

Approved: 2020-06-10

**Measurement System Identification:  
Not Measurement Sensitive**



**NASA TECHNICAL STANDARD**

**National Aeronautics and Space Administration**

**NASA-STD-8739.8A**

**Approved: 2020-06-10  
Superseding NASA-STD-8739.8  
With Change 1**

**SOFTWARE ASSURANCE AND SOFTWARE SAFETY STANDARD**

**APPROVED FOR PUBLIC RELEASE – DISTRIBUTION IS UNLIMITED**

**DOCUMENT HISTORY LOG**

<b>Status</b>	<b>Document Revision</b>	<b>Approval Date</b>	<b>Description</b>
Baseline	Initial	2004-07-28	Initial Release
	1	2005-05-05	Administrative changes to the Preface; Paragraphs 1.1, 1.4, 1.5, 2.1.1, 2.2.2, 3, 5.1.2.3, 5.4.1.1; 5.6.2, 5.8.1.2, 6.7.1.a, 7.3.2, 7.3.3, 7.5, 7.5.1; Table 1; Appendix A; Appendix C to reflect NASA Transformation changes, reflect the release of NASA Procedural Requirements (NPR) 7150.2, NASA Software Engineering Requirements and to make minor editorial changes. Note: Some paragraphs have changed pages as a result of these changes. Only pages where content has changed are identified by change indications.
	A	2020-06-10	The revised document addresses the following significant issues: combined the NASA Software Assurance Standard (NASA-STD-8739.8) with the NASA Software Safety Standard (NASA-STD-8719.13), reduction of requirements, bring into alignment with updates to NPR 7150.2, added a section on IV&V requirements to perform IV&V, and moved guidance text to an Electronic Handbook. This change combines the updates to NASA-STD-8739.8 and the content of NASA-STD-8719.13. The update includes the NASA software safety requirements and cancels NASA-STD-8719.13 standard.

**FOREWORD**

This NASA Technical Standard is published by the National Aeronautics and Space Administration (NASA) to provide uniform engineering and technical requirements for processes, procedures, practices, and methods that have been endorsed as standard for NASA facilities, programs, and projects, including requirements for selection, application, and design criteria of an item.

This standard was developed by the NASA Office of Safety and Mission Assurance (OSMA). Requests for information, corrections, or additions to this standard should be submitted to the OSMA by email to [Agency-SMA-Policy-Feedback@mail.nasa.gov](mailto:Agency-SMA-Policy-Feedback@mail.nasa.gov) or via the “Email Feedback” link at <https://standards.nasa.gov>.



F. Groen for T. Wilcutt

---

Terrence W. Wilcutt  
NASA Chief, Safety and Mission Assurance

June 10, 2020

---

Approval Date

**TABLE OF CONTENTS**

**DOCUMENT HISTORY LOG ..... 2**  
**FOREWORD..... 3**  
**TABLE OF CONTENTS ..... 4**  
**LIST OF APPENDICES ..... 4**  
**LIST OF TABLES ..... 4**

**1. SCOPE ..... 5**  
1.1 Document Purpose ..... 5  
1.2 Applicability ..... 6  
1.3 Documentation and Deliverables ..... 6  
1.4 Request for Relief ..... 6

**2. APPLICABLE AND REFERENCE DOCUMENTS ..... 6**  
2.1 Applicable Documents ..... 6  
2.2 Reference Documents ..... 7  
2.3 Order of Precedence ..... 8

**3. ACRONYMS AND DEFINITIONS ..... 9**  
3.1 Acronyms and Abbreviations ..... 9  
3.2 Definitions ..... 9

**4. SOFTWARE ASSURANCE AND SOFTWARE SAFETY REQUIREMENTS... 15**  
4.1 Software Assurance Description ..... 15  
4.2 Safety-Critical Software Determination ..... 15  
4.3 Software Assurance and Software Safety Requirements ..... 16  
4.4 Independent Verification & Validation (IV&V) ..... 46  
4.5 Principles Related to Tailoring the Standard Requirements ..... 53

**LIST OF APPENDICES**

APPENDIX A. Appendix A Guidelines for the Hazard Development involving Software ..... 55

**LIST OF TABLES**

Table 1. Software Assurance and Software Safety Requirements Mapping Matrix ..... 17  
Table 2. Additional considerations when identifying software causes in hazard analysis ..... 57

# SOFTWARE ASSURANCE AND SOFTWARE SAFETY STANDARD

## 1. SCOPE

### 1.1 Document Purpose

1.1.1 The purpose of the Software Assurance and Software Safety Standard is to define the requirements to implement a systematic approach to Software Assurance (SA), software safety, and Independent Verification and Validation (IV&V) for software created, acquired, provided, or maintained by or for NASA. Various personnel in the program, project, or facility, and Safety and Mission Assurance (SMA) organizations can perform the activities required to satisfy these requirements. The Software Assurance and Software Safety Standard provides a basis for personnel to perform software assurance, software safety, and IV&V activities consistently throughout the life of the software, that is, from its conception, through creation to operations and maintenance, and until the software is retired.

1.1.2 The Software Assurance and Software Safety Standard, in accordance with NPR 7150.2, NASA Software Engineering Requirements, supports the implementation of the software assurance, software safety, and IV&V sub-disciplines. The application and approach to meeting the Software Assurance and Software Safety Standard will vary based on the system and software products and processes to which they are applied. The Software Assurance and Software Safety Standard stresses coordination between the software assurance sub-disciplines, as well as with system safety, system reliability, hardware quality, system security, and software engineering, to maintain the system perspective and minimize duplication of effort.

1.1.3 The objectives of the Software Assurance and Software Safety Standard include:

- a. Ensuring that the processes, procedures, and products used to produce and sustain the software conform to all requirements and standards specified to govern those processes, procedures, and products.
- b. Ensuring that the software systems are safe and that the software safety-critical requirements and processes are followed.
- c. Ensuring that the software systems are secure.

1.1.4 The Software Assurance and Software Safety Standard is compatible with all software life-cycle models. The Software Assurance and Software Safety Standard does not impose a particular life-cycle model on each software project; it does support a standard set of life-cycle phases as defined in NPR 7150.2.

1.1.5 In this standard, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The terms “may” denotes a discretionary privilege or permission, “can” denotes statements of possibility or capability, “should” denotes a good practice and is recommended, but not required, “will” denotes expected outcome, and “are/is” denotes descriptive material.