



Dryden Flight Research Center
Edwards, California 93523

DCP-S-002, Revision B-2
Expires July 12, 2010

Dryden Centerwide Procedure

Code S

Hazard Management Procedure

(With changes 01-28-08)

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	4
2.0	SCOPE & APPLICABILITY	4
3.0	PROCEDURE OBJECTIVES	4
4.0	RELEVANT DOCUMENTS.....	5
4.1	Authority Documents.....	5
4.2	Reference Documents	6
4.3	Informational Documents	6
4.4	Forms.....	6
5.0	WAIVER AUTHORITY.....	6
6.0	ACRONYMS, & DEFINITIONS.....	7
6.1	Acronyms.....	7
6.2	Definitions	8
7.0	HAZARD MANAGEMENT	12
8.0	FLOWCHART	14
9.0	HAZARD IDENTIFICATION AND RECORDING	17
9.1	Hazard Reports.....	17
9.2	Tailoring of the Hazard Report Form.....	18
10.0	HAZARD CLASSIFICATION	19
10.1	General Guidance.....	19
10.2	Hazard Action Matrix.....	19
10.3	Hazard Probability.....	20
10.4	Hazard Severity	21
10.5	Failure Tolerance	23
10.6	Residual Risk Reporting	23
10.7	Accepted Risk.....	24
10.8	Tailoring of the Hazard Action Matrix	24
11.0	HAZARD MITIGATION AND ANALYSIS	25
11.1	Hazard Mitigation	25
11.2	Hazard Analysis	26
12.0	HAZARD MANAGEMENT AND TRACKING	27
12.1	Configuration Control	27
12.2	Hazard Tracking.....	28
12.3	Dryden Management Review.....	29
12.4	Exceptions	30
12.5	Lesson Learned	30
13.0	METRICS & TREND ANALYSIS	31
14.0	MANAGEMENT RECORDS & RECORDS RETENTION	32

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

ATTACHMENTS

Attachment A: Sample Hazard Report Form	33
Attachment B: Hazard Report Field Instructions	35
Attachment C: Risk Mitigation Order of Precedence Worksheet	37
Attachment D: Sample Hazard Action Matrix	39
Attachment E: Sample Accepted Risk List	45

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

1.0 PURPOSE OF DOCUMENT

This procedure documents the Hazard Management processes, methods, and techniques that are accepted at Dryden for eliminating or minimizing the occurrence of accidents and mishaps. The term “risk” in this procedure deals with the severity and probability of occurrence of an accident or mishap that might result from a hazardous act or condition. System Safety Engineering terminologies are defined and other applicable documents and procedures are identified. Accepted methods of identifying, categorizing, and analyzing hazards are presented, 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 safety and mission success as well as contribute to successful accomplishment of Dryden aerospace projects.

2.0 SCOPE & APPLICABILITY

This procedure presents the System Safety Engineering techniques that are used at Dryden to help preclude occurrence of personal injury, loss of test article, or loss of mission during the conduct of Aerospace Projects. It applies to aerospace and ground systems for which Dryden assumes ground, range, flight safety, or mission success responsibility, including that of customers or support contractors. It includes Contractor Furnished Equipment (CFE), Government Furnished Equipment (GFE), and Ground Support Equipment (GSE) that is either unique to the project or program, has not had previous safety analysis, or is being used in an application not covered in previous analysis. Its specific application to flight research operations will include, at a minimum, the test article or vehicle, support subsystems or vehicles, and ground research capabilities.

This process will be followed for all new capabilities and projects at Dryden except where specifically waived by the Independent Technical Authority (ITA) or the Center Director.

This procedure is not intended to address project schedule or budget risks.

3.0 PROCEDURE OBJECTIVES

The objectives of this procedure are to provide a structured approach to hazard management.

- All hazards are identified, understood, and documented.
 - The hazards are submitted in a data format acceptable for historical data recording (electronic database format).

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

- Through identification, analysis, planning, tracking, and control efforts, eliminate or minimize risk.
- Appropriate levels of management understand and have documented acceptance of all risks that are incurred during the conduct of a project.
- Continual efforts are made during the conduct of a project to eliminate or minimize hazards that have been newly identified or previously accepted.
- Lessons learned are briefed to management and recorded into the Lesson Learned Information System (LLIS). Prior to operations, review previous lessons and after operations record what was learned.

4.0 RELEVANT DOCUMENTS

The underlying goal of this procedure is shared by many supporting procedures at Dryden. In turn, this procedure supports [DHB-X-001](#), Airworthiness and Flight Safety Review (AFSRB), (Dryden) Flight Readiness Review (FRR), Mission Success Review (MSR), Technical Brief (TB), and Mini-Tec Brief (MTB) Guidelines by providing prime information needed to accomplish its goals. The Hazard Action Matrix and the Accepted Risk List are prime sources of information for the [DHB-X-001](#) processes.

- [DOP-S-032](#), Quality Assurance & Safety, Health, & Environmental Offices Review for All Types of Procurement Requests Including Credit Card Purchases, and [DCP-S-006](#), Quality Assurance Audits, are primary quality procedures that assure that processes are being used to preclude poor workmanship or low quality components.
- [DCP-S-004](#), System Safety Support, delineates the process for managing risk and system safety on Dryden projects.
- [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 preclude software interactions with hardware from creating mishaps. These procedures support this Hazard Management Procedure by providing “front line” sources of hazard mitigation.

4.1 Authority Documents

NPR 8715.3	NASA Safety Manual
NSTS 1700.7	Safety Policy and Requirements for Payloads
NPR 7120.5A	NASA Program and Project Management Processes and Requirements
NASA-STD-8719.7	Facility System Safety Guidebook
NASA-STD 8719.13A	Software Safety

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

DCP-X-008	Tech Brief (T/B) AND Mini-Tech Brief (MINI T/B)
DCP-X-009	Airworthiness and Flight Safety Review Process
DOP-S-006	Software Safety Job Instruction

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-004	System Safety Support
DCP-S-007	Software Assurance
DCP-S-046	Software Quality Assurance Audit Procedure
DHB-P-002	Project Manager's Handbook

4.3 Informational Documents

DHB-X-001	Airworthiness and Flight Safety Review, Independent Review, Mission Success Review, Technical Brief and Mini-Tech Brief Guidelines
---------------------------	--

4.4 Forms

DFRC 328-8	Hazard Report
D-WK 330-8	Risk Mitigation Worksheet
D-WK 331-8	Accepted Risk List
TEM-001a/b	Hazard Action Matrix

5.0 WAIVER AUTHORITY

Waivers granted to this procedure shall be documented in project documentation (e.g., System Safety Plan). Waivers should be submitted by the project or research lead during the formulation phase. The DFRC Office of Safety and Mission Assurance (OS&MA) will retain a copy of all official hazard risk management waivers.

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

- A. The Project Manager is responsible for ensuring waivers and variances to the content of the Dryden Hazard Management Procedure have been obtained.
- B. The 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 Director of Office of Safety and Mission Assurance and the Chief Engineer are the Independent Technical Authority (ITA) Board. The ITA Board has the approval authority for waivers and variances to the content of the Dryden Hazard Management Procedure.
- D. The Project Manager will assure that the official waiver or variance is properly filed and maintained with the project records.

6.0 ACRONYMS, & DEFINITIONS

6.1 Acronyms

AFSRB	Airworthiness and Flight Safety Review Board
ARL	Accepted Risk List
CCB	Configuration Control Board
CCR	Configuration Change Request
CDR	Critical Design Review
CFE	Contractor Furnished Equipment
CSFP	Critical Single Failure Point
DCP	Dryden Centerwide Procedure
DHB	Dryden Handbook
DIR	Dryden Independent Review
DoD	Department of Defense
ETA	Event Tree Analysis
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode and Effects Criticality Analysis
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
GFE	Government Furnished Equipment
GSE	Government Support Equipment
HA	Hazard Analysis
HAM	Hazard Action Matrix

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

HR	Hazard Report
ITA	Independent Technical Authority
LLIS	Lessons Learned Information System
MIL-STD	Military Standard
MOA	Memorandum of Agreement
NSTS	National Space Transportation System
O&SHA	Operating and Support Hazard Analysis
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PRA	Probability Risk Assessment
QA	Quality Assurance
RSO	Range Safety Officer
SCA	Sneak Circuit Analysis
SHA	System Hazard Analysis
SPF	Single Point Failure
SPP	Safety Program Plan
SSHA	Subsystem Hazard Analysis
SSP	System Safety Plan
SSS	Software System Safety
SSWG	System Safety Working Group
V&V	Validation & Verification

6.2 Definitions

Accepted Risk	A risk that 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.
Airworthy	The test vehicle operates 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.

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

Flight Safety	The test vehicle, support aircraft, all crewmembers, and uninvolved aircraft return from the test flight without injury or damage unless the mission is designed to expend the vehicle. The flight starts at launch or at brake release for takeoff and ends after landing when wheels stop. 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	A segment of ground safety that addresses the risks associated with the access to and operation of all facilities. This includes special support capabilities that are resident within these facilities.
Failure Tolerance	Capability of a system to perform in a <i>predictable</i> manner after a failure of specified hardware or software components.
Fail-Operational Ability	Capability of a system to perform in a <i>fully operational</i> 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 an unsafe act or condition. A hazard is the threat of harm. Mil-Std-882 D defines hazard as "Any real or potential condition that can cause injury, illness, or death to personnel; damage to or loss of equipment or property; or damage to the environment." The NASA Procedures and Guidelines (NPR) 8715.3 hazard definition is "A Hazard is an existing or potential condition (event), which can result in or contribute to a mishap."
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 Phase	A discrete functional period in the life cycle of a system. In the context of this procedure, this equates to an interval of

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

exposure to a potential mishap caused by a specific hazard.

Mission Rules Those rules that govern the unique project aspects of the planning and conduct of a mission operation. These rules shall include changes to limitations or procedures already established as part of NASA-Dryden or manufacturer-approved control and operating procedures. These rules will be categorized as Safety Critical Go/No-Go Criteria, Mission Critical Go/No-Go Criteria, or Mission Go/No-Go Criteria.

Safety Critical Go/No-Go Criteria – A set of safety conditions that shall be satisfied before a mission operation may begin or continue. Failure to satisfy these conditions will result in a mission abort and if airborne, a return-to-base (RTB). If failure to satisfy all conditions results in a decision affecting continuation of a specific maneuver, actions will be taken to terminate or complete the maneuver consistent with the level of immediate risk.

Mission Critical Go/No-Go Criteria – A set of safety conditions that shall be satisfied before a specific test maneuver or condition can be attempted and/or continued. Failure to satisfy these conditions will prohibit or terminate these specific maneuvers or exclude attainment of conditions. If failure to satisfy all conditions results in a decision affecting termination of a specific maneuver, actions will be taken to terminate or complete the maneuver consistent with the level of immediate risk.

Mission Go/No-Go Criteria – A set of non-safety conditions that should be satisfied if a specific maneuver or attainment of condition is to meet a specific research objective.

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 No injury to the public or personnel and no damage to property on the ground or to uninvolved aircraft from the

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

test vehicle in the event of a mishap. Normally effected by ensuring that a vehicle will stay and/or land within the test range and ensuring that the collective expected casualties (E_C) stays less than 30 per million. 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.
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 independent 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 HAZARD MANAGEMENT

Historically, the Dryden approach to Hazard Management has been to tailor industry, government, and NASA Headquarters accepted processes (including Mil Spec and NASA Handbooks) that are relevant, practical, and efficient. Because of the variety of aerospace programs at Dryden, projects may have varied risk baselines. The level of analysis should be commensurate with the overall risk profile as determined by project safety issues, complexity, and size. The application of the processes in this procedure establishes a graduated severity/probability matrix. Projects with relatively little risk will require a modest amount of effort to document that fact. Projects with significant risk are able to identify hazards early in the design process and either design them out, provide for mitigation to an acceptable level of risk, or present them to Dryden management to become accepted risks.

In this context, the conduct of a project means from its beginning to its end. It is expected that every project conducted under Dryden purview will have a system safety plan that specifies the project's approach to hazard management. It is further expected that the project will review and make use of earlier, related lesson learned as well as contribute to the Lessons Learned Information System (LLIS). The goals of this procedure are to assure that the applied knowledge, intelligence, common sense, and diligence are key to the safe conduct of flight research missions at Dryden. These processes are used by Center Management as a measure of the risk that will be accepted for the conduct of a mission, and they assist a project team to continuously work to minimize mission risk. Responsibility for implementation of these processes rests with the Dryden Project Team, particularly the project team leads: the project manager, chief engineer, operational engineer, and system safety engineer. As the leader of the team, the Project Manager shall assure that these hazard management processes are appropriately integrated into project activities, and the team leads will assist in this effort.

Development plans and procurement contracts for project related hardware, software, or services should address hazards associated with deliverable items. Project Plans, Configuration Management Plans, and System Safety Plans shall provide an integrated documentation basis for these hazard management processes (e.g., establish a configuration control board, establish how the mitigation and verification actions are managed and tracked). Flight planning and briefings shall remain vigilant to risks associated with the mission. To assure that these processes are effective in maintaining safe operations, the entire Project Team, including the project pilot, the operations support team, and the technical disciplinary or subject matter experts, shall actively participate in the hazard management process.

The Hazard Management flowchart represents the highest level and intent of the Dryden Hazard Management Process. The project formulation stage (blocks 1 through 7) addresses to the conceptual phase of the project, where it is imperative to have early safety involvement so hazards may be mitigated by design when applicable, thereby,

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

saving time and expense. Blocks 8 through 18 address the formal process for hazard management by laying out eleven steps from identification through the documentation of any lessons learned during the process, as well as stressing the importance of communication and documentation throughout the process.

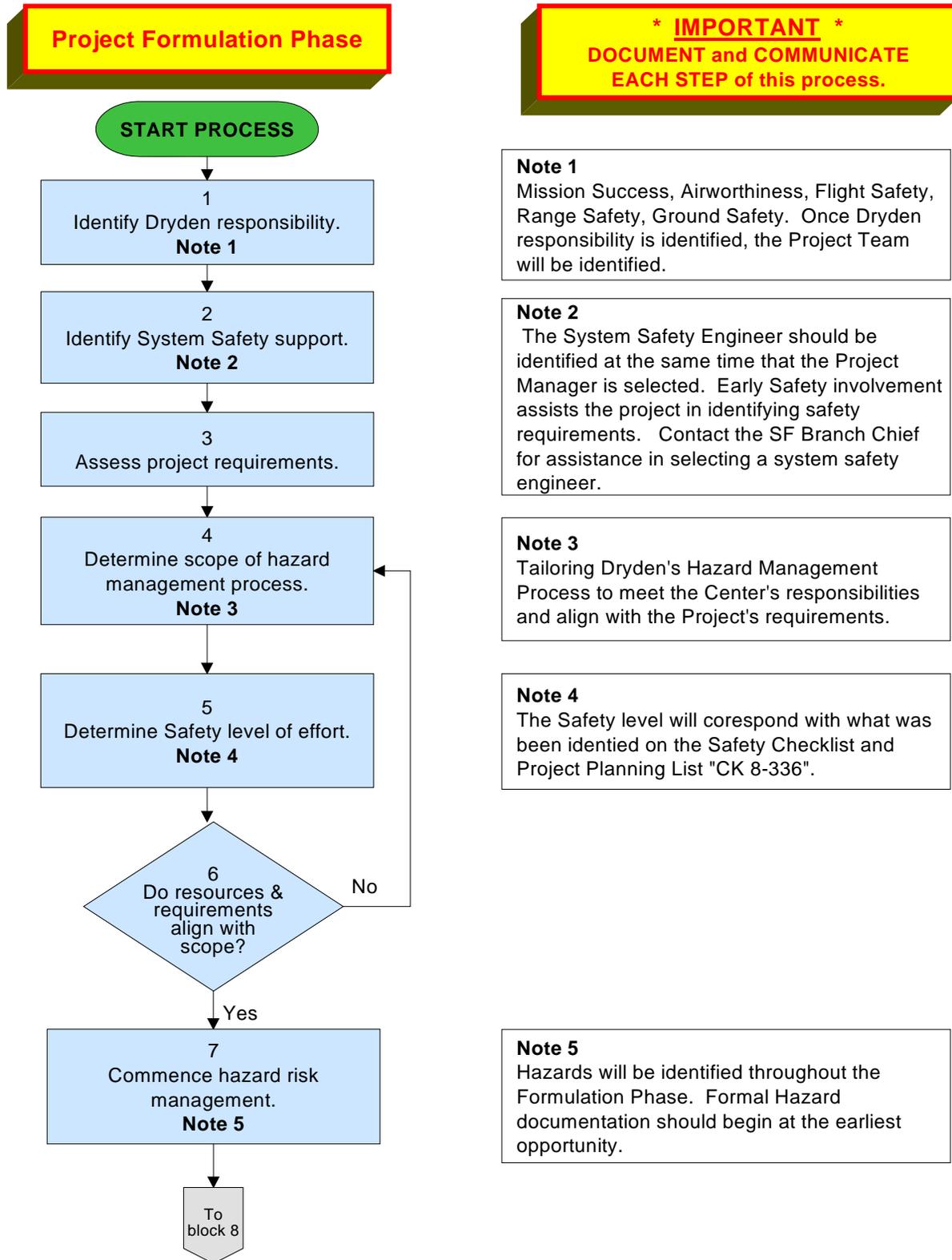
Four items constitute the foundation of this procedure:

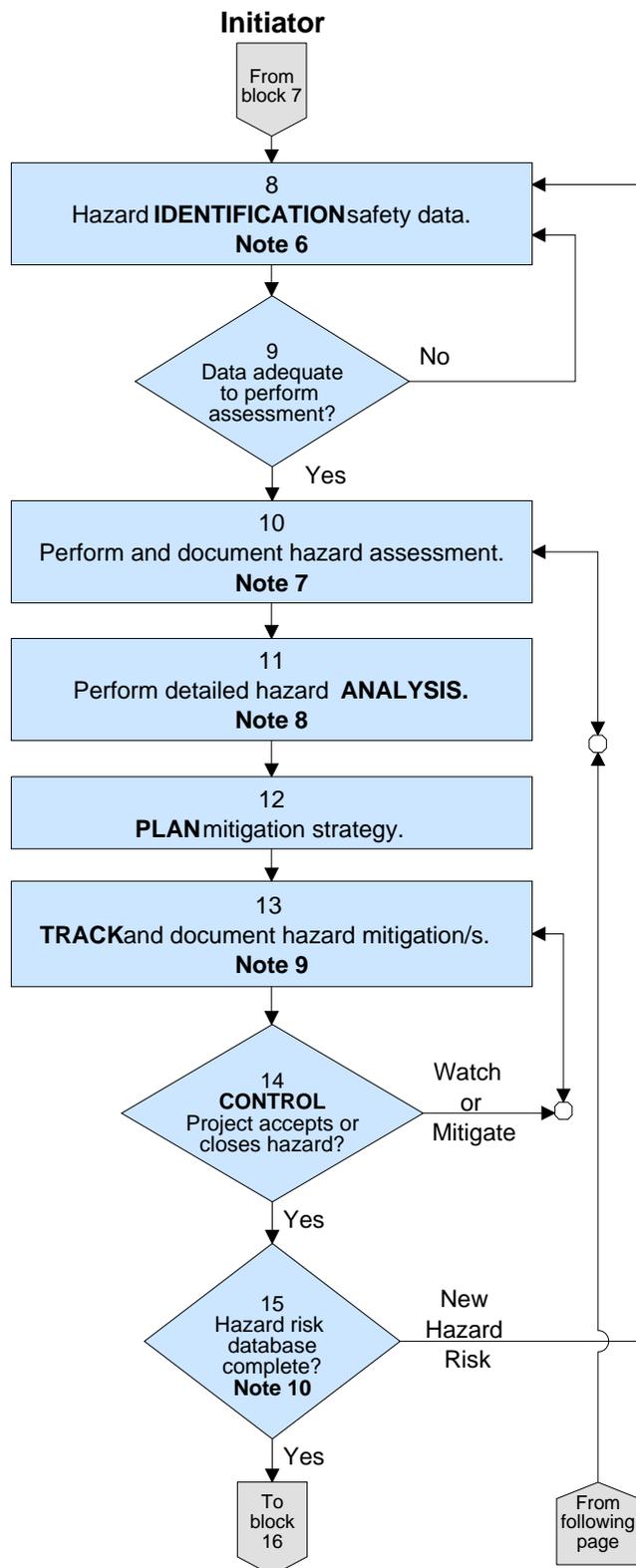
- Hazard Report form ([DFRC 328-8](#)) including instructions (Attachments A & B)
- Risk Mitigation Order of Precedence Worksheet ([D-WK 330-8](#)) including instructions (Attachment C)
- Hazard Action Matrix, [TEM-001a](#) and [TEM-001b](#), (Attachment D)
- Accepted Risk List ([D-WK 331-8](#)) (Attachment E).

This flowchart incorporates the fundamentals of continuous risk management: identify, analyze, plan, track, and control, each supporting the effort to properly document and communicate the hazards associated with the project's activities.

It is an objective of hazard management at DFRC to identify, and when possible, subsequently eliminate or mitigate all significant hazards. The System is only as good as what the project team puts into it in terms of skill, knowledge, intelligence, common sense, and diligence.

8.0 FLOWCHART





*** IMPORTANT ***
DOCUMENT and COMMUNICATE
EACH STEP of this process.

Note 6
 Hazard report statement condition and severity written up on DFRC Hazard Report [Form 8-328](#) or equivalent:

- Data from similar projects
- Safety design requirements
- Reliability analysis
- Failure modes
- Failure rates
- Critical items list
- Design specifications, drawings, & schematics
- Trade studies
- Operations scenarios
- Safety surveillance of operations & tests

Note 7
 Hazard attributes: Assess during Preliminary Hazard Analysis

- Probability, Severity, Timeline
- Classified and prioritized hazard risk list

Note 8
 Perform detailed hazard analysis

- System hazard analysis
- Subsystem hazard analysis
- Operating and support hazard analysis
- Supporting analysis

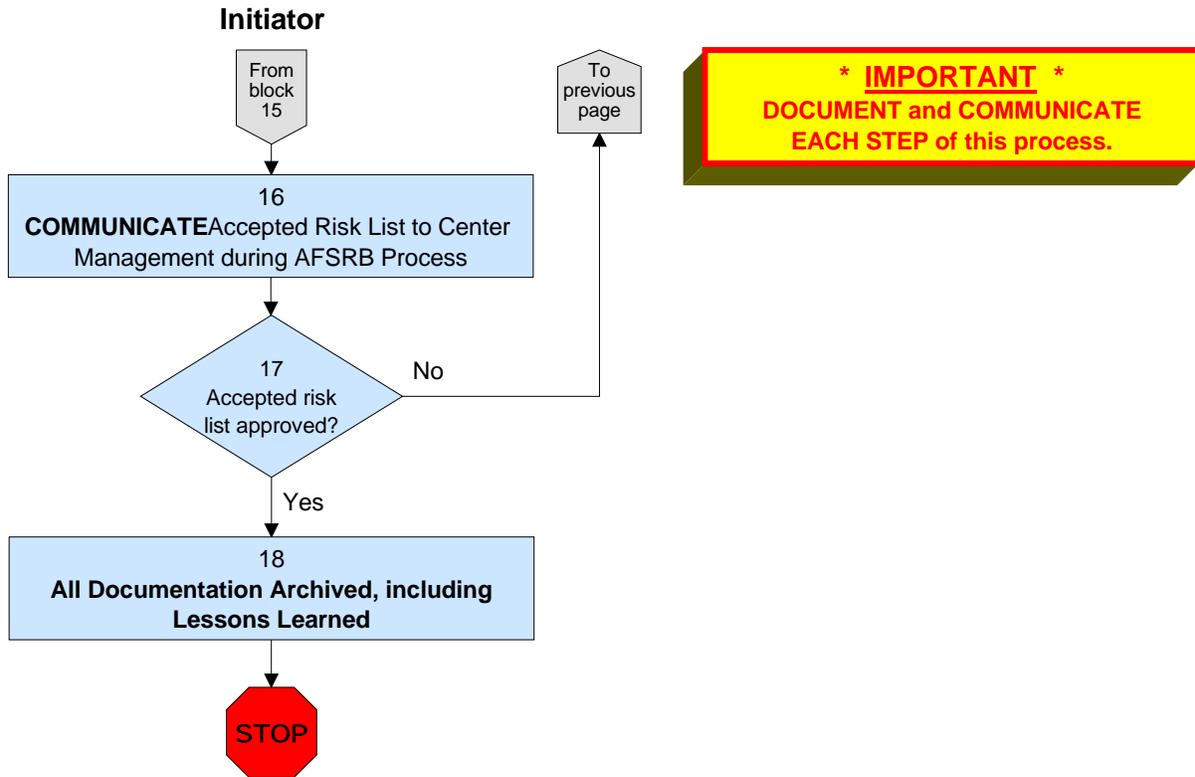
Note 9
 The Hazard Action Matrixes (HAMs) [TEM-001a and b](#) are used to determine which hazards go onto the Accepted Risk List (ARL) DFRC [Form 8-331](#).
 Mitigation Action - Accept, Watch, or Mitigate

- Develop action/verification plan
- Report hazard risk status
- Track hazard risk attributes
- Track action plan

Note 10

- Update database
- Determine next step
- Close hazard risk or
- Continue current plan or
- Make plan corrections or
- Invoke contingency plan
- Prepare to brief ARL to Center Management

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



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

9.0 HAZARD IDENTIFICATION AND RECORDING

9.1 Hazard Reports

The Hazard Report (HR) form is the primary tool used to document hazards. A compilation of these forms for all the identified hazards associated with a project serves as the primary documentation of the various hazard analyses. All identified hazards shall be evaluated for their severity and for the probability of occurrence. The potential mishap is the effect, or outcome, of the hazard. A hazard cause is the condition that contributes to the hazard. It could be unsafe design, environment factors, failure, human error, etc. Hazards should be described in a scenario that addresses the cause (source) and effect (outcome); or source, mechanism, and outcome (i.e., consequence) to characterize the potential harm of the hazard. Hazard controls are the measures that eliminate a hazard or reduce the probability of the hazard effect (outcome). If the Hazard controls change the severity (i.e., the consequence) of the hazard, then a new hazard shall be identified that addresses the new consequence (outcome).

Detailed instructions for completing the Hazard Report form are included as Attachment A. During the hazard identification process, it is important for the form to clearly describe the hazard, identify the condition or unsafe act followed by the worst-case consequence, its cause(s) and effect(s), and set an initial hazard category (Section 11.0, Risk Mitigation and Analysis). Given the forgoing information, the Hazard Report, form [DFRC 328-8](#), can proceed to the next phase of the System Safety Process. Typically, hazards are formally tracked through the project's System Safety Working Group (SSWG). In some cases, a CCB process may be used in place of or in conjunction with the SSWG to document and track hazards. In either case, the process to be utilized on each specific project should be part of the Configuration Management Plan ([DCP-P-016](#)).

Hazard Reports can be written by **anyone** at **anytime** during the conduct of a project. Many of the hazards associated with a project are identified early in the design and development phase through the use of formalized hazard analysis techniques. A Preliminary Hazard Analysis (PHA) shall be conducted to identify hazards at the projects Preliminary Design Review (PDR). Typically, the Subsystem Hazard Analysis (SSHA) and the System Hazard Analysis (SHA) will be reported at the project's Critical Design Review (CDR). The Operating and Support Hazard Analysis (O&SHA) will be reported prior to the projects Flight Readiness Review (FRR). These analyses will refine the PHA and identify additional hazards that become apparent as the understanding of a project's systems and

operational requirements mature. Additional hazard analysis techniques and tools are discussed in Section 11.0.

Usually, a project's Discrepancy Reporting (DR) system, [DCP-P-018](#), Discrepancy Report Process for Flight Project Critical Systems, is an on-going means of identifying problems that may be hazards. DRs shall be reviewed not only to ensure that they are corrected, but shall be compared with known hazards to ensure that any new hazards are identified. If a new hazard is identified, a Hazard Report shall be initiated.

Customarily, the vehicle contractor will do the analysis and correct and control identified hazards prior to the delivery of the vehicle or test article. The results of the hazard analysis must be presented at the various design reviews. A copy of all analyses must be part of the aircraft deliverables and should be merged into the Dryden format for the hazards reports and the Hazard Action Matrix. Hazard identification, analysis, and reporting do not terminate at delivery.

The hazard analysis process, like the entire safety process, must be an on-going, active, "living" process if it is to function correctly. Through the life of the program, analysis must constantly be reviewed for currency and accuracy. This is especially important since Dryden's flight vehicles, due to the nature of flight research programs, are continually undergoing configuration changes.

9.2 Tailoring of the Hazard Report Form

Each hazard identified through the hazard analysis process shall be reported using a Hazard Report (HR) form. The standard form, [DFRC 328-8](#) is available at Dryden Forms Online. Code SF, the Flight Assurance Branch, has developed and maintains an automated Hazard Report Database. Access to this automated system is available through the project's assigned system safety engineer. Coordination of the automated system safety database with the more traditional CCB hazard report tracking process will be maintained. The assigned system safety engineer and the project's configuration control administrator will share the responsibility for this coordination. If necessary to meet unique project needs, the HR form may be tailored by contacting the Dryden Forms Manager to create a project-specific form compatible with the automated tracking process. Tailored forms not compatible with the automated tracking process and database format will require the project's SSWG/CCB to internally control the hazard report process, ensuring the required fields from the HR can be transferred to a database. In all cases where a non-standard Hazard Report form is used, the project shall specify which procedures will be used in the System Safety Plan and shall brief the Independent Technical Authority Director agent of the ITA Board

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

early in the project to gain variance and/or approval for the process to be used. The ITA Director shall gain concurrence from the ITA Board prior to endorsing. Any areas where participating organizations have different definitions of hazard report or approval requirements should be clearly understood and explained in the System Safety Plan.

10.0 HAZARD CLASSIFICATION

Many methods have been developed to quantify the probability of the risk associated with the potential severity of a hazard and its probability of occurrence. DFRC has adopted a method tailored after the NASA Safety Manual, NPR 8715.3.

10.1 General Guidance

This procedure is published to provide each project with a tool that will facilitate their implementation of the Hazard Risk Management process. Risk management is a PROJECT responsibility. Because of the nature of flight research activities, most of the hazards that shall be assessed for both severity and probability will deal with one-of-a-kind aerospace vehicles operating in short-term projects during which very few flight hours will be accrued. Because of this, data about components supplied by vendors or project contractors (both failure data and calculated reliability numbers) should be utilized with caution, and the project shall consider whether or not that data needs be modified to make it fit their project. The project SHALL NOT simply take numbers given to them and plug them into the Hazard Action Matrix to see where they fit. Serious thought and sound judgment shall be utilized in the application of the Hazard Risk Management process. When making qualitative assessments, ensure the controls that are in place are assessed and documented for likelihood of occurrence in accordance with the defined program system safety plan and that clear rationale is used in documenting the justification of the classification of the hazard category.

10.2 Hazard Action Matrix

There are two Dryden Residual Risk Hazard Action Matrixes (HAMs) (Attachment D) that have been developed to serve as the primary safety hazard management classification process. The purpose of these templates are to relate human safety hazards, loss of high-dollar value assets, and/or loss of mission in terms of the hazard's severity with its probability in order to identify the associated overall hazard risk. The Hazard Action Matrixes identify the level of management approval required for actual acceptance of risks (Accepted Risks) by the shaded areas on the HAMs. The Hazard Action Matrixes Instructions reflect the accepted Dryden wording for hazard probability estimations and severity classifications of mishap occurrence as is describe in the following

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

sections. Projects should not change the substance of the HAM presentation if it is planned for use as part of a Dryden Airworthiness Process. Final hazard classifications should be added to the matrix only after the project or program has exhausted ALL possible corrective and controlling actions utilizing the Risk Mitigation Procedures of Section 11.0, Hazard Mitigation and Analysis.

10.3 Hazard Probability

The probability estimations are derived from NPR 8715.3, "NASA Safety Manual". "Probability is the likelihood that an identified hazard will result in a mishap, based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and affected population." The probability is based on the scope and duration of the risk being assessed and presented to Center Management. The probability estimation [Pr] requires quantification (analysis/calculated), or a qualitative assessment can be utilized with appropriate justification (clear rationale) for the assessment. When probabilistic risk assessment methods (quantification) are used, list the numerical probability of occurrence for this cause. When qualitative risk assessment methods are used, the controls that are in place shall be assessed and documented for likelihood of occurrence in accordance with the defined program system safety plan (shall have clear rationale/justification).

HAMs Probability [Pr] Estimations

A: Expected to Occur

- Likely to Occur Immediately on the order of ($Pr > 10^{-1}$)
- Expected to occur often in the life of the program/item. Expected to be experienced continuously in on-going programs.

B: Probable to Occur

- Probably will occur on the order of ($10^{-1} > Pr > 10^{-2}$)
- Will occur several times in the life of a program/item.

C: Likely to Occur

- May occur on the order of ($10^{-2} > Pr > 10^{-3}$)
- Likely to occur sometime in the life of a program/item, but multiple occurrences are unlikely. Controls have significant limitations or uncertainties.

D: Unlikely to Occur

- Unlikely but possible to occur on the order of ($10^{-3} > Pr > 10^{-6}$)
- Unlikely to occur in the life of the program/item, but still possible. Controls have minor limitations or uncertainties.

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

E: Improbable to Occur

- Improbable to occur on the order of ($10^{-6} > Pr$)
- Occurrence theoretically possible, but such an occurrence is far outside the operational envelope. Typically robust hardware, operational safeguards, and/or strong controls are put in place with mitigation actions to reduce risk from a higher level to an improbable state (probability E)

10.4 Hazard Severity

Severity can be broken out into personal injury or loss of asset/mission. Personal injury can be broadened to include death, disability, illness, and several categorizations of injury, life threatening, lost-time, minor, etc. Loss of asset/mission can be broadened to include loss of system, substantial system damage, minor system damage, property damage, and loss or compromise of mission (incomplete mission success).

The project is responsible for identifying “Loss of Mission” and Mission Success Criteria. This gives the project risk practitioner a basis for loss of mission/mission success risk assessment and will support management assessment of project risk. Abort, Return to Base (RTB), and test shutdown are often primary mitigating actions that may preclude a higher level event (e.g., Category I or II). The Loss of Mission (Category III severity on the HAM) is typically the loss of one particular sortie, flight, ground test, or the like. It is accepted that “Loss of Mission” may be a fairly common occurrence in flight research activities because we are here to discover what works and what doesn’t. However, we must be accountable by determining the consequences for “Loss of Mission” which may be expressed in cost to the project. In research flight testing you may expect to experience several “Loss of Missions” in order to achieve “Mission Success”. It is the combination of the events you have direct control over (Mission Success) and the events beyond your direct ability to control (Mission Assurance) that determine the ultimate success of the program.

Severity estimations are derived from NPR 8715.3, “NASA Safety Manual”. Severity is an assessment of the worst potential consequence, defined by degree of injury, property damage, or the cost of an unforeseen event (loss of mission), which could occur. The severity and probability estimations are required so management will have some measure of risk to assess the overall hazard risk of the project. The number and cost of the vehicles/test articles and the length of the project/exposure (number of cycles/flight hours, affected population, test location, etc.) shall be considered when establishing hazard categories.

Human Safety Hazard Severity Classifications

CLASS I (CATASTROPHIC)

- A condition that may cause death or permanently disabling/life-threatening injury, or loss of crew.

CLASS II (CRITICAL)

- A condition that may cause severe/lost time injury or occupational illness.

CLASS III (MINOR)

- A condition that may cause medical treatment for a minor injury or occupational illness (no lost time).

CLASS IV (NEGLIGIBLE)

- A condition that could cause the need for minor first aid treatment (though would not adversely affect personal safety or health).

Loss of Asset/Mission Hazard/Risk Severity Classifications

CLASS I (CATASTROPHIC)

- A condition that may cause the destruction of facility on the ground, major system, vehicle, termination of project, or loss of the only opportunity for critical data. Recovery/replacement cost equal to or greater than \$1M.

CLASS II (CRITICAL)

- A condition that may cause major loss/damage to facility, system, equipment, flight hardware, vehicle, long term project delay, or loss of major project critical data. Recovery/replacement cost equal to or greater than \$250K, but less than \$1M.

CLASS III (MODERATE)

- A condition that may cause loss of mission (sortie, flight, return-to-base, test shut-down, etc.), loss of minor project critical data, minor loss/damage to facility, system, equipment, or flight hardware. Recovery/replacement cost equal to or greater than \$25K, but less than \$250K.

CLASS IV (NEGLIGIBLE)

- A condition that may cause loss of non-critical data, subject's facility, system, or equipment to more than normal wear and tear. Recovery/replacement cost less than \$25K.

10.5 Failure Tolerance

The DFRC adopts NPR 8715.3, Section 1.8 as the failure tolerance policy for aerospace vehicles. Redundancy requirements specified therein are considered highly desirable design criteria. However, because of the nature of the work done at Dryden (research, development, and test of one-of-a-kind-items), redundancy is not always achieved. Therefore, the requirements specified herein will establish the acceptable levels of risk.

All subsystem-level Single Point Failures (SPFs) and critical operations associated with hazard category I or II failures and within this procedure will be identified as early as possible, but not later than the Critical Design Review. Prior to the Critical Design Review, a probability of failure will be substantiated for each subsystem not meeting redundancy standards specified in NPR 8715.3. All safety and/or mission assurance critical operations will have inhibits as specified in NPR 8715.3 as part of the design. All significant safety and mission assurance SPFs (not including items such as engines and wings, or pilots) and a credible analytical assessment of their probability of failure that have residual risk will be presented at the AFSRB and reviewed at all Tech Briefs. Probabilities presented will be quantified when practical rather than exploiting the qualitative assessment. Failure Modes and Effect Analysis and/or Fault Tree Analysis, discussed in Section 11.0, Hazard Mitigation and Analysis, are tools for facilitating the detection of SPFs.

10.6 Residual Risk Reporting

The Hazard Action Matrixes (HAMs) (Attachment D) map the residual risks that are required to be reported. The solid red shaded areas on the HAM are regarded as “Primary Risk Areas” and, as a matter of policy, will not normally be accepted at the Center level. The red cross-hatched areas on the HAM are regarded as “Accepted Risk Areas” and as such require acceptance and approval as “Accepted Risks” by Center Director with appropriate rationale. The white areas on the HAM are the hazard/residual risk areas for which the Project/Project Management has resources and methodology to manage all corrective and mitigating actions using project approved hazard management plans. Hazards/residual risks in this area are not “Accepted Risks” in that they do not require Center-level acceptance and approval.

Template [TEM-001a](#): Residual risk levels in the Primary Risk Areas, as a matter of policy, will not normally be accepted at the Center level and must be further mitigated. In event that human safety hazard falls within the Primary Risk Area after reasonable mitigations have occurred, and cannot be mitigated further, acceptance will normally require a higher authority

than the Center for approval. If such approval is granted, these hazards will constitute "Accepted Risks".

Template [TEM-001b](#): Residual risk levels in the Primary Risk Areas, as a matter of policy, will not normally be accepted at the Center level and must be further mitigated. In event that loss of asset/mission (mission success) hazard falls within the Primary Risk Area after reasonable mitigations have occurred, and cannot be mitigated further, it may be accepted by the Center Director with appropriate rationale. If such approval is granted, these hazards/residual risks will constitute "Accepted Risks".

Reporting a hazard on the HAM is a proactive process of communication that gives senior management a clear understanding of hazard risk status of the project. All hazards that fall on each HAM shall be reported to senior management.

10.7 Accepted Risk

Establish a formal, closed loop, risk acceptance process to identify and track program hazards with residual risk. Ensure residual risks are accepted in writing. The format for the Accepted Risk List is form [D-WK 331-8](#). (Attachment E). In all cases, where a decision is made to accept a risk, that decision will be coordinated with the governing SMA organization and communicated to the next higher level of management for review. Reporting the accepted risks to the Center Director, the Safety & Mission Assurance (SMA) Director, and Chief Engineer is accomplished as part of the hazard management process. The Accepted Risk List

- Shall document all hazards that have been identified as accepted risks on the Hazard Action Matrix.
- Shall be presented at the AFSRB and every Tech Brief.
- Shall be presented for the Center Director's concurrence in the AFSRB findings Memorandum from the AFSRB Chair.

The AFSRB Chair shall retain a copy of the Memorandum as a record of the project's Accepted Risk.

10.8 Tailoring of the Hazard Action Matrix

The definitions of Probability, Categories, and Accepted Risks on the Dryden Hazard Action Matrix ([TEM-001a/b](#)) should satisfy the requirements of the majority of DFRC aerospace research projects. In some instances, however, projects may feel the need to tailor the matrix. These situations might include space access projects for which loss of mission-critical data might be seen as catastrophic. Another increasingly common situation is the one in which different organizations have been

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

assigned ground safety, range safety, flight safety, and mission success responsibilities. Other participants may use their own Hazard Action Matrix or convert the data into the Dryden format. In all cases of tailoring the Hazard Action Matrix, the project shall specify the procedures to be used in the System Safety Plan and shall brief the ITA Director agent of the ITA Board (S&MA Office Director and Chief Engineer (AFSRB Chair)) early in the project to gain (variance) approval for the process to be used. The ITA Director shall gain concurrence from the ITA Board prior to endorsing. Any areas where participating organizations have different definitions of Accepted Risk categories or approval requirements should be clearly understood and explained in the System Safety Plan. The most restrictive DFRC requirements will always apply to areas of DFRC responsibility.

11.0 HAZARD MITIGATION AND ANALYSIS

11.1 Hazard Mitigation

The Risk Mitigation Order of Precedence and a supporting worksheet are provided in Attachment C. In general, the order of precedence has been derived from experience that has shown time and again that eliminating a hazard is the most positive means of preventing it from causing a mishap. That same experience has shown that when special procedures are used to mitigate a hazard's risk, it is likely that the procedures may be misapplied and a mishap may occur, anyway. The order of preference is as follows:

- 1) Design to Eliminate the Hazard or to Minimize Risk (e.g., electrical fire eliminated by using a pneumatic system or using redundancy in flight controls to lower the probability of occurrence of flight control failure.)
- 2) Incorporate Safety Features and/or Safety Devices to Minimize Risk (e.g., safety lock-out or inhibit devices.)
- 3) Incorporate Warning/Caution/Detection Devices to Minimize Risk (e.g., flashing light with a sign to indicate that there is a radiation hazard present.)
- 4) Use Special Procedures/Training/Personal Protective Equipment to Minimize Risk (e.g., test procedures that contain warnings and precautions with regard to test being performed, high pressure training, ear plugs, safety glasses, gloves, and hard hats.)
- 5) Use of Placards to Minimize Risk (e.g., High Voltage label placed on a panel over a high voltage area with intent to prevent unqualified personnel from opening panel.)

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

Note: Many hazards may require a combination of these approaches to fully mitigate.

Attachment C provides a Risk Mitigation Worksheet ([D-WK 330-8](#)) that can be used to verify mitigations listed on the Hazard Report form.

11.2 Hazard Analysis

Advanced hazard analysis tools include the Fault Tree Analysis (FTA), Failure Modes and Effects Analysis (FMEA), Failure Modes and Effects Criticality Analysis (FMECA), Event Tree Analysis (ETA), Sneak Circuit Analysis (SCA), and Probabilistic Risk Assessment (PRA). One key aspect of many of these approaches is the development of a Systems Safety Working Group (SSWG) to ensure early involvement of system safety, discipline, and operations engineers, as well as pilots, when applicable. In addition, a SSWG provides early impetus for the system design engineers to identify the hazards associated with the design.

The FTA can model the failure of a single event or multiple failures that lead to a system failure. The FTA is a top down analysis versus the bottom up approach of the FMEA or event tree analysis. The FTA method identifies an undesirable event and the contributing elements (faults and/or conditions) that would precipitate it. The contributing elements are interconnected with the undesirable event using network paths through Boolean logic gates. The FTA is a potential source of analytical probabilities.

The FTA, or equivalent logic analyses, is preferred for evaluating the effects of ground and flight hardware and with software faults, interfaces, environmental conditions, and human error on the system. The top-level fault tree will be based on the top undesired event, "loss of vehicle and/or personnel during aerospace operations." The top-level fault tree will be developed in a manner that will identify program operational and mission phases as they relate to the top undesired event. The mission phase events will most probably be based on Preliminary Hazard Analyses. The top-level fault tree may also include other basic analyses such as Subsystem Hazard Analyses (SSHAs), Operating and Support Hazard Analyses (O&SHAs), and any other advanced reliability analyses (i.e., Failure Modes and Effects Analyses [FMEAs]) that will support the further development of the detailed trees.

The following basic steps are used to conduct FTA:

- Define the top event and/or system failure of interest.
- Define the physical and analytical boundaries.
- Define the treetop structure.

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

- Develop the path of failures for each branch to the logical initiating failure.

Once the fault tree has been developed to the desired degree of detail, the various paths can be evaluated to arrive at a probability of occurrence. Cut sets are combinations of component failures causing system failure (i.e., causing the top event of the tree). Minimal cut sets are the smallest combinations causing system failure. The technique is universally applicable to systems of all kinds, with the following ground rules:

- The undesirable system events that are to be analyzed/abated, and their contributors, need to be foreseen.
- Each of those undesirable system events shall be analyzed individually.

The Failure Modes and Effects Analysis (FMEA) is a bottoms-up systematic, inductive, methodical analysis performed to identify and document all identifiable failure modes at a prescribed level and to specify the resultant effect of the modes of failure. It is usually performed to identify Critical Single Failure Points (CSFPs) in hardware. In relation to formal hazard analyses, FMEA is a subsidiary analysis.

In many projects, the research vehicle contractor will conduct system safety analyses and correct and control identified hazards prior to the delivery of the vehicle or test article. The results of the hazard analyses should be presented at the various design reviews. A copy of all contractor analyses should be part of the contract deliverables. The project and/or program managers shall ensure that the contractors perform required hazard analyses to identify hazards and ensure their resolution. Hazard analyses shall address design and operational hazards associated with hardware, software, operations, and operational environments.

12.0 HAZARD MANAGEMENT AND TRACKING

12.1 Configuration Control

The Project Manager is responsible for tracking all hazards and putting a process in place that ensures that all mitigating actions are implemented. Typically, hazards are formally tracked through the project's System Safety Working Group (SSWG), which normally includes the project manager, pilot (if required), chief engineer, operations engineer, and the system safety engineer, as a minimum. In some cases, a CCB process may be used in place of or in conjunction with the SSWG to document and track hazards. In either case, the process to be utilized on each specific

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

project will support the System Safety Plan as it addresses hazard management and tracking. These plans should address how hazards are entered into the system, who reviews hazards, and the process used to determine if all required and/or appropriate mitigating actions have been identified and implemented. In many cases, the resolution of a hazard may require a change in configuration. If the configuration of a flight vehicle is changed to resolve a hazard, the configuration change process will be utilized. For projects utilizing a SSWG to track hazards, it shall be clearly identified in the Configuration Management Plan and the System Safety Plan as to how all the participants submit hazards, where the official HRs are kept, and how the interface with the project CCB works. The project may also elect to tailor the hazard report form to suit unique project needs. If a tailored hazard report form is not compatible with the automated tracking process and database format, then the project's SSWG/CCB shall internally control the hazard report process and the hazard report shall be placed into a format to allow the required fields from the HR to be transferred to a database.

12.2 Hazard Tracking

Hazards are documented and tracked using a hazard report form. As noted previously in Section 9.0, the project may use the standard Hazard Report form, [DFRC 328-8](#), or may tailor a project-specific form. Tailored forms shall be submitted to the Dryden Forms Manager to request a new form number. The System Safety Plan should detail which hazard form the project is using. Some DFRC projects use the Aircraft Documentation Control Office to generate and track HRs and other CCB forms, and some projects utilize unique documentation systems. The Configuration Management Plan should specify how the project-specific system handles hazard reports.

When all possible mitigating actions determined for a hazard have been implemented and verified, the HR shall be dispositioned as "Mitigated". Once an HR form is mitigated, the associated hazard shall be identified on the Hazard Action Matrix. The hazard classification of a mitigated hazard should be the classification AFTER all mitigating actions are complete (i.e., the final classification reflects the residual risk of the hazard). All applicable hazards for the project will be shown on the Hazard Action Matrix. The goal is to mitigate all hazards, prior to flight, to their lowest possible risk level. A hazard report can be "eliminated" if the hazard is found to no longer exist because of either redesign or discovery of improper analysis. The safety perspective is that "Eliminated" also means that any residual risk falls in the less than 10^{-9} chance of occurrence and there are data documented that backs this probability. All open hazards that are identified Category I or II, Probability (A) through (D), which are

“eliminated” between Tech Briefings shall be presented to Dryden management, along with the closing action, at the next Tech Brief.

12.3 Dryden Management Review

As part of the hazard management process, Dryden management shall be made aware of the hazards associated with any flight project.

In all cases, where a decision is made to accept a risk, that decision will be coordinated with the governing SMA organization and communicated to the next higher level of management for review. Reporting the accepted risks to the Center Director, the Safety & Mission Assurance (SMA) Director, and Chief Engineer is accomplished as part of the hazard management process. Dryden management shall be aware of the hazards associated with any project. Prior to the first flight of a research vehicle, a Hazard Action Matrixes ([TEM-001a/b](#)) charts and an Accepted Risk List ([D-WK 331-8](#)) shall be prepared by the project and presented to both the Flight Readiness Review (FRR) committee and the Airworthiness and Flight Safety Review Board (AFSRB). The project shall present their accepted risk to SMA Director and Chief Engineer directly and/or through FRR committee. The Accepted Risk List shall be presented for the Center Director’s concurrence in the AFSRB findings Memorandum from the AFSRB Chair, i.e., for all accepted risks. The AFSRB Chair shall retain a copy of the Memorandum as a record of the project’s Accepted Risk. During the duration of the flight program, the Accepted Risk List shall be presented at each subsequent Tech Brief. The Accepted Risk presentation should include:

- A clear statement of all Accepted Risks with titles, effects, and the residual risk level and probability.
- A very brief discussion on how the residual risk levels were derived for all Accepted Risks. They should be presented in the order of preferred mitigation types, i.e., design, safety devices, warning devices, procedures/training, and/or placards.
- A depiction of the Accepted Risks and remaining residual hazards based on phase of project. The Hazard Action Matrixes presentations are the accepted method for this. Separate Hazard Action Matrixes should be presented for multiple phases of operations (e.g., ground, range, captive carry, flight, etc.), if appropriate.
- An assessment of probability of achieving the technical objectives from the test/test block being briefed.

Mission Success is defined as those activities performed in line and under the control of the program or project that are necessary to provide assurance that the program or project will achieve its objectives. The

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

Project Plan will define quantifiable (e.g., using a percent as a base of measurement) mission success and partial mission success (if applicable) and the specific accomplishments that need to be met for each. In addition, the project will define mission failure with respect to not achieving the above success criteria. The overall mission success activities will typically include risk assessments, system safety engineering, reliability analysis, quality assurance, electronic and mechanical parts control, software validation, failure reporting and resolution, complexity scaling factors (see Note 1 below), and other activities that are normally part of a program or project work structure. The projects shall perform an overall mission success risk assessment with the tailored definitions for likelihood and consequence for mission success. This assessment will consider the cumulative effect of the positive and negative influences of the projects. The mission success assessment must be made from the conception of the objectives through the completion (a continuous risk management process). Management reviews occur at different intervals and it will be expected for the project to report on the likelihood of mission success at each review.

Note 1 – The complexity scaling factors can include, but are not limited to, Design Heritage, Requirement Changes, Contractor Experience, Mission Design, Range, Total Thrust, Number of Engines, Structure Material, Existing Structure, Static Margin, Factors of Safety, Flight Controls, Landing Gear, Technological Challenges, and Other Influences, as necessary.

12.4 Exceptions

Dryden recognizes that the nature of flight-testing innovative, one-of-a-kind aerospace aeronautical vehicles often presses the “standard requirements” associated with flight-proven vehicles and technologies. Exceptions to the requirements presented throughout this procedure may be established during the formulation stage of the development of a project. Any such exceptions should be identified in the appropriate project documentation and shall be identified in the System Safety Plan. Approval of the exceptions will occur when the S&MA Director approves the System Safety Plan subsequent to being reviewed by the Flight Assurance Branch and the ITA Director. Any exceptions that affect the airworthiness process (e.g., the requirements for the HAM and how risk may be presented) shall require the approval of the Dryden Chief Engineer.

12.5 Lesson Learned

Each program and project shall document in its system safety plan, risk management plan or project plan how lessons learned are going to be

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

addressed for the project. The primary objective of documenting and reviewing lessons learned is to apply the knowledge gained from past experience to current and future projects in order to avoid the repetition of past failures and mishaps.

Each program and project shall review and apply significant lessons learned from the past at the conception of the project and throughout the program or project life cycle to ensure the appropriate steps are taken to avoid similar consequences. NASA's Lessons Learned Information System (LLIS) (<http://llis.gsfc.nasa.gov/>) should also be consulted prior to major milestones. In addition, throughout the project's life cycle, each project manager shall document and submit any significant lessons learned to the LLIS in a timely manner.

The lesson needs to be significant in that it has a real or assumed impact on operations; valid in that it is factually and technically correct; and applicable in that it identifies a specific design, process, or decision that reduces or eliminates the potential for failures and mishaps, or reinforces a positive result.

13.0 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., Preliminary Design Reviews, Critical Design Reviews, Technical Briefings, 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.

A second measurement of the success of this procedure is the amount of debris that falls outside the restricted areas or the amount of damage due to errant debris, in the event that an FTS is commanded or a UAV crashes outside of the restricted areas.

Trend analysis will be performed on the following metrics:

- 1) Compliance: Number, frequency, and severity of non-conformance reports and findings resulting from audits and review boards.
- 2) Functionality: Number of failures during testing and redesign requests due to functionality problems.

Trends will be determined from the following metrics:

- 1) Mission failures due to unidentified hazards
- 2) Failures due to unidentified root causes or hazard mitigations

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

NCRs resulting from annual Internal Assessment and External Assessment are an indicator of the performance of this procedure.

Trend analysis of the root cause(s) of those non-conformances will be performed with the intent to continually improve the procedure.

In the event of a mishap, trend analysis of the root cause of investigation findings will be utilized in a similar manner.

14.0 MANAGEMENT RECORDS & RECORDS RETENTION

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

Although generated by a 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](#)) 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](#)).

Attachment A: Sample Hazard Report Form



National Aeronautics and
 Space Administration
 Dryden Flight Research Center

HAZARD REPORT (HR)

Page _____ of _____

<u>Project</u>	<u>Originator</u>	<u>Site</u>	<u>HR Short Title</u>		<u>Phase</u>	<u>Date</u>	<u>HR No.</u>
<u>Sub-System</u>	<u>CI No.</u>	<u>Related Documents</u>	<u>ID No.</u>	<u>Assigned To</u>	<u>Human Safety Category</u>	<u>Loss of Assets/Mission Category</u>	
<u>Hazard Description</u>							
<u>Hazard Cause(s) (Source, Contributing Factors)</u>							
<u>Hazard Effect(s) (Outcome, Potential Mishap)</u>							
PLANNED HAZARD MITIGATION ACTIONS (CONTROLS/VERIFICATIONS)							
Mitigation Number:		<input type="checkbox"/> Complete		<input type="checkbox"/> Repetitive			
Mitigation Title:							
Mitigation Description:		<input type="checkbox"/> Mitigation Types: <input type="checkbox"/> Design <input type="checkbox"/> Safety Devices <input type="checkbox"/> Warnings <input type="checkbox"/> Procedures/Training <input type="checkbox"/> Placards <input type="checkbox"/> Other					
Verification Description:		<input type="checkbox"/> Verification Methods: <input type="checkbox"/> Inspection <input type="checkbox"/> Demonstration <input type="checkbox"/> Verification of Records <input type="checkbox"/> Analysis <input type="checkbox"/> Test <input type="checkbox"/> Other					
Assigned To:		Dated Last Modified:		Date Completed:			
Notes		Continue additional Mitigation Actions on Continuation Sheet					
FINAL HAZARD CATEGORY JUSTIFICATION STATEMENTS							
Final Severity Justification							
Final Probability Justification							
CONFIGURATION CONTROL BOARD (CCB)/SYSTEM SAFETY WORKING GROUP (SSWG) ACTIONS							
<input type="checkbox"/> Pilot (Signature Required) <input type="checkbox"/> Open (Valid HR with pending mitigation)		Remarks					
<u>Orig./ Sys Safety Rep. Signature</u>	<u>Date</u>	<u>CCB/SSWG Chair Signature</u>	<u>Date</u>	<u>Pilot/Project Signature</u>	<u>Date</u>		
FINAL DISPOSITION							
<input type="checkbox"/> Mitigated (Risk reduction actions closed/completed)		<input type="checkbox"/> Accepted Risk (Residual risk requiring CD approval)		<input type="checkbox"/> Eliminated		Final HS Cat.:	Final LA/M Cat.:
Planned Mitigation Actions Completed <input type="checkbox"/> (if not, state why):							
<u>SS Rep/ CCB/SSWG Chair Sign.</u>	<u>Date</u>	<u>Closing Authority/Project Sign.</u>	<u>Date</u>	<u>Pilot/Project Signature</u>	<u>Date</u>		

DFRC 328-8

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

HAZARD REPORT (HR) Continuation Sheet

Page ____ of ____

<u>Project</u>	<u>Originator</u>	<u>Site</u>	<u>HR Short Title</u>	<u>Phase</u>	<u>Date</u>	<u>HR No.</u>
(Use for any HR field that requires additional space) <div style="position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); opacity: 0.1; font-size: 100px; font-weight: bold; pointer-events: none;"> SAMPLE </div>						
RISK MITIGATION SUMMARY						
Design Features:						
Safety Features/Devices:						
Warning/Cautions/Detection Devices						
Procedures/Training/Personal Protection Equipment						
Placards						

DFRC 328-8

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

Attachment B: Hazard Report Field Instructions

HR FIELD	EXPLANATION / EXAMPLES
Project	Enter official project title.
Originator	Enter name of person writing the original HR.
Site	Enter the location of the flight ops, ground test, lab, facility, etc. that this HR applies to.
HR Short Title	Enter a title short and use the "Hazard Description" box for further explanation. Short Titles should be in the format of "effect: cause". For example, Fire: Fuel Leak, or Structure Fail: Landing Gear Collapse. Definition from NPR8715.3, NASA Safety Manual: A hazard is an existing or potential condition that can result in or contribute to a mishap.
Phase	If this project has more than one phase, input the name of the phase that this HR applies to. The HR shall apply only to the phase listed. Phases (Ground, Taxi, Captive Carry, Range, Flight, etc.) provide scope and hazard clarification.
Date	Enter date of origination or current update. Changing the date each time the HR is updated allows you to control the latest version of the HR.
HR No.	In most cases, the SSWG/CCB will assign a unique number to each HR. When a SSWG/CCB is not used, the System Safety engineer or the Project Manager may assign the HR number.
Sub-System	Enter name of the relevant vehicle sub-system most affected by this HR.
CI No.	Systems or sub-systems may be assigned a "Configuration Item" number, if applicable. This numbering system is normally detailed in the Project Plan or the Configuration Management Plan.
Related Documents	List any procedure, discrepancy report number, related hazard report, etc. that provides more detail of this potential hazard, if applicable.
ID No.	List the vehicle tail number, equipment model and/or serial number, or other unique identifier, if applicable.
Assigned To	Enter the persons name assigned primary responsibility for the HR mitigation.
Current Hazard Human Safety (HS) and Loss of Asset/Mission (LAM) Category	The initial hazard category shall be entered by the CCB or SSWG and confirmed by the Project Manager and/or CCB Chairperson when the HR is opened based on the mitigations in place and the corresponding letter/number combination derived from the Hazard Action Matrix (TEM-001a & TEM-001b). Current hazard category (normally presented at PDR, CDR, AFSRB, and/or Tech Brief on the Hazard Action Matrix) will be the letter/number combination derived after each mitigation action has been completed until all mitigations are addressed. The CCB/SSWG/Project Manager will enter the current Hazard Category as category changes to HS and/or LAM box.
Hazard Description	This is an expansion on the "HR Short Title". State, in detail, the unsafe act or condition that creates the associated risk and any other pertinent information. Include the mechanism by which the hazard manifests the final effect.
Hazard Cause(s)	Enter the condition that contributes to the hazard. It could be unsafe design, environment factors, failure, human error, etc. Hazards should be described in a scenario that addresses the Cause (Source). List all credible causes for this hazard and identify them separately (e.g., by letter A, B, C, etc.).
Hazard Effects(s)	The potential mishap is the effect of the hazard or Outcome. List each credible effect of this hazard.
Planned Hazard Mitigation Actions	The CCB Chairperson, SSWG Chairperson, or Project Manager will enter this information. List each planned action, even if not completed. As each action is completed, the "Assigned To" person shall list the drawing, document, safety component, procedure, training course, etc. after each statement that verifies the mitigation. Procedural and training mitigations need to identify who is responsible for ensuring the procedure is followed and training, including reoccurring training, is completed as well as how this tasking is going to be accomplished. Number each mitigation statement.
Final Severity Justification	Using the Hazard Action Matrix (TEM-001) as reference, explain in more detail the worst credible severity associated with the residual risk of this hazard after mitigations are completed with appropriate clear rationale for the assessment.

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

Final Probability Justification	Using the Hazard Action Matrix (TEM-001) as reference, explain in more detail the highest credible probability associated with the residual risk of this hazard after mitigations are completed. Supporting data shall be quantification (analysis/calculated) or a qualitative assessment can be utilized with appropriate clear rationale for the assessment.
Open	The CCB/SSWG Chairperson/Project Manager shall mark this box when the HR is officially opened. Until then, it is considered a "Draft" document.
Remarks	The CCB/SSWG/ Chairperson/Project Manager shall enter the appropriate information here. Often, this box is used to enter status information, reminders, or an explanation as to why an HR was not considered credible (and not opened). HRs that are not opened should not be discarded, but kept with the project records for reference.
HR Originator, CCB/SSWG Chairperson, and Pilot/Project Signatures	In some cases, the project does not have a "Project Pilot" (i.e., lab tests, ground tests, etc.). In these cases, the Project Manager, Lead Engineer, or other delegated authority may sign. For example, the project may delegate sign-off of ground Hazard Reports to the Operations Engineer or Crew Chief as the delegated authority for ground safety risks. HR opening authority signature requirements shall be identified in either the Project Plan or the System Safety Plan. Opening signatures signify concurrence with the credibility and validity of the HR. Enter the date signed.
Mitigated	The CCB/SSWG Chairperson/Project Manager shall check this box when the HR is officially mitigated and all appropriate risk reduction actions have been completed and verified.
Accepted Risk	Accepted risk is based on the final hazard category (see the project's Hazard Action Matrix for accepted risk categories). The CCB/SSWG Chairperson/Project Manager shall check this box if the HR shall be added to the Accepted Risk List (D-WK 331-8).
Eliminated	The CCB/SSWG Chairperson/Project Manager shall check this box when the HR is officially eliminated (e.g., design change eliminates hazard, HR combined with another HR, found not to be a credible/valid hazard, etc.) The safety perspective is that "Eliminated" also means that any residual risk falls in the less than 10^{-9} chance of occurrence or the hazard has been eliminated by completely removing the hazard causal factors.
Final Hazard HS and/or LAM Category	This is the letter/number combination derived from the Hazard Action Matrix (TEM-001) normally found in the project's System Safety Plan or in DCP-S-002. The CCB/SSWG/Project Manager will enter the Final Hazard HS and/or LAM Category after all mitigation actions have been completed.
Planned Mitigation Actions Completed	Check this box if all planned mitigation actions are completed or explain the reason for each one that is not completed.
CCB/SSWG Chair, Other Closing Authority, and Pilot/Project Signatures	In some cases, the project does not have a "Project Pilot" (i.e., lab tests, ground tests, etc.). In these cases, the Project Manager, Lead Engineer, or other delegated authority may sign. For example, the project may delegate sign-off of ground Hazard Reports to the Operations Engineer or Crew Chief as the delegated authority for ground safety risks. HR closing authority signature requirements shall be identified in either the Project Plan or the System Safety Plan. Closing signatures signify concurrence with the final disposition of the HR. Enter the date signed.
Risk Mitigation Summary	This area was provided for the user to track each mitigation by the order of precedence so it can be accessed where emphases in mitigation actions lay (e.g., Design, Safety Devices, Warning Devices, Procedures/Training, and Placards).

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

Attachment C: Risk Mitigation Order of Precedence Worksheet

RISK MITIGATION WORKSHEET

PROJECT: _____ DATE: _____

HAZARD REPORT NO: _____ COMPLETED BY: _____

HAZARD REPORT TITLE: _____

HAZARD CONTROLS BY RISK MITIGATION ORDER OF PRECEDENCE

1. Design to Eliminate the Hazard or to Minimize Risk:

➤ Hardware:

➤ Software:

2. Incorporate Safety Features/Safety Devices:

3. Warning/Caution/Detection Devices:

4. Procedures/Training/Personal Protective Equipment:

5. Placards:

Remarks/Comments:

D-WK 330-8

Risk Mitigation Order of Precedence

Hazard: The presence of a potential risk situation caused by an unsafe act or condition.

The ultimate goal of a safety program is for developers to design systems that contain no hazards. However, since the nature of most complex systems makes it impossible or impractical to design them completely hazard-free, a successful safety program often provides a system design where there exist no hazards resulting in an unacceptable level of mishap risk. As hazard analyses are performed, hazards will be identified that will require resolution. The risk mitigation design order of precedence defines the order to be followed for satisfying safety requirements and reducing risks.

The Dryden hazard reduction order of precedence is as follows:

Design to Eliminate the Hazard or to Minimize the Risk: Hazards shall be eliminated by design, where possible. The first consideration in the design process is to eliminate elements that present risk. When possible, consider selecting “safe” components when designing systems that present high energy or high-pressure hazards to the system or personnel. “Safe” components are those that have a proven safety and reliability record. The safety perspective is that “Eliminated” also means that any residual risk falls in the less than 10^{-9} chance of occurrence and there are data documented that backs this probability.

The major goal throughout the design phase shall be to ensure inherent safety through the selection of appropriate design features as fail-operational/fail-safe combinations and appropriate safety factors. Damage control, containment, and isolation of potential hazards shall be included in design considerations.

Incorporate Safety Features/Safety Devices to Minimize the Risk: Known hazards that cannot be eliminated through design selection shall be reduced to an acceptable level through the use of appropriate safety devices as part of the system, subsystem, or equipment. When possible, provisions shall be made for periodic functional checks of safety devices.

Incorporate Warning/Caution/Detection Devices to Minimize the Risk: Where it is not possible to preclude the existence or occurrence of a known hazard, devices shall be employed for the timely detection of the hazardous condition and the generation of an adequate warning. Warning signals and their application shall be designed to minimize the probability of false/wrong signals or of improper personnel reaction to the signal. Caution and warning signals shall be standardized within like types of systems.

Develop/Utilize Special Procedures, Training, and Personal Protective Equipment (PPE) to Minimize the Risk: Where it is not possible to reduce the magnitude of existing or potential hazards through design, or the use of safety and warning devices, special procedures shall be developed to counter hazardous conditions for enhancement of ground and flight crew safety. Precautionary notations incorporated into operating procedures shall be standardized and placed immediately before the potentially hazardous step or operation. Tasks and activities deemed to be “Safety Critical” may require certification of personnel proficiency.

Incorporate Placards to Minimize the Risk: Where it is not possible to preclude the existence or occurrence of a known hazard, placards shall be employed for the timely detection of the hazardous condition and the generation of an adequate written advisory.

In the Dryden Hazard Report (DFRC 328-8) “Risk Mitigation” section, indicate how the Risk Mitigation Order of Precedence was applied by checking one or more of mitigation types boxes.

Ideally, training, procedures, placards, or other forms of written advisory shall not be the only risk reduction method used to mitigate Category I or II hazards.

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

Attachment D: Sample Hazard Action Matrix



National Aeronautics and
 Space Administration
 Dryden Flight Research Center

**Human Safety
 Hazard Action Matrix (HAM)
 Residual Risk**

	Probability [Pr] Estimations				
Injury Severity Classifications	A: Expected to occur (Pr > 10 ⁻¹)	B: Probable to occur (10 ⁻¹ ≥ Pr > 10 ⁻²)	C: Likely to occur (10 ⁻² ≥ Pr > 10 ⁻³)	D: Unlikely to occur (10 ⁻³ ≥ Pr > 10 ⁻⁶)	E: Improbable to occur (10 ⁻⁶ ≥ Pr)
I: Catastrophic					
II: Critical					
III: Minor					
IV: Negligible					
	DFRC Policy: Human Safety Primary Risks are NOT Accepted at the Center level. When considered, risk acceptance requires Center Director approval and will normally require higher authority approval. These are " Accepted Risks " only by exception.				
	Risk acceptance requires Center Director approval. These are " Accepted Risks ".				
	Risk acceptance requires Project Manager approval.				

TEM-001a (12/2004)

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



National Aeronautics and
 Space Administration
 Dryden Flight Research Center

Loss of Asset/Mission Hazard Action Matrix (HAM) *Residual Risk*

	Probability [Pr] Estimations				
Injury Severity Classifications	A: Expected to occur ($Pr > 10^{-1}$)	B: Probable to occur ($10^{-1} \geq Pr > 10^{-2}$)	C: Likely to occur ($10^{-2} \geq Pr > 10^{-3}$)	D: Unlikely to occur ($10^{-3} \geq Pr > 10^{-6}$)	E: Improbable to occur ($10^{-6} \geq Pr$)
I: Catastrophic					
II: Critical					
III: Minor					
IV: Negligible					
	DFRC Policy: Human Safety Primary Risks are NOT Accepted at the Center level. When considered, risk acceptance requires Center Director approval and will normally require higher authority approval. These are " Accepted Risks " only by exception.				
	Risk acceptance requires Center Director approval. These are " Accepted Risks ".				
	Risk acceptance requires Project Manager approval.				

TEM-001b

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

Dryden Residual Risk Hazard Action Matrixes (HAMs) Instructions

Hazard Action Matrix Introduction

There are two Dryden Residual Risk Hazard Action Matrixes (HAMs) that have been developed to serve as the primary safety hazard management classification process. The purpose of these templates are to relate human safety hazards on TEM-001a and, loss of asset/mission on TEM-001b in terms of the hazard's severity with its probability in order to identify the associated overall hazard risk. The Hazard Action Matrixes identify the level of management approval required for actual acceptance of risks (Accepted Risks) by the shaded areas on the HAMs. The hazard action matrixes instructions reflect the accepted Dryden wording for hazard probability estimations and severity classifications of mishap occurrence. Projects should not change the substance of the HAM presentation if it is planned for use as part of the Dryden Airworthiness Process.

Hazard Probability

The probability estimations are derived from NPR 8715.3, "NASA Safety Manual". "Probability is the likelihood that an identified hazard will result in a mishap, based on an assessment of such factors as location, exposure in terms of cycles or hours of operation, and affected population." The probability is based on the scope and duration of the risk being assessed and presented to Center Management. The probability estimation [Pr] requires quantification (analysis/calculated), or a qualitative assessment can be utilized with appropriate justification (clear rationale) for the assessment. When probabilistic risk assessment methods (quantification) are used, list the numerical probability of occurrence for this cause. When qualitative risk assessment methods are used, the controls that are in place shall be assessed and documented for likelihood of occurrence in accordance with the defined program system safety plan (shall have clear rationale/justification).

HAMs Probability [Pr] Estimations

A: Expected to Occur

- Likely to Occur Immediately on the order of ($Pr > 10^{-1}$)
- Expected to occur often in the life of the program/item. Expected to be experienced continuously in on-going programs.

B: Probable to Occur

- Probably will occur on the order of ($10^{-1} > Pr > 10^{-2}$)
- Will occur several times in the life of a program/item.

C: Likely to Occur

- May occur on the order of ($10^{-2} > Pr > 10^{-3}$)
- Likely to occur sometime in the life of a program/item, but multiple occurrences are unlikely. Controls have significant limitations or uncertainties.

D: Unlikely to Occur

- Unlikely but possible to occur on the order of ($10^{-3} > Pr > 10^{-6}$)
- Unlikely to occur in the life of the program/item, but still possible. Controls have minor limitations or uncertainties.

E: Improbable to Occur

- Improbable to occur on the order of ($10^{-6} > Pr$)
- Occurrence theoretically possible, but such an occurrence is far outside the operational envelope. Typically robust hardware, operational safeguards, and/or strong controls are put in place with mitigation actions to reduce risk from a higher level to an improbable state (probability E)

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

Hazard Severity Categories

Hazard Severity Categories

Severity can be broken out into personal injury or loss of asset/mission. Personal injury can be broadened to include death, disability, illness, and several categorizations of injury, life threatening, lost-time, minor, etc. Loss of asset/mission can be broadened to include loss of system, substantial system damage, minor system damage, property damage, and loss or compromise of mission (incomplete mission success).

The project is responsible for identifying “Loss of Mission” and Mission Success Criteria. This gives the project risk practitioner a basis for loss of mission/mission success risk assessment and will support management assessment of project risk. Abort, Return to Base (RTB), and test shutdown are often primary mitigating actions that may preclude a higher level event (e.g., Category I or II). The Loss of Mission (Category III severity on the HAM) is typically the loss of one particular sortie, flight, ground test, or the like. It is accepted that “Loss of Mission” may be a fairly common occurrence in flight research activities because we are here to discover what works and what doesn’t. However, we must be accountable by determining the consequences for “Loss of Mission” which may be expressed in cost to the project. In research flight testing you may expect to experience several “Loss of Missions” in order to achieve “Mission Success”. It is the combination of the events you have direct control over (Mission Success) and the events beyond your direct ability to control (Mission Assurance) that determine the ultimate success of the program.

Severity estimations are derived from NPR 8715.3, “NASA Safety Manual”. Severity is an assessment of the worst potential consequence, defined by degree of injury, property damage, or the cost of an unforeseen event (loss of mission), which could occur. The severity and probability estimations are required so management will have some measure of risk to assess the overall hazard risk of the project. The number and cost of the vehicles/test articles and the length of the project/exposure (number of cycles/flight hours, affected population, test location, etc.) shall be considered when establishing hazard categories.

Human Safety Hazard Severity Classifications

CLASS I (CATASTROPHIC)

- A condition that may cause death or permanently disabling/life-threatening injury, or loss of crew.

CLASS II (CRITICAL)

- A condition that may cause severe/lost time injury or occupational illness.

CLASS III (MINOR)

- A condition that may cause medical treatment for a minor injury or occupational illness (no lost time).

CLASS IV (NEGLIGIBLE)

- A condition that could cause the need for minor first aid treatment (though would not adversely affect personal safety or health).

Loss of Asset/Mission Hazard/Risk Severity Classifications

CLASS I (CATASTROPHIC)

- A condition that may cause the destruction of facility on the ground, major system, vehicle, termination of project, or loss of the only opportunity for critical data. Recovery/replacement cost equal to or greater than \$1M.

CLASS II (CRITICAL)

- A condition that may cause major loss/damage to facility, system, equipment, flight hardware, vehicle, long term project delay, or loss of major project critical data. Recovery/replacement cost equal to or greater than \$250K, but less than \$1M.

CLASS III (MODERATE)

- A condition that may cause loss of mission (sortie, flight, return-to-base, test shut-down, etc...), loss of minor project critical data, minor loss/damage to facility, system, equipment, or flight hardware. Recovery/replacement cost equal to or greater than \$25K, but less than \$250K.

CLASS IV (NEGLIGIBLE)

- A condition that may cause loss of non-critical data, subject’s facility, system, or equipment to more than normal wear and tear. Recovery/replacement cost less than \$25K.

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

Residual Risk Reporting

The Hazard Action Matrixes (HAMs) map the residual risks that are required to be reported. The solid red shaded areas on the HAM are regarded as “Primary Risk Areas” and, as a matter of policy, will not normally be accepted at the Center level. The red cross-hatched areas on the HAM are regarded as “Accepted Risk Areas” and as such require acceptance and approval as “Accepted Risks” by Center Director with appropriate rationale. The white areas on the HAM are the hazard/residual risk areas for which the Project/Project Management has resources and methodology to manage all corrective and mitigating actions using project approved hazard management plans. Hazards/residual risks in this area are not “Accepted Risks” in that they do not require Center-level acceptance and approval.

Template [TEM-001a](#): Residual risk levels in the Primary Risk Areas, as a matter of policy, will not normally be accepted at the Center level and must be further mitigated. In event that human safety hazard falls within the Primary Risk Area after reasonable mitigations have occurred, and cannot be mitigated further, acceptance will normally require a higher authority than the Center for approval. If such approval is granted, these hazards will constitute “Accepted Risks”.

Template [TEM-001b](#): Residual risk levels in the Primary Risk Areas, as a matter of policy, will not normally be accepted at the Center level and must be further mitigated. In event that loss of asset/mission (mission success) hazard falls within the Primary Risk Area after reasonable mitigations have occurred, and cannot be mitigated further, it may be accepted by the Center Director with appropriate rationale. If such approval is granted, these hazards/residual risks will constitute “Accepted Risks”.

Reporting a hazard on the HAM is a proactive process of communication that gives senior management a clear understanding of hazard risk status of the project. All hazards that fall on each HAM shall be reported to senior management.

Accepted Risk Reporting

Reporting of all accepted risk (RED/Red Cross-Hatched Areas of the HAM) hazards to the Center Director is mandatory.

In all cases, where a decision is made to accept a risk, that decision will be coordinated with the governing SMA organization and communicated to the next higher level of management for review. Reporting the accepted risks to the Center Director, the Safety & Mission Assurance (SMA) Director, and Chief Engineer is accomplished as part of the hazard management process. Dryden management shall be aware of the hazards associated with any project. Prior to the first flight of a research vehicle, a Hazard Action Matrixes ([TEM-001](#)) charts and an Accepted Risk List ([D-WK 331-8](#)) shall be prepared by the project and presented to both the Flight Readiness Review (FRR) committee and the Airworthiness and Flight Safety Review Board (AFSRB). The project shall present their accepted risk to SMA Director and Chief Engineer directly and/or through FRR committee. The Accepted Risk List shall be presented for the Center Director's concurrence in the AFSRB findings Memorandum from the AFSRB Chair, i.e., for all accepted risks. The AFSRB Chair shall retain a copy of the Memorandum as a record of the project's Accepted Risk. During the duration of the flight program, the Accepted Risk List shall be presented at each subsequent Tech Brief. The Accepted Risk presentation should include:

- A clear statement of all Accepted Risks with titles, effects, and the residual risk level and probability.
- A very brief discussion on how the residual risk levels were derived for all Accepted Risks. They should be presented in the order of preferred mitigation types, i.e., design, safety devices, warning devices, procedures/training, and/or placards.
- A depiction of the Accepted Risks and remaining residual hazards based on phase of project. The Hazard Action Matrixes presentations are the accepted method for this. Separate Hazard Action Matrixes should be presented for multiple phases of operations (e.g., ground, range, captive carry, flight, etc.), if appropriate.
- An assessment of probability of achieving the technical objectives from the test/test block being briefed.

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

Document History Log
IPP Review Date: October 2004

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		11-20-98		
Revision	A	02-02-99		Unknown. Not documented.
Revision	B	01-21-05	All	<ul style="list-style-type: none"> • Complete document update to relate how the Hazard Management Process has been improved. • Added flowchart for Hazard Management Process • Hazard Report (HR): Enhanced the determination and tracking of risk mitigations. Modified instructions for use. • Added Section 10.4, Added failure tolerance guidance with respect to redundancy hazard management. • Added Section 10.5, Residual Risk Reporting • Hazard Action Matrix (HAM): Moved human safety into separate HAM. Updated Severity and Probability categories to be more inline with NPRs, particularly for primary risk • Accepted Risk List (ARL): Added hazard category, mitigation actions, phases of project, and submission for management decision • Added Section 11.0, Mitigation and Hazard Analysis • Added Section 12.3, Dryden Management Review • Added Section 12.5, Lesson Learned • Added Waiver Authority, Metrics & Trend Analysis • Added Management Records & Records Retention
Admin Change	B-1	07-13-05	40	Replaced inaccurate Asset/Mission HAM with correct version.
Admin Change	B-2	01-28-08	All	<ul style="list-style-type: none"> • Added expiration date to header • Removed highlights and numbers from requirement statements • Removed reference to cancelled DHB-S-001 • Updated form numbers • Minor editorial changes

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