be implemented throughout a program/project or contract, including methods of approach, safety milestones, and assigned responsibilities for fulfilling these tasks.

6. INSTRUCTIONS

6.1 Introduction: The following activities will be conducted to ensure that system safety risks are identified and reduced to an acceptable level.

6.2 System Safety Planning: System safety planning details the activities of system safety management and system safety engineering which constitute the system safety program for a subject program or activity. System Safety program planning shall be implemented at the program level with supporting sub-tier documentation for any associated contractor efforts.

6.2.1 Program System Safety Plans (PSSP) - The program SSP shall describe the total system safety effort including all

CHECK THE MASTER LIST at <https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

| | | |
|-----------------------------------|--------------------|--------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 5 of 10 |

system safety related roles and responsibilities. The plan will include detailed task implementations based on the requirements of this document and related reference documents. Any specific tailoring and/or modifications will be identified in the Program System Safety Plan. The program organization and related system safety relationships and responsibilities will be described along with reporting and review functions for the subject program. In addition, the plan will describe how MSFC S&MA system safety elements will conduct their independent assessment role. Methods for the definition, tracking and resolution of potential safety risk issues shall be identified. PSSP should also provide for interfacing with the NASA Engineering and Safety Center and the Center Independent Technical Authority for the identification and performance of independent engineering and safety assessments.

6.2.2 Contractor System Safety Plan Content: Contractor effort for a subject program will be defined by a contractor system safety plan which will detail how the contractor will implement and comply with the project system safety requirements and safety tasks defined in the contract. System safety requirements can be levied by a Request for Proposal, Announcement of Opportunity, Cooperative Agreement Notice, NASA Research Announcement, or other proposal request. As a minimum, the contractor system safety plan will identify responsibilities, implementation methods, products and program milestone activities. Appendix I of NPR 8715.3 provides recommended formats and an outline for safety plan content which may be tailored according to provisions in the PSSP.

6.3 System Safety Provisions: System Safety shall be a considered in all programmatic and technical activities at MSFC. Program involvement shall include as minimum the following activities.

6.3.1 Program Roles

6.3.1.1 Program Management: The program manager is ultimately responsible for the safety of the program. The program system safety organization (government and contractor) is responsible for providing the best possible analysis and related information to support safety risk decisions. In addition to the direct program support role, elements of the MSFC S&MA organization will provide independent assessments of the subject program as

| | | |
|-----------------------------------|--------------------|--------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 6 of 10 |

part of a system of checks and balances to assure that potential safety issues are being properly addressed.

6.3.1.2 Program Reviews: System safety shall be actively considered during all major program reviews including milestone reviews during the development phases and readiness or operational reviews during the operational phase. System safety products will be evaluated and representatives of the assigned S&MA organization will participate in the reviews.

6.3.1.3 Risk Management: The program system safety organization (government and contractor) will be an important part of the respective program continuous risk management processes. The system safety organization will provide supporting hazard analyses and other safety risk assessments and will participate in the program risk management process.

6.3.1.4 Change Review: In the course of any program, systems are changed to enhance capabilities and to provide more efficient operation. With each change, the original safety aspects could be impacted, resulting in either increased or reduced safety risk. Each proposed change will be subjected to a safety evaluation to include specific and systemic impacts. The system safety analysis will be updated when required to show any risk changes.

6.3.1.5 Problem Identification and Resolution: The program system safety organization (government and contractor) will participate in the subject program's problem identification and resolution process. System safety assessments will also be made of any accidents or incidents involving flight hardware to assure that functions or features that serve as hazard controls have not been compromised.

6.3.1.6 Procurement: Procurement for design, development, fabrication, test or operations of systems, equipment, and facilities shall include appropriate system safety requirements as specified in NASA FAR Supplement, Subpart 1823.70. System safety tasks shall be specific so potential bidders can understand the requirements. The Safety and Mission Assurance organization will participate in the development of the system safety tasks, provide safety inputs to the Source Evaluation Board and to Performance Evaluation Boards, and conduct independent assessments of the contract system safety deliverables.

**CHECK THE MASTER LIST at <https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE**

| | | |
|-----------------------------------|--------------------|--------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 7 of 10 |

6.3.2 S&MA Relationships: The system safety program will provide for the exchange of system safety information and identify areas of mutual support within the Safety, Reliability, Maintainability and Quality Assurance (SRM&QA) elements of the Safety and Mission Assurance Directorate. System safety is dependent on reliability analyses including Failure Modes and Effects Analysis (FMEA) and Probability Risk Analysis (PRA) assessments to aid in the identification of hazard causes and safety risk evaluation. The quality program assures that hardware is built to print and processes are done per approved procedures which assures hazard controls are in place.

6.3.3 Engineering and Technical Interfaces: There must be a close working relationship between the engineering and the system safety organizations with a continuous exchange of information during the life cycle of a program. The organizations will jointly assess proposed program technical standards that relate to system safety requirements to assure compliance with NASA policy on Technical Standards and applicable Agency system safety requirements. NASA NPD 8070.6B provides the NASA Technical Standards policy. To be most effective, the System Safety effort should function as an active participant on the design development and implementation teams working to prevent issues and concerns and not be in a "reaction" mode of identifying design issues and concerns only at program milestone reviews.

6.4 System Safety Products

6.4.1 System Safety Analysis: System safety analysis provides a means of systematically and objectively identifying hazards and determining their risk levels. System safety analysis also provides the mechanism for documenting hazard elimination or control. Safety analysis methods may include system hazard analysis, fault tree analysis, sneak circuit, or other analysis methods that may be beneficial to hazard elimination or reduction process. The flight or development systems program typically defines the format of the analysis, the analysis methods, and the required life cycle reevaluation, which should be documented in the program system safety plan.

The system safety engineer should make full use of related risk assessment tools (FTA, FMEA, PRA, etc.), when he/she is performing the safety analysis. As noted in "Verification of

**CHECK THE MASTER LIST at <https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE**

| | | |
|--|--------------------|--------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 8 of 10 |

Hardware, Software, and Ground Support Equipment for MSFC Projects" (MWI 8050.1), identified hazard controls and control verification items will be submitted to the program verification plan to assure traceability and implementation.

For flight systems that have the potential to create orbital debris, an orbital debris analysis will need to be developed that meets the requirements of NPD 8710.3, "NASA Policy for Limiting Orbital Debris Generation." Further information on safety and hazard analysis techniques is provided in NPR 8715.3 and QD10-SS-011.

6.5 System Safety Program Reviews: System safety reviews will be conducted by the program or project as required by the level one or two organizations that are being supported. The purpose of these reviews is to evaluate the status of hazard analysis, hazard controls, verification techniques and program implementation.

7. NOTES

None

8. SAFETY PRECAUTIONS AND WARNING NOTES

None

9. RECORDS

The program or project office maintains the following records:

9.1 System Safety Plan

9.2 System Safety Analysis

Documentation shall be maintained throughout the life of the project and for a period of not less than 5 years following payload launch and 6 years after the launch of the final item of a series.

10. PERSONNEL TRAINING AND CERTIFICATION

None

11. FLOW DIAGRAM

CHECK THE MASTER LIST at <https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE

| | | |
|--|--------------------|--------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 9 of 10 |

A generalized depiction of the relation of the system safety program effort to the typical design, development and operational program phases is provided in Attachment 1. The system safety effort should be a part of the different cycles within the program evolutionary flow from program initiation to program operations.

12. CANCELLATION

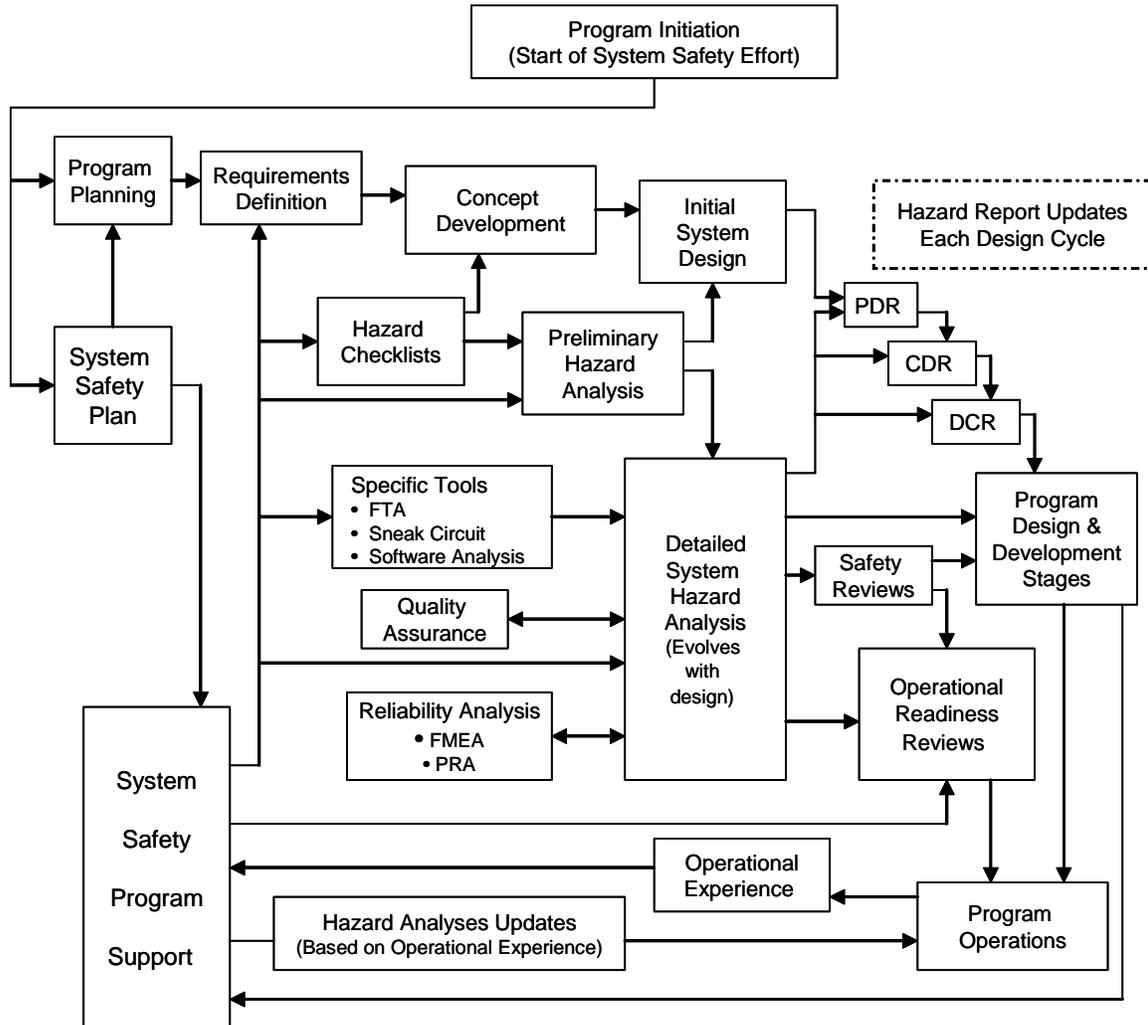
MWI 1700.2A dated March 26, 2001

Original signed by
Axel Roth for

David A. King
Director

| | | |
|-----------------------------------|--------------------|---------------|
| Marshall Work Instruction QD01 | | |
| System Safety Program | MWI 1700.2 | Revision: B |
| | Date: June 7, 2004 | Page 10 of 10 |

Attachment 1 System Safety Plan Flow Chart



CHECK THE MASTER LIST at <https://repository.msfc.nasa.gov/directives/directives.htm>
VERIFY THAT THIS IS THE CORRECT VERSION BEFORE USE