Ames Procedural Requirements

APR 8705.1
Effective Date: September 19, 2023
Expiration Date: September 19, 2028

COMPLIANCE IS MANDATORY

Subject: System Safety and Mission Assurance

Responsible Office: Code Q / Safety and Mission Assurance Directorate

CHANGE LOG

Status [Baseline /Revision /Cancelled]	Document Revision	Date of Change	Description
Baseline	-	9/19/2023	New baseline version. Updated terminology to "SMA," "SSMA," and CIL. Revised roles and responsibilities to reflect actual support. Revised Chapter 2 "SMA Approach" and changed the content of the chapter to define SMA support for internal and external support. Added information for risk classifications. Changed terminology from "independent and imbedded" to "oversight and "insight." Removed all references to operational concept and absorbed most information in other areas of the APR. Removed Chapter 3, Minimum Quality Management System Requirements for NASA ARC Work. Removed Chapter 4, SS&MA Compliance Matrix. Removed SS&MA Plan Outline.

TABLE OF CONTENTS

PREFACE

P.1 Purpose

P.2 Applicability

P.3 Authority

P.4 Applicable Documents and Forms

P.5 Measurement/Verification

P.6 Cancellation

CHAPTER 1 RESPONSIBILITIES

1.1 Project Manager (PM)

1.2 SMA Director

1.3 SSMA (Code QS) Division Chief

1.4 Project SMA Lead

1.5 Software Assurance (SA) Function

1.6 Quality Assurance/Quality Engineering (QA/QE) Function

1.7 Systems Safety (SS) Function

CHAPTER 2 SMA APPROACH

2.1 Risk Classification Guidance

2.2 Risk-Based SMA

2.3 Ames Quality Management System (AQMS) Compliance

2.4 Overview of Safety and Mission Assurance for External Projects

2.5 SMA Support to Projects

CHAPTER 3 SMA RECORDS

APPENDIX A. DEFINITIONS

APPENDIX B. ACRONYMS

APPENDIX C. REFERENCES

PREFACE

P.1 PURPOSE

a. The scope of this APR defines the Center's Safety and Mission Assurance (SMA) requirements for flight projects and/or flight activities performed at or managed by Ames Research Center (ARC).

P.2 APPLICABILITY

a. This directive is applicable to ARC and associated facilities supporting flight project activities. For the purposes of this APR flight projects include spaceflight, aeronautics, rockets, and sounding rockets.

b. This directive applies to all flight project work (herein referred to as a project) being led by Ames Research Center including those activities which are not captured under the Program/project designation (ref. NPR 7120.5 and NPR 7120.8).

c. For those activities wherein Ames is partnering with other domestic or foreign Governments, academics, and/or industry partners, or other NASA Centers, the applicable procedural requirements will be jointly negotiated by the cognizant authorities and delineated in the statement of work or customer agreement for the activity. This agreement will establish the hierarchy and reconciliation of the procedural requirements to be followed.

d. This APR applies to all ARC employees and contractors who support the above-described activities as a member of a technical team or in any other capacity.

e. This directive applies to contractors, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

f. This document does not apply to facility projects, which are governed by NPR 8715.3, NASA General Safety Program Requirements, NPR 8820.2, Facility Project Requirements, and APR 7120.3, Development and Operation of Center Critical Facilities and Infrastructure.

g. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes an expected outcome, and "are/is" denotes descriptive material.

h. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

P.3 AUTHORITY

a. NPD 8700.1, NASA Policy for Safety and Mission Success

P.4 APPLICABLE DOCUMENTS AND FORMS

a. NPR 7120.5, NASA Space Flight Program and Project Management Requirements

b. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements

c. NPR 7150.2, NASA Software Engineering Requirements

d. NPR 8735.2, Hardware Quality Assurance Program Requirements for Programs and Projects

e. APR 1120.1, Ames Safety and Mission Assurance Technical Authority (SMATA) and Health and Medical Technical Authority (HMTA).

f. APR 5100.1, Purchasing

g. APR 8735.5, Procurement Quality Assurance (PQA) Requirements

h. NF 1707, Special Approvals and Affirmations of Requisitions

i. NASA-STD-8739.8, Software Assurance and Software Safety Standard

j. NASA-HDBK-2203, NASA Software Engineering Handbook

k. QS-033, Customer Agreement

P.5 MEASUREMENT/VERIFICATION

a. Verification of conformance to requirements in this directive are measured through Center and Responsible Organizational management reviews, self-assessments, and subsequent analysis and reports of conformance to requirements, as well as periodic internal audits.

P.6 CANCELLATION

a. APR 8705.1, System Safety and Mission Assurance, dated May 16, 2018.

Eugene Tu
Director

DISTRIBUTION STATEMENT:

Internal and external distribution.

CHAPTER 1 RESPONSIBILITIES

1.1 Project Manager (PM) shall ensure:

a. The SSMA Division is notified of projects in the formulation phase to determine the necessary resources for support.

b. Code QS Customer Agreement (CA) form QS-033 is reviewed and approved.

c. There exists a clear line of communication with the assigned SMA Lead to raise concerns, problems, issues, and tailoring desires.

d. Safety requirements are defined, managed, implemented, and controlled with SMA support.

e. The SMA Lead is included in the project risk process, reviews, and boards.

f. SMA Management is invited to Project Milestone Reviews.

g. SMA Plans are created and submitted for review and approval.

h. Procurements of flight hardware, safety-critical, mission critical, and special processes comply with APR 5100.1, Purchasing, with the use of NF 1707 and APR 8735.5, Procurement Quality Assurance (PQA) Requirements.

i. All items associated with Critical Work are documented on a Project Critical items List (CIL), including:

(1) Any critical attributes and/or key characteristics associated with the items on the CIL.

(2) Items on the CIL that require Complex Work.

1.2 SMA Director shall:

a. Establish Code Q's work priorities.

b. Provide resources to the SSMA Division necessary to perform the SMA function, beyond project provided resources.

c. Exercise SMA Technical Authority (TA) and delegate, as appropriate, to the SSMA Division Chief.

1.3 SSMA (Code QS) Division Chief shall:

a. Appoint program and project SMA Leads.

b. Negotiate, authorize, and oversee SMA support for projects and other activities requesting or requiring SMA support.

c. Evaluate and approve project SMA plans.

d. Review and approve the Code QS CA, form QS 033

e. Exercise SMA TA if a disagreement arises between the project and the SMA Lead.

f. Delegate SMA TA, when appropriate, to the SMA Lead and designating that role as the Chief Safety and Mission Assurance Officer (CSO) (see APR 1120.1).

g. Report SMA resource requirements to the SMA Director.

h. Regularly review and assess project SMA support, oversight, and product deliverables.

i. Assign SMA Internal Review Board (IRB) members upon request from project or program.

j. Ensure Code QS staff are adequately trained to perform their SMA work responsibilities and meet agency training requirements.

1.4 Project SMA Lead

1.4.1 The Project SMA Lead determines the appropriate level of effort for each SMA discipline (Quality Assurance, Software Assurance, System Safety, etc.) for what is required to support the project. The SMA Lead and Code QS Division Chief negotiate the final allocation with the PM. The SMA Lead shall:

> *Note: SMA Lead may sometimes be referred to as either CSO or MAM. The CSO has technical authority as defined in APR 1120.1. The MAM has only lead responsibilities defined in this section.*

a. Manage and oversee all project SMA activities.

b. Assist the Project Manger to determine the Project SMA requirements and the resources needed to fulfill Agency and Center policies and requirements, and applicable Ames Quality Management System (AQMS) requirements. The expected resources will be defined in the Code QS CA. This determination will be based on an assessment of the project's accepted risk posture, mission requirements, duration, and environments.

c. Support program/project offices in the determination of the CIL, including identification of the applicable quality management system requirements to apply to the work associated with the CIL.

d. Develop the project Safety and Mission Assurance Plan (SMAP) which will include project specific SMA requirements, roles, responsibilities, and activities. The SMAP will be updated and maintained over the project life cycle to assure SMA changes are captured. The SMAP may include other plans depending on the project size and complexity.

e. Assist projects and requirements owners to identify applicable SMA requirements to be incorporated into procurement contracts.

f. Verify and assure project compliance with Agency and Center SMA policies, requirements, and standards.

g. Qualify heritage or pre-existing hardware; inspect and evaluate any systems designed, fabricated, or used on a previous project to determine suitability for the current project. At a minimum, evaluate the following factors:

(1) Storage and transportation conditions between fabrication/usage and project utilization.

(2) Limited-life items such as lubricants, seals, etc.

(3) Effects of previous usage.

(4) Quality/state of system documentation.

h. Support all milestone and project reviews, as well as peer reviews.

i. Notify the SSMA Division Chief when a technical or milestone review is scheduled.

1.5 Software Assurance (SA) Function shall:

a. Perform all software assurance activities for the project as specified in the Code QS Customer Agreement.

b. Provide the SMA Lead with a status of any issues, noncompliance, or risks and track to closure.

c. Develop and maintain the project Software Assurance Plan.

d. Verify project compliance with Agency and Center Software Assurance policies, requirements, and standards.

e. Participate in supplier selection and assure that Capability Maturity Model Integration Maturity Level 2 was part of the evaluation criteria when appropriate (software classified as Class B or higher).

f. Assess the need for IV&V support based on the project's software classification and resources.

1.6 Quality Assurance/Quality Engineering (QA/QE) Function shall:

Fulfill all Quality Assurance (QA) and Quality Engineering (QE) activities as specified in the Code QS Customer Agreement. These activities may include:

a. Assigning and witnessing Mandatory Inspection Points (MIPs), reviewing drawings, verifying hazard controls, tracking nonconformances, attending Material Review Boards (MRBs), performing receiving inspections, witnessing testing, and assuring project compliance to project levied standards and requirements.

b. Generating a Quality Assurance Plan in accordance with NPR 8735.2, Hardware Quality Assurance Program Requirements for Programs and Projects (depending on the size and risk posture of the project).

1.7 Systems Safety (SS) Function shall:

a. Work with systems engineering to conduct system safety hazard analyses across the project systematically: hardware, software, facility, and personnel.

b. Help in identifying, characterizing, and controlling hazards to an acceptable level of risk.

c. Verify effectiveness and track hazard controls to closure.

d. Assure compliance with all applicable safety requirements which may include the development of safety products for the project.

e. Generate the System Safety Plan which establishes safety requirements, milestones, managed responsibilities, and analysis methods for accomplishing the program safety objectives.

CHAPTER 2 SMA APPROACH

All activities associated with System Safety and Mission Assurance at Ames Research Center are managed by the SSMA Division (Code QS) through the following means identified in this section.

2.1 Project Types with Risk-Based SMA Guidance

Note: Referenced from GPR 8705.4, Risk Classification and Risk-Based SMA Practices for GFSC Payloads and Systems.

2.1.1 NPR 7120.5-governed projects are divided into four risk classifications, Classes A through D, per NPR 8705.4. This section does not include Classes A or B as ARC does not typically manage these types of projects; however, ARC personnel may support an external project managed at another Center and will follow their processes and requirements

2.1.2 Some missions may have a subsystem that may be designated as a lower risk classification than the overall mission success criteria. Therefore, the SMA requirements and approach applied to each subsystem will vary dependent on their respective risk classifications.

2.1.3 The following guidance provides clarity for risk classifications for Class C and D projects managed at ARC. The following guidance also provides some clarity for NPR 7120.8 projects, which are not risk classified, managed at ARC.

2.1.3.1 Class C: Moderate risk posture. This would represent an instrument or spacecraft whose loss would result in a loss or delay of some key national science objectives.

2.1.3.2 Class D: Allowable technical risk is medium by design. Many credible single point failures mission risks may exist. New technologies may be employed that may not be fully compatible with some traditional requirements, which must be accounted for when requirements are imposed.

2.1.3.3 NPR 7120.8 Projects are not defined by risk classifications. Some level of failure at the project level is expected but at a higher level (program level), there would normally be an acceptable failure rate across a portfolio of individual projects defined with the program office. Failure of an individual project during the mission lifetime is considered as an accepted risk, and hence is not considered a mishap, but if the failure rate were too high, special review may be required.

2.2 Risk-Based SMA

2.2.1 Risk-based SMA is the process of “right-sizing” resources to optimize the probability for safety and mission success by focusing on mitigating specific risks that are applicable to the project versus simply enforcing a set of requirements indiscriminately.

2.3 Ames Quality Management System (AQMS) Compliance

2.3.1 When projects meet the requirements of the AQMS scope, the project will comply with APD 1280.1 requirements. SMA will support AQMS audit request with the project to meet Ames internal audit requirements.

2.3.2 SMA assures AS9100 compliance with the project, suppliers, and contracts. There will be some companies that are certified to only ISO 9001-2015 that can meet the intent of AQMS by the product or manufacturing performed. These approvals, by SMA representatives and the PM, need to be documented to show suitable risk acceptance. This documentation will be held at the project level.

2.4 Overview of Safety and Mission Assurance for External Projects

For those activities wherein Ames is responsible for a task within a project led by an organization outside of Ames, the applicable procedural requirements are jointly negotiated by the cognizant authorities and delineated in a Memorandum of Understanding (MOU) or equivalent. This agreement will establish the hierarchy and reconciliation of the procedural requirements to be followed.

2.5 SMA Support to Projects

2.5.1 Technical Authority

When a project is assigned an SMA Lead, the Technical Authority remains with the Code QS Division Chief. When Technical Authority is delegated to the SMA Lead by the Code QS Division Chief, their role will be designated as the CSO for the project.

2.5.2 SMA project support can be performed as either insight or oversight based on the project's accepted risk posture. The nature and the level of support shall be documented in Code QS form QS 033 Customer Agreement Form.

2.5.2.1 Insight SMA Support

a. Insight is a surveillance approach whereby the Project may accept a slightly higher level of risk based on any of the following: performing verifications of inspections versus performing inspections, leveraging previous experience with a supplier, leveraging previous audits and analyses (e.g., gap analysis), or partial reliance on a supplier's quality system, and may include reduced surveillance.

b. SMA insight support may be requested by a project to support milestone/project reviews, small low-cost projects with accepted risk without SMA support, or other reviews requiring SMA TA evaluation. A request for SMA support may start as an independent assessment that is captured in a QS Customer Agreement to determine the level of SMA support and staffing requirements for a project.

2.5.2.2 Oversight SMA Support

a. Oversight is a surveillance approach that is more engaged, thorough, and rigorous. SMA tracks and verifies design requirements (design, design changes, design risks, design hazards, nonconformances, and software development) and mission success impacts. Per NPR 8735.2, this approach is a continuum that can range from low intensity, such as SMA concurrence in reviews (e.g., PDR, CDR), to high intensity in which SMA has day-to-day involvement in the decision-making process (e.g., hardware/software inspections).

b. Oversight SMA support is part of the project and Work Breakdown Structure (WBS) that is funded to support the required resources effort during the project lifecycle. SMA is integrated with the project while maintaining their independence, with oversight responsibilities to assure safety and mission success within the accepted risk posture.

Note: A gap analysis may support either the insight or the oversight approach.

2.5.3 SMA Requirements Identification

2.5.3.1 SMA requirements will be documented in one or more of the following:

a. Program-Level Mission Assurance Requirements (MAR) is a Program level SMA requirements document. When a MAR is required by the Program, the SMA Lead will work with the PM to develop and tailor any requirements before submission to the Program.

b. Project-Level SMA Lead will generate a SMAP defining the SMA requirements that will be levied on the project. The SMAP is developed with the appropriate balance of applicable requirements aligned with the project risk classification (NPR 8705.4 or NPR 7120.8). The SMAP will be generated utilizing the Code QS Class D SMAP Template. For NPR 7120.5 projects with a Class D risk classification, this template provides the SMA requirements for the project. For NPR 7120.8 projects, the SMAP Template will be a starting point and tailored to meet the project's needs.

c. At the discretion of the SMA Lead and SSMA Division Chief, the project size and complexity may allow a CA to be sufficient in lieu of a SMAP.

2.5.3.2 The tailoring of SMA requirements is developed with the PM and the Lead Systems Engineer (LSE as defined in APR 1120.2) The accepted risk posture, mission duration, and mission environment are assessed to help determine how to tailor SMA requirements and determine the resources required to support the project. The tailored requirements are defined in the Project SMAP. The project shall comply with the approved SMA requirements stated in the enacted SMAP.

2.5.3.3 Deviation and Waivers

The decision to deviate or waive a requirement shall be generated in the Problem Reporting And Corrective Action (PRACA) database under the waiver page per APR 8735.2, Deviation/Waiver Process, and obtain the SMA Lead review and approval before submitting for official approval by the Center TAs (SMA or Chief Engineer (CE)).

2.5.3.4 Escalation Process for Residual Risk

If the Project's residual safety risk cannot be approved/concurred with at the Project level, then the matter is escalated through the successive and parallel program/project and SMA authority management chains for resolution. Reference APR 1120.1, Ames Safety and Mission Assurance Technical Authority (SMATA) and Health and Medical Technical Authority (HMTA). The first level of SMA TA is the CSO, when delegated, otherwise the SSMA Division Chief.

CHAPTER 3 SMA RECORDS

The following are SMA-generated documents that will be archived in the QS database:

- Code QS Customer Agreement
- Letters of Delegation
- Memorandum of Understanding

APPENDIX A. DEFINITIONS

Assure	To provide confidence that a target act will be performed and/or a target condition will be met (e.g., that upon fulfilling SMA requirements a system's risk will not exceed the limits established for safety or fail to meet its mission performance objectives).
Code QS Customer Agreement	Agreement between the Project and Code QS on the level of effort of resources and expectations agreed upon.
Deviation	A documented authorization releasing a program or project from meeting a requirement before the requirement is put under configuration control at the level the requirement will be implemented.
Ensure	To take action that results in a target action being performed and/or a target condition being met (e.g., that the SMA requirements have been fulfilled as reflected by tangible evidentiary artifacts).
Hazard	A state or set of conditions, internal or external to a system, that has the potential to cause harm.
Safety	Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment, property, facility, or damage to the environment.
SMA Lead	Assigned to projects as either a Chief Safety Officer or Mission Assurance Manager to provide overall SMA support.
Waiver	(1) A written authorization to depart from a specific requirement. (2) A documented authorization releasing a program or project from meeting a requirement after the requirement is put under configuration control at the level the requirement will be implemented.

APPENDIX B. ACRONYMS

APR	Ames Procedural Requirements
AQMS	Ames Quality Management System
ARC	Ames Research Center
CA	Customer Agreement
CE	Chief Engineer
CIL	Critical Items List
CSO	Chief Safety Officer
IRB	Independent Review Board
IV&V	Independent Verification and Validation
MAM	Mission Assurance Manager
MAR	Mission Assurance Requirements
MIP	Mandatory Inspection Point
MOU	Memorandum of Understanding
MRB	Material Review Board
MSE	Mission Systems Engineer
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
PDR	Preliminary Design Review
PQA	Procurement Quality Assurance
PRACA	Problem Reporting and Corrective Action
PSE	Project Systems Engineer
QA	Quality Assurance
QE	Quality Engineering
SA	Software Assurance
SMA	Safety and Mission Assurance
SMAP	Safety and Mission Assurance Plan
SME	Subject Matter Expert
SS	Systems Safety
SSMA	System Safety and Mission Assurance
TA	Technical Authority
WBS	Work Breakdown Structure

APPENDIX C. REFERENCES

C.1 NPD 8700.1, NASA Policy for Safety and Mission Success

C.2 NPR 7120.5, NASA Program and Project Management Processes and Requirements

C.3 NPR 7120.8, NASA Research and Technology Program and Project Management Requirements

C.4 NPR 8000.4, Agency Risk Management Procedural Requirements

C.5 NPR 8621.1, NASA Procedural Requirement for Mishap and Cloe Call Reporting, Investigating, and Recordkeeping

C.6 NPR 8705.4, Risk Classification for NASA Payloads

C.7 NPR 8715.1, NASA Occupational Safety and Health Programs

C.8 NPR 8715.3, NASA General Safety Program Requirements

C.9 NPR 8715.5, Range Flight Safety Program

C.10 NPR 8715.6, NASA Procedural Requirements for Limiting Orbital Debris

C.11 NPR 8715.7, Payload Safety Program

C.12 NPR 7150.2, NASA Software Engineering Requirements

C.13 NPR 8735.1, Procedures for Exchanging Parts, Materials, Software, and Safety Problem Data Utilizing the Government-Industry Data Exchange Program (GIDEP) and NASA Advisories

C.14 NPR 8735.2, Hardware Quality Assurance Program Requirements for Programs and Projects

C.15 APD 1280.1, ARC Quality Management System

C.16 APD 8700.1, Problem, Nonconformance, Preventative and Corrective Action Management Policy

C.17 APR 1120.1, Ames Safety and Mission Assurance Technical Authority and Health and Medical Technical Authority

C.18 APR 1280.4, Ames Quality Management System (AQMS) Requirements

C.19 APR 1740.1, Airworthiness and Flight Safety

C.20 APR 5100.1, Purchasing

C.21 APR 7120.51, Reviews for Spaceflight Projects

C.22 APR 7150.2, Software Engineering Requirements

C.23 APR 8000.4, Risk Management Process Requirements

C.24 APR 8715.1, Ames Health, and Safety Procedural Requirements

C.25 APR 8730.1, Metrology and Calibration

C.26 APR 8739.10, Ames Electrical, Electronic, and Electromechanical (EEE) Parts Control Requirements

C.27 APR 8735.1, Procedures for Preparation and Handling of NASA Advisories and Government-Industry Data Exchange Program (GIDEP) Alerts, Safe Alerts, and Problem Advisories

C.28 APR 8735.2, Deviation/Waiver Process

C.29 APR 8735.3, Control of Nonconforming Products and Services

C.30 APR 8735.5, Procurement Quality Assurance (PQA) Requirements

C.31 NF 1707, Special Approvals and Affirmations of Requisitions

C.32 QS 033, Code QS Customer Agreement

C.33 QS 002, Procurement Quality Requirements

C.34 QS 005, Receiving Inspection Report NASA-STD-8739.1, Workmanship Standard for Polymeric Application on Electronic Assemblies

C.35 NASA-STD-8709.22, Safety & Mission Assurance Acronyms, Abbreviations, & Definitions

C.36 NASA-STD-8719.14, Process for Limiting Orbital Debris

C.37 NASA-STD-8719.24, NASA Payload Safety Requirements

C.38 NASA-STD-8719.24 Annex, NASA Payload Safety Requirements Annex

C.39 NASA-STD-8719.9, Lifting Standard

C.40 NASA-STD-8729.1, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems

C.41 NASA-STD-8739.4, Workmanship Standard for Crimping, Interconnecting Cables, Harnesses, and Wiring

C.42 NASA-STD-8739.5, Workmanship Standard for Fiber Optic Terminations, Cable Assemblies, and Installation

C.43 NASA-STD-8739.6, Implementation Requirements for NASA Workmanship Standards

C.44 NASA-STD-8739.8, Software Assurance and Software Safety Standard

C.45 NASA-HDBK-2203, NASA Software Engineering and Assurance Handbook

C.46 AFSCMAN 91-710, Air Force Space Command Manual (AFSPCM) Vol 3

C.47 AS9100, Quality Management Systems-Requirements for Aviation, Space, and Defense Organizations