



Dryden Flight Research Center
Edwards, California 93523

DCP-S-004, Revision C
Expires August 4, 2011

Dryden Centerwide Procedure

Code S

System Safety Support

Electronically approved by
Assistant Director for Management Systems

Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

CONTENTS

1.0	PURPOSE OF DOCUMENT	3
2.0	SCOPE & APPLICABILITY	3
3.0	PROCEDURE OBJECTIVES	3
4.0	RELEVANT DOCUMENTS.....	3
4.1	Authority Documents.....	4
4.2	Reference Documents	4
4.3	Forms.....	5
5.0	WAIVER AUTHORITY.....	5
6.0	ABBREVIATIONS, ACRONYMS, & DEFINITIONS	5
6.1	Acronyms	5
6.2	Definitions	6
7.0	FLOWCHART	9
8.0	METRICS & TREND ANALYSIS	15
9.0	MANAGEMENT RECORDS & RECORDS RETENTION	15

1.0 PURPOSE OF DOCUMENT

This document represents the System Safety processes that are accepted at Dryden for eliminating or minimizing the occurrence of accidents and mishaps. System Safety Engineering terminologies and typical project-level System Safety steps are identified, and the responsibilities of Center management and project personnel toward appropriate documentation, management, and tracking of risks are specified. The premise for this procedure is that the accomplishment of its goals will add value to, and contribute to successful accomplishment of Dryden aerospace projects.

2.0 SCOPE & APPLICABILITY

The scope of this document covers projects at Dryden except where specifically waived by the Chief Office of Safety and Mission Assurance (OS&MA). This process covers flight activity conducted at the center, and augmented by the processes of the OS&MA, Chief Engineer, and Research Engineering Directorate.

As outlined in NPR 8000.4, Continuous Risk Management (CRM) programmatic risks are candidate elements of the project risk level estimate during the project approval phase. But, continued analysis and monitoring of these risks will be accomplished by the Project Manager (PM). The PM will be responsible for tracking and reporting of these risks, as well as safety risks to Senior Management through the existing project review process at the Dryden Program Management Council (DPMC).

3.0 PROCEDURE OBJECTIVES

The objective of this procedure is to provide a structured approach to System Safety engineering processes for managing risk and hazards on aerospace and ground systems, as required, for which Dryden assumes ground, range, flight safety, airworthiness, or mission success responsibility.

4.0 RELEVANT DOCUMENTS

The underlying objective of this procedure is shared by many supporting procedures at Dryden. Specifically, this procedure supports DHB-X-001, Airworthiness and Flight Safety Review (AFSRB), independent review, Mission Success Review (MSR), Technical Brief (T/B), and Mini-Tech Brief (MT/B) guidelines by providing prime information needed to accomplish its goals. The Hazard Action Matrix and the Accepted Risk List are also prime sources of information for the DHB-X-001 processes. Other relevant documents are as follows:

- DCP-S-006, Quality Assurance Audit, is the primary quality procedure that assures that processes are being used to identify and prevent poor workmanship or low quality components.

Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

- DCP-S-007, Software Assurance Procedure, DCP-S-046, Flight Research Software Assurance Audit and Corrective Action Procedure, and DOP-S-006, Software Safety Job Instruction, are procedures that are designed to prevent software interactions with hardware from creating mishaps. These procedures support this System Safety Support Procedure by providing “front line” sources of hazard mitigation.

4.1 Authority Documents

NPR 8000.4	NASA Risk Management Procedural Requirements w/Change 1 (4/13/04)
NPR 8715.3	NASA Safety Manual
NPR 7120.5	NASA Program and Project Management Processes and Requirements
NPR 7150.2	NASA Software Engineering Requirements
NASA-STD-8719.7	Facility System Safety Guidebook
NASA-STD-8739.8	Software Assurance Standard
NASA-STD 8719.13A	Software Safety Standard

4.2 Reference Documents

MIL-STD-882	DoD Standard Practice for System Safety
DCP-P-016	Configuration Management of Flight Research Projects
DCP-P-017	Configuration Change Process for Flight Project Critical Systems
DCP-P-018	Discrepancy Reporting Process for Flight Project Critical Systems
DCP-S-001	Aircraft Mishap Response Procedure
DCP-S-002	Hazard Management Procedure
DOP-S-006	Software Safety Job Instruction
DCP-S-007	Software Assurance
DCP-S-046	Flight Research Software Assurance Audit and Corrective Action Procedure
DCP-X-008	Tech Brief (T/B) AND Mini-Tech Brief (Mini-T/B)
DCP-X-009	Airworthiness and Flight Safety Review Process
DHB-S-001	System Safety Handbook
DHB-X-001	Airworthiness and Flight Safety Review, Independent Review, Mission Success Review, Technical Brief and Mini-Tech Brief Guidelines

Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

4.3 Forms

DFRC 8-328	Hazard Report
DFRC 8-331	Accepted Risk List
TEM-001a/b	Hazard Action Matrix
WK 8-330	Risk Mitigation Worksheet
CK 8-336	Safety Checklist for Dryden Programs

5.0 WAIVER AUTHORITY

Waivers granted to this procedure shall be documented in project documentation (e.g., Project Plan, Risk Management Plan, or System Safety Plan). Waivers should be submitted by the project or research lead during the formulation phase.

- A. The Project Manager is responsible for ensuring waivers and variances to the content of the Dryden System Safety Support Procedure have been obtained.
- B. The assigned System Safety Engineer will review and evaluate request for waivers or variance and make recommendations based on findings to the Code SF branch chief.
- C. The Chief, OS&MA, has the approval authority for waivers and variances to the content of the Dryden System Safety Support Procedure.
- D. The Project Manager will assure that the official waiver or variance is properly filed and maintained with the project records.

6.0 ABBREVIATIONS, ACRONYMS, & DEFINITIONS

6.1 Acronyms

AFSRB	Airworthiness and Flight Safety Review Board
ARL	Accepted Risk List
CCB	Configuration Control Board
CDRL	Contract Data Requirements List
CRM	Continuous Risk Management
DPMC	Dryden Program Management Council
FAM	Flight Assurance Matrix
FMEA	Failure Mode and Effects Analysis
FRR	Flight Readiness Review
FTA	Fault Tree Analysis

Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

HA	Hazard Analysis
HAM	Hazard Action Matrix
HR	Hazard Report
MIL-STD	Military Standard
MT/B	Mini-Tech Brief
MSR	Mission Success Review
NPR	NASA Procedural Requirements
ORR	Operational Review Board/Operational Readiness Review
O&SHA	Operating and Support Hazard Analysis
OS&MA	Office of Safety and Mission Assurance
PAG	Program Approval Group
PHA	Preliminary Hazard Analysis
PM	Project Manager
RMP	Risk Management Plan
RSHA	Range Safety Hazard Analysis
RTB	Return-To-Base
SF	Flight Assurance Office
SHA	System Hazard Analysis
SSHA	Subsystem Hazard Analysis
SSWG	System Safety Working Group
T/B	Technical Brief

6.2 Definitions

Accepted Risk	A risk that Dryden senior management has accepted as necessary for the accomplishment of a proposed activity. A hazard whose residual risk falls into an “accepted risk” category on the Hazard Action Matrix (TEM-001 a/b).
Airworthy	A test vehicle deemed to operate in a safe manner within a prescribed flight envelope and according to prescribed procedures without sustaining damage.
Airworthiness	The process of qualifying an air vehicle and related parts as ready for flight.
Aviation Safety	The operational aspects of Flight Safety, generally covering those Flight Crew elements dealing with preventative measures such as mishap prevention, mishap reporting, safety awareness and training, and safety inspections.
Flight Safety	The test vehicle, support aircraft, all crewmembers, and uninvolved aircraft return from the test flight without injury or

Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

damage unless the mission is designed to expend the vehicle. No injury to personnel or damage to property occurs on the ground (e.g., flying too low, sonic booms, dropped objects, or crashes into personnel or property).

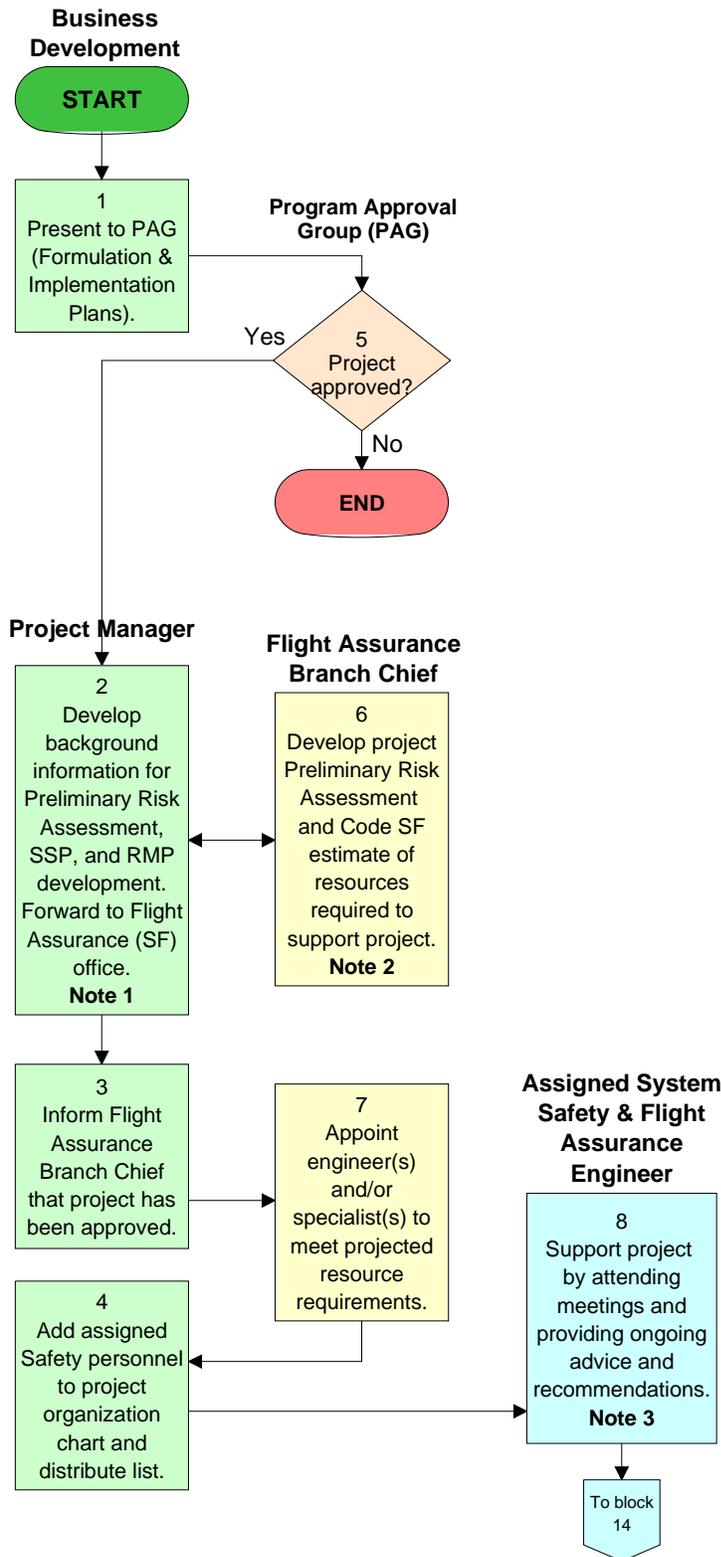
Facility Safety	Safe operations of all facilities.
Failure Tolerance	Ability of a system to perform in a predictable manner after a failure of specified hardware or software components.
Fail-Operational Ability	Ability of a system to perform in a fully operational manner after a failure of hardware or software components.
Fail-Safe	Ability to sustain a failure and retain the capability to safely terminate or control the operation.
Ground Safety	No injury to personnel or damage to equipment in any phase of ground operations, which include all activities that are not flight specific. Ground operations end at launch or at brake release for takeoff roll and recommence after landing roll wheels stop.
Hazard	A hazard is the presence of a potential risk situation caused by the potential for an unsafe act or condition. "A Hazard is an existing or potential condition (event), which can result in or contribute to a mishap."
Hazard Analysis	The timely determination of potential hazards and mitigations for those conditions which could cause a mishap, whether found in the hardware/software systems, the person-machine relationship, or both.
Immediate Cause	An act that led to an undesired outcome or mishap.
Mechanism	The activity that allows an immediate cause to create a mishap.
Mishap	An unexpected, unforeseen, or unintended event that causes injury, loss, or damage to personnel, equipment, property, the environment, or mission accomplishment.
Mission Probability	The aggregate probability of occurrence of the full chain of events that could lead to a specific mishap.
Mission Success	Defined by project prior to the start of test. Desired flight data suitable for analysis is received and flight safety is achieved. The successful achievement of the desired mission objectives, ranging from demonstrating basic flight capability of the vehicle to acquiring specific vehicle characteristic data at a desired flight condition.

(Note: If the mission success criteria for a mission is to fly the aircraft safely, then flight safety and mission success are equivalent for that flight.)

Mitigation	An action taken to reduce the risk of exposure to a hazard.
Range Safety	Range Safety evaluates and mitigates risk to the public and property from Dryden flight operations. There is a recognized overlap with “Flight Safety”. Risk management of the hazards of flight operations that threaten public and property, excluding hazards to the test article.
Responsible Test Organization (RTO)	That organization which is responsible for ensuring that all necessary and appropriate test practices, procedures, and operating requirements are developed and followed to reduce and manage risk to the greatest degree possible while maximizing the likelihood of mission success.
Risk	A quantifiable perception of the combined severity of damage and probability of occurrence of a mishap. Risk assessment consists of evaluating the Severity of consequences and the Probability that the consequences will result.
Root Cause	One of multiple factors (events, conditions, or organizational factors) that contributed to or created the proximate cause and subsequent undesired outcome and, if eliminated or modified, would have prevented the undesired outcome or mishap.
Shall	Requirement that is binding; an absolute requirement of the specification or mandatory provisions.
Should	This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
System Safety Working Group	A group formed of project personnel, normally led by the assigned system safety engineer, specifically tasked to manage the day-to-day activities of the project’s risk management process throughout the life of the project.
Target	The people, equipment, property, mission, or environment that would incur damage or be lost as a result of a mishap.
Variance	Any deviation by the project from NASA Dryden Requirements that still meet or exceed the intent of the stated requirements, as determined by the independent approving authority.
Waiver	Any deviation by the project from NASA Dryden Requirements that does not meet the intent of the stated requirement, but is determined to be safe and permissible by the approving authority.
Will	Facts or Declaration of purpose.

Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

7.0 FLOWCHART



Note 1
Collect background information for Preliminary Risk Assessment, System Safety Plan (SSP) and Risk Management Plan (RMP) via Dryden Safety Checklist (Dryden form [CK 8-336](#)). Some of the topics on the checklist are

- NASA exposure level
- Research priority level
- Vehicle owner
- Flight Safety responsibility
- Ground Safety responsibility
- Range Safety responsibility
- Mission Success responsibility
- Airworthiness responsibility

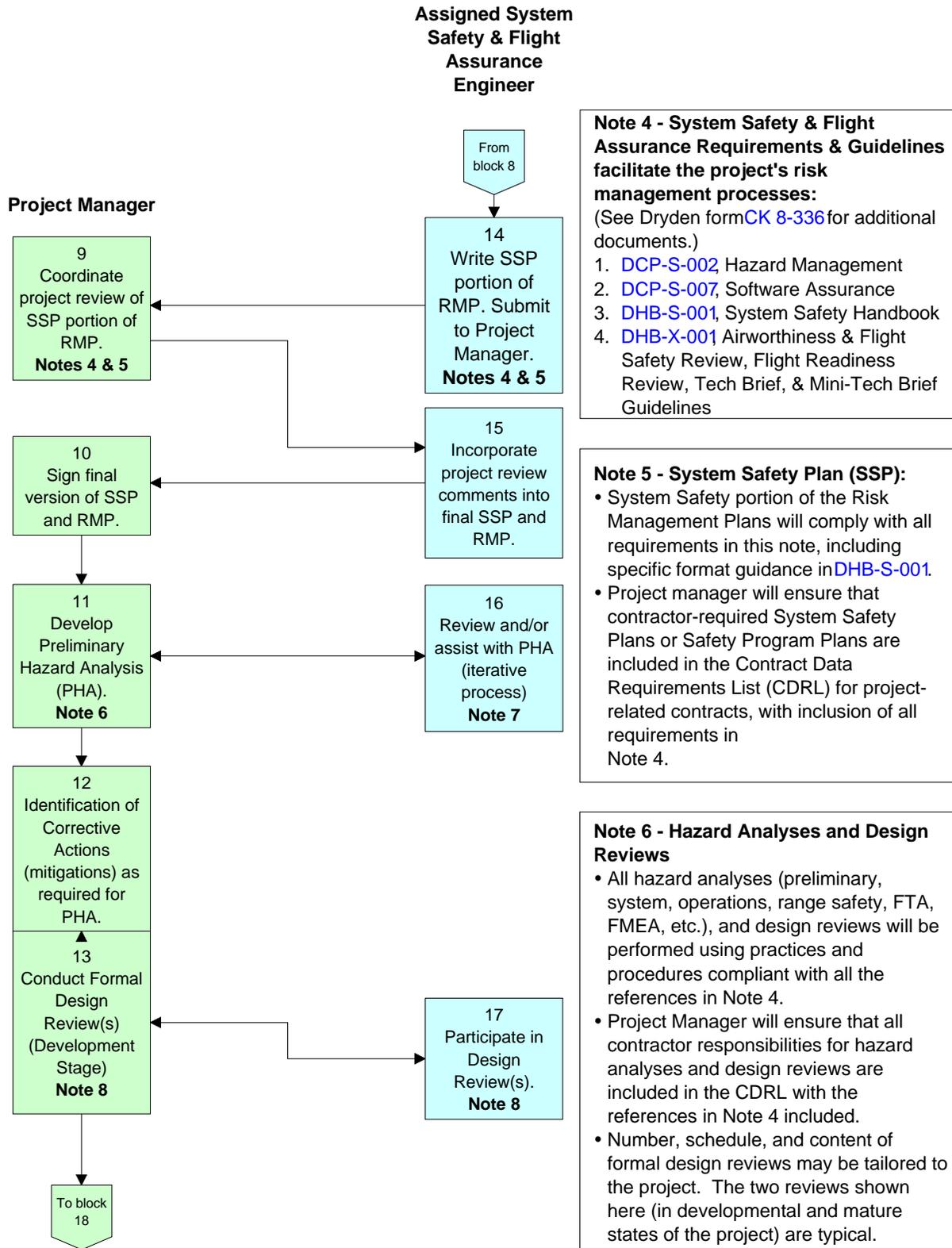
Note 2 - Project risk preliminary estimate and resources content via activity analysis:

- High, medium, or low risk
- Number of full-time equivalents (civil service & contractor)
- Cost estimates

Note 3
The System Safety Engineer is responsible for the timely status update to the Flight Assurance Matrix (FAM), a server-based safety project support tool that provides easy visual status of project safety documentation, hazard analysis, and risk assessment. This tool is reviewed weekly and updated as appropriate, with the project status briefed during the weekly Code SF staff meeting.

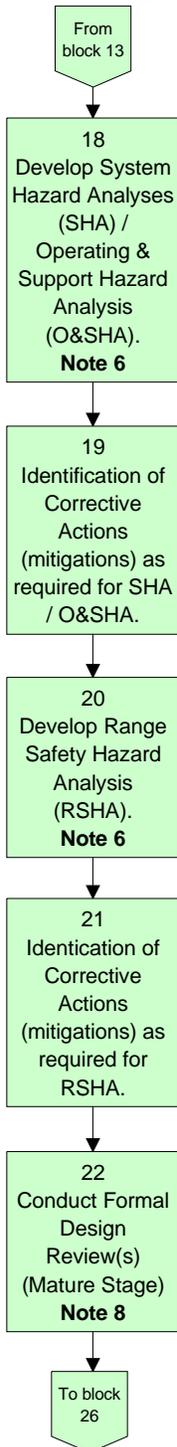
A new option of the FAM

- provides a dropdown page for identification of significant Continuous Risk Management issues, and
- provides the status of the issue, and
- provides the corrective actions/plans, or points to its location in the project database or assigned personnel, to allow a closed-loop approach to track specific project issues/concerns.

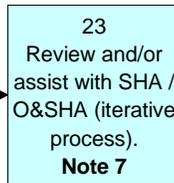


Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

Project Manager

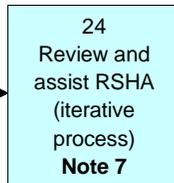


Assigned System Safety & Flight Assurance Engineer



Note 7 - System Safety Engineering Responsibilities for Hazard Analyses

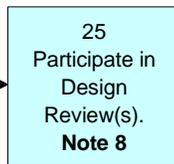
- Depending upon the level-of-effort for the project, the system safety engineer will develop the analysis, assist with developing the analysis, review an in-house analysis, or review a contractor analysis for compliance with all instructions and guidance in Note 4.
- Level-of-effort depends on responsibilities agreed upon in the System Safety Plan and RMP for the completed for CK 8-336 and Note 2.
- All requirements of DCP-S-002, Hazard Management, must be met.

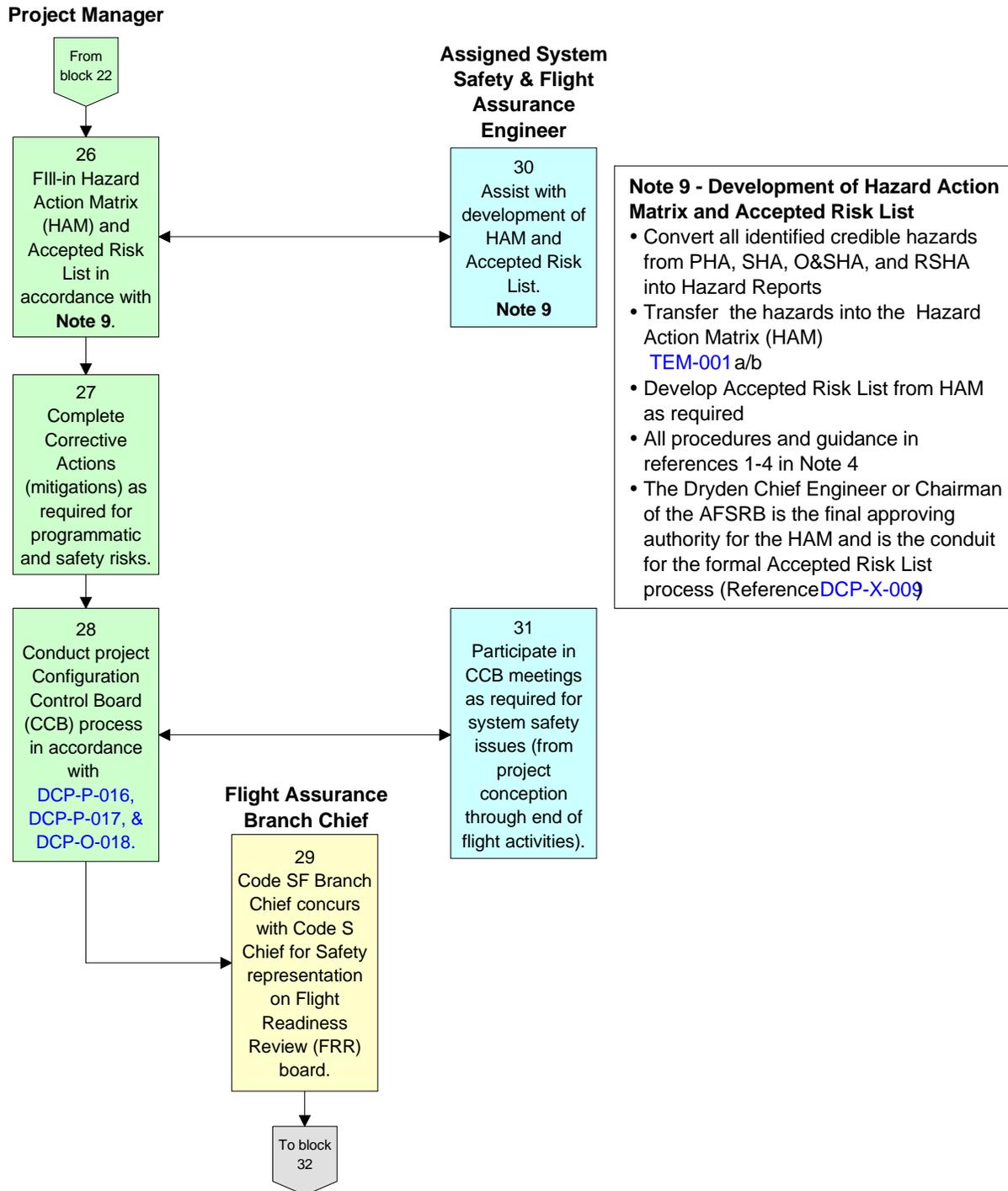


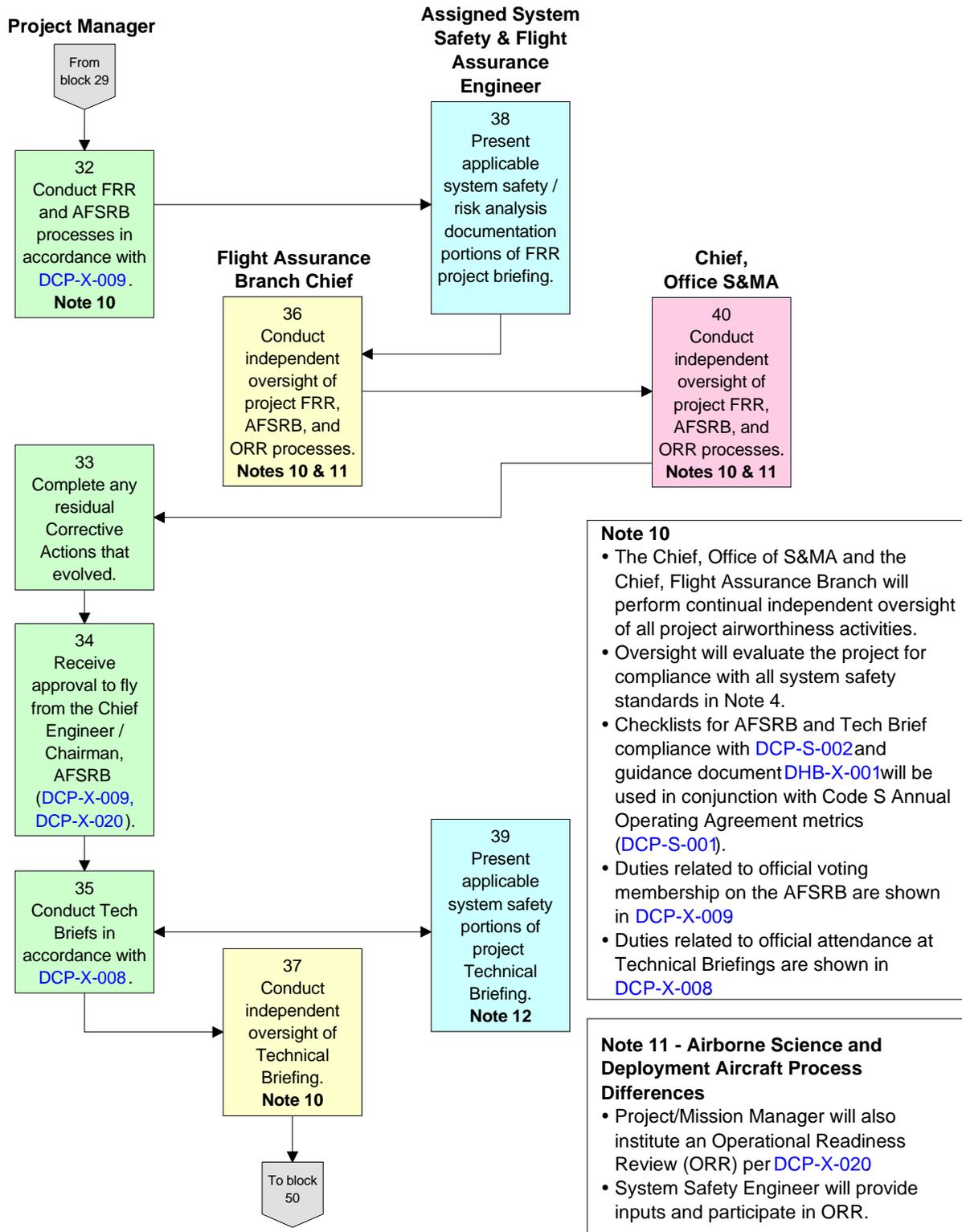
Note 8 - System Safety and Flight Assurance Engineering Responsibilities for Design Reviews

The system safety engineer should participate in design reviews. Duties may include

- Attendance and discussion insights
- Preparation and delivery system safety portions of the review (oral and written)
- Summary reports of hazard analysis results and status
- Technical input for solutions to system safety issues / concerns.







Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.

8.0 METRICS & TREND ANALYSIS

A measurement of the success of this procedure is the project's ability to successfully deliberate the residual risk during reviews (i.e., Project Approval Group, Preliminary Design Reviews, Critical Design Reviews, Technical Briefings, DPMC, etc.) and especially during the Airworthiness Flight Safety Review where managers will be provided sufficient information relating to the hazards of the project to allow them to make informed decisions.

Trends will be determined from the following status items:

- A. Timeliness of safety-related project documentation and hazard analysis
- B. Timeliness of completion of specific project risk issues/problems

In the event of a mishap, trend analysis of the root cause of investigation findings will be utilized in a similar manner. The Flight Assurance Matrix (FAM) tracks the documentation and hazard analysis status.

9.0 MANAGEMENT RECORDS & RECORDS RETENTION

The Hazard Report (HR), Hazard Action Matrix (HAM), and Accepted Risk List (ARL) are Quality Records generated by this procedure and DCP-S-002.

Although generated by this Code S procedure, accomplishment and maintenance of these records are the responsibility of the Project Manager. The Project Manager, in accordance with the process specified in the Configuration Management Plan (DCP-P-016) and the System Safety Plan (DHB-S-001), will keep the official Hazard Reports. The Hazard Action Matrix (HAM) and the Accepted Risk List will be kept in the project's configuration management file (DHB-P-002).

Flight Assurance Matrix (FAM) weekly status briefings will be retained as part of the Safety and Mission Assurance Branch reports. The FAM is a web-based product that is maintained on the server.

Records generated by this process are maintained and archived according to NPR 1441.1, Records Retention Schedule.

Document History Log

This page is for informational purposes and does not have to be retained with the document.

Status Change	Document Revision	Effective Date	Page	Description of Change
Baseline		1-12-99		
Revision	A	1-28-99	All	Minor revisions to the wording in the notes and blocks.
Revision	B	4-15-99	All	<ul style="list-style-type: none"> • Modified Notes 3, 4, 5, 6, 8, 10 • Added new Note 9 • Renumbered Notes and reference to Notes in blocks. • Deleted reference to MIL-STD-882 in Note 3 • Modified terminology for Design Review through process
Revision	C	8-8-06	All	<ul style="list-style-type: none"> • Modified all pages and notes • Modified terminology for system safety throughout process • Reformatted to new Dryden document format
Admin Change	C	9-5-06		<ul style="list-style-type: none"> • Title page: Removed word "Procedure" from title • Doc History Log: Added Rev. C effective date of 8-8-06

Before use, check the Master List to verify that this is the current version.
Dryden distribution only. Contact MSO regarding external distribution.