A-P-T RESEARCH, INC.
AN EMPLOYEE-OWNED COMPANY

Final Report

SYSTEM SAFETY METRICS METHOD FOR SPACE LAUNCH SYSTEMS

16 October 2018
Prepared for:
Federal Aviation Administration (FAA)
Office of Commercial Space Transportation (AST)
800 Independence Avenue SW, Washington, DC 20591

Prepared by:
A-P-T Research, Inc.
4950 Research Drive, Huntsville, Alabama USA 35805
Under subcontract to ACTA, Inc.
Doc. No. CDSP-FL004-18-00401

This page intentionally left blank.

PREFACE

This report was developed under contract to the Federal Aviation Administration (FAA) Office of Commercial Space Transportation (AST) to ACTA Inc. (Contract Number: DTFAWA-17-D-00050) and subcontract from ACTA Inc. to APT Research, Inc. (Contract Number SDTFAWA-17-D-00050-1). This document is the Final Report for Task Order 001-18-APT. The Statement of Work (SOW) for this task order is included in Appendix B.

CONTENTS

FIGURES

TABLES

APPENDICES

ACRONYMS

ATP	Acquisition and Technology Programs
AST	Office of Commercial Space Transportation
DSOC	Defense Safety Oversight Council
FAA	Federal Aviation Administration
SEAC	Safety Engineering & Analysis Center
SME	Subject Matter Expert
SOW	Statement of Work
SSMM	System Safety Metrics Method
SSMMSLS	System Safety Metrics Method for Space Launch Systems

This page intentionally left blank.

EXECUTIVE SUMMARY

This report describes an audit tool called the System Safety Metrics Method for Space Launch Systems (SSMMSLS). This audit tool is a tailored version of an earlier tool called the System Safety Metrics Method (SSMM). The SSMM was developed in 2006 through a series of workshops funded by the Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs (ATP) Task Force. These workshops brought together approximately 20 of the nation's system safety subject matter experts (SMEs) from a variety of industry, government, and academic backgrounds. At the conclusion of the workshops, the team developed a set of 39 queries (or questions) to be used to audit the "goodness" of a system safety program throughout its lifecycle.

The SSMMSLS is the next generation of this tool, developed under subcontract by the SEAC (Safety Engineering & Analysis Center) and funded by FAA AST. The SSMMSLS (with a set of 55 queries) encompasses requirements from the best standards relating to system safety aspects of space launch activities. These standards document best practices in system safety program development and execution as well as requirements for managing risk associated with launch and re-entry activities. In addition, the SSMMSLS contains enhancements and updates to the original queries based on new standards and publications available. The ideal application for the SSMMSLS is as an audit tool. The tool described in this report can not only be used for independent audit within a space launch licensing activity, it can also be used as an internal tool to assess and improve system safety.

The SSMMSLS also has applications in an alternative path to obtaining a space launch license. This alternative path, also developed by the SEAC, includes two phases.[1] The first phase is an audit using the SSMMSLS tool by SMEs to determine the level of maturity of the applicant's safety program. The second phase is the application of the "Safety Case Approach," which is widely used internationally. The Safety Case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensive, and valid case that a system is safe, for a given application in a given environment.[2]

I. BACKGROUND DISCUSSION

During the workshops to develop the SSMM, 20 System Safety SMEs from the armed services, academia, and industry collaborated to identify 155 indicators of a good system safety program. The SMEs then narrowed these indicators into a condensed set of 39 queries, which

[1] This work was funded under contract to APT by FAA AST. This alternative path is described in detail in CDSP-FL004-18-00402A New Path to Launch Licenses published by the SEAC. To obtain a copy e-mail info@apt-research.com.

[2] This Safety Case definition is from the U.K. Ministry of Defence (MOD) Standard 00-56, "Safety Management Requirements for Defence Systems."

covered six program elements: Program Initiation, Hazard Identification, Risk Assessment, Risk Reduction, Risk Acceptance, and Hazard Tracking. An overview of the System Safety Program Elements is shown in Figure 1.

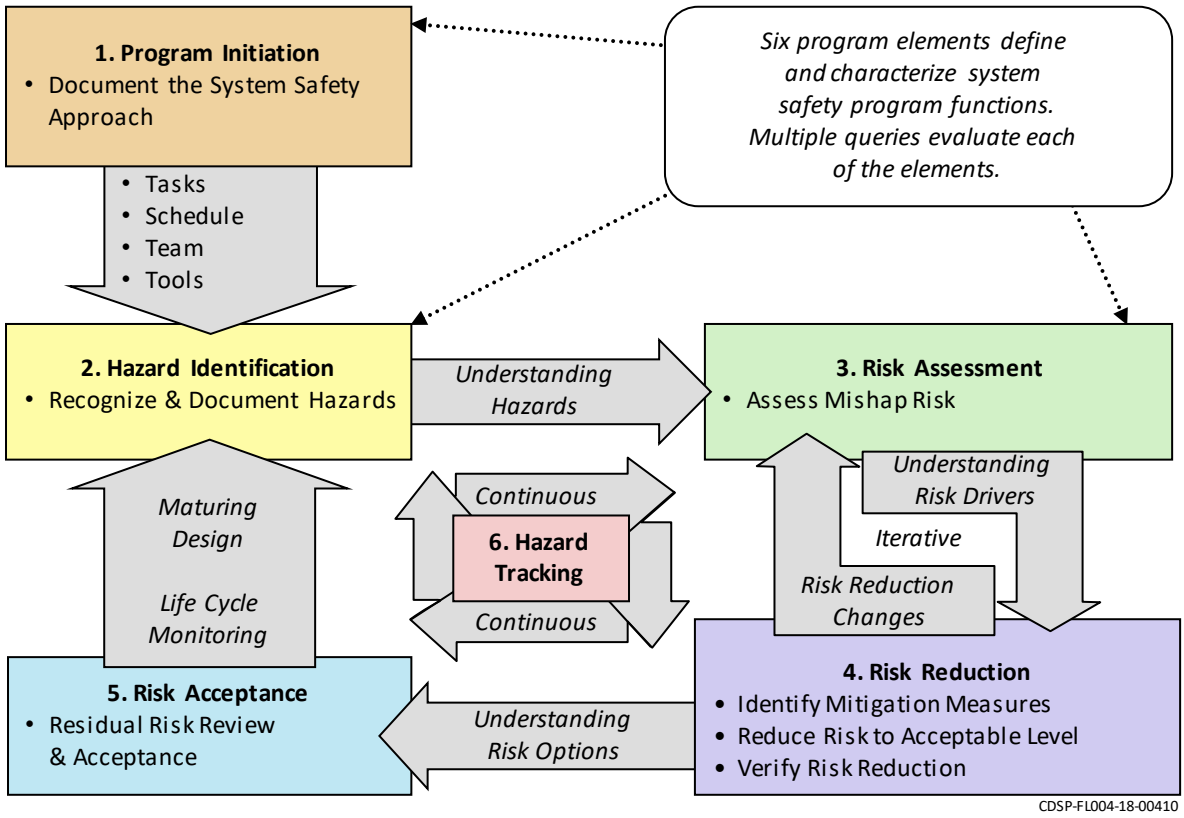


Figure 1: System Safety Program Elements

Each of the 39 queries were scored on a scale of 0-5 by an auditor and the averages were taken for each program element. The result was an overall program assessment. Interpretation of the results is self-explanatory and readily discernible. In the sample results illustrated in Figure 2, it is apparent that in order to improve the System Safety program, efforts should be devoted to improving the elements of Program Initiation and Hazard Tracking. Overall, the program evaluated is between a marginal and fair level.

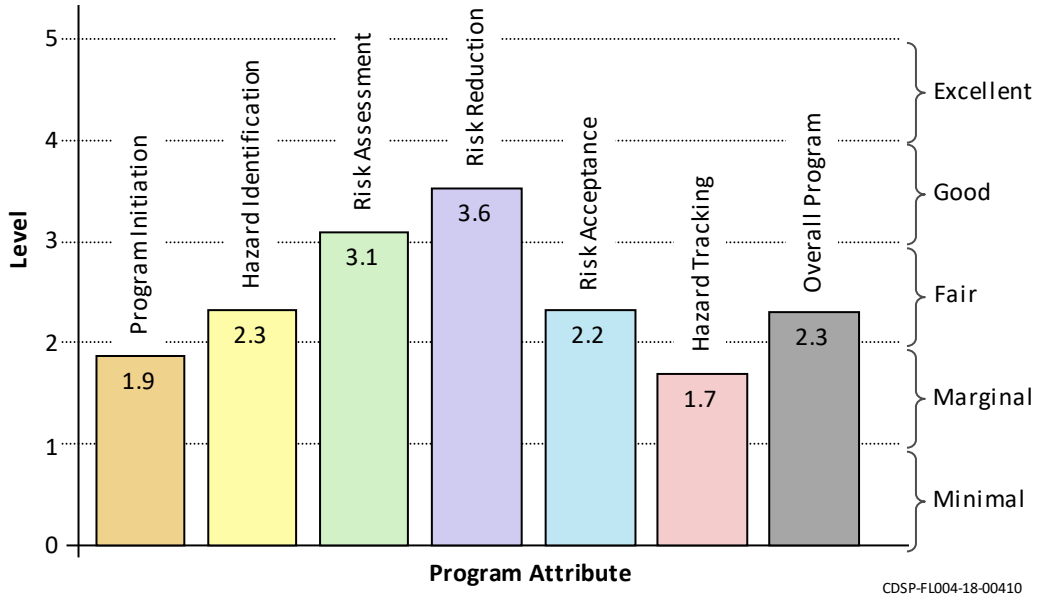
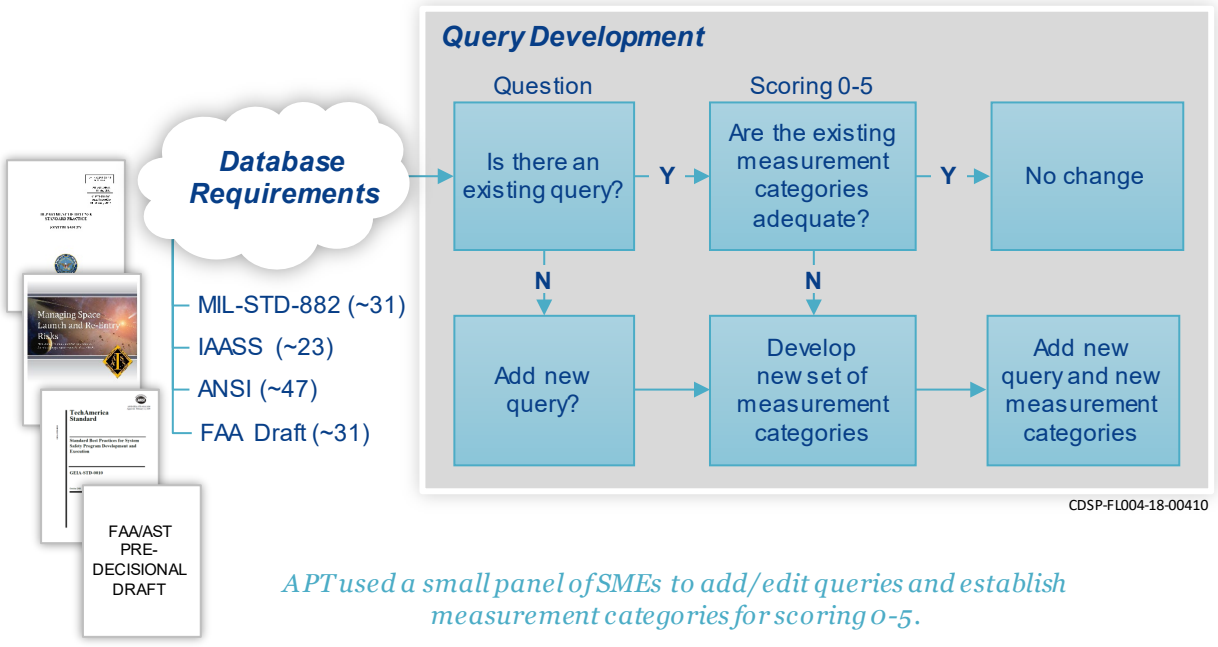


Figure 2: Sample Audit Results

Since that time, the SSMM has served as a useful tool to gauge the quality of a safety program throughout the lifecycle of the program. In 2018, APT was tasked by FAA AST to tailor the existing tool for space systems.

II. DEVELOPMENT PROCESS

An overview of the development process used to accomplish the task is shown in Figure 3.



APT used a small panel of SMEs to add/edit queries and establish measurement categories for scoring 0-5.

Figure 3: Development Process

The first step in tailoring the tool was to review existing documentation and place the requirements into a database. APT used a small group of SMEs to review the four documents and database the requirements.

Standard Best Practices for System Safety Program Development and Execution, GEIA-STD-0010 - This standard describes the best practices for applying system safety, the discipline of identifying and mitigating mishap risk encountered in the development, test, production, use, and disposal of systems, subsystems, equipment, and facilities. The G-48 System Safety Committee of the Information Technology Association of America, or ITAA (formerly GEIA), developed this document.

Department of Defense Standard Practice for System Safety, MIL-STD-882E - This system safety standard practice identifies the Department of Defense (DoD) Systems Engineering (SE) approach to eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated. This Standard covers hazards as they apply to systems / products / equipment / infrastructure (including both hardware and software) throughout design, development, test, production, use, and disposal.

Managing Space Launch and Re-Entry Risks – This paper was developed and published by the IAASS's (International Association for the Advancement of Space Safety) Launch and Re-entry Technical Committee. This paper describes the minimum recommended requirements for managing risk associated with launch and re-entry.

System Safety Draft Reg Text –

This is a draft document that was provided to APT by AST.

Each requirement was carefully evaluated to determine if the existing requirement was covered by one of the original 39 queries and if so, were the current measurement categories adequate. In some cases, only the measurement categories were edited, and in other cases new queries and measurement categories were developed.

III. THE SYSTEM SAFETY METRICS METHOD FOR SPACE LAUNCH SYSTEMS

The SSMMSLS consists of six program elements, a set of queries, detailed measurement categories for each query, and a method to tabulate the results.

1.0 Program Elements

The SSMMSLS includes six major program elements. They are:

1. Program Organization & Initiation
2. Hazard Identification & Tracking
3. Risk Assessment
4. Risk Reduction
5. Risk Acceptance
6. A Priori Standard

In the original tool, Hazard Identification and Hazard Tracking were considered separate elements. In tailoring, the tool for space systems these elements were combined into a single program element entitled “Hazard Identification & Tracking.” An additional program element “A Priori Standard” was also added. This element evaluates how the program meets the criteria associated with the collective risk to the public and the individual risk to the public.

2.0 Queries

The queries are grouped into six program elements. Table 1 list all the queries and identifies the program element to which that query belongs.

It should be noted that several of the six program elements can be adequately probed with only a few inquiry items, while others may require more. The goal was not to limit the number of queries associated with a specific program element, but to only include the number of queries necessary to adequately assess all aspects of the program element.

Table 1: Query Items

1 Program Organization & Initiation	2 Hazard Identification & Tracking	3 Risk Assessment	4 Risk Reduction	5 Risk Acceptance	6 A Priori Standard

#	Query	Program Element
1	How does system safety (including hardware, software, and human factors) manning allocation compare to actual needs?	1 Program Organization & Initiation

1 Program Organization & Initiation	2 Hazard Identification & Tracking	3 Risk Assessment	4 Risk Reduction	5 Risk Acceptance	6 A Priori Standard

#	Query	Program Element
2	Are the five program elements and functions recognized and integrated into an overall System Engineering (or Program Engineering) process (i.e., program initiation, hazard identification & tracking, risk assessment, risk reduction, & risk acceptance)?	1 Program Organization & Initiation
3	What authority does the system safety organization have?	1 Program Organization & Initiation
4	Which model best describes system safety organization structure and reporting level?	1 Program Organization & Initiation
5	Is management practice consistent with current standards?	1 Program Organization & Initiation
6	What level of regard prevails for the system safety program description documents (including hardware, software, and human factors)?	1 Program Organization & Initiation
7	Does the system safety program specifically address public safety associated with Hazardous Material Management, Environmental, Safety, and Occupational Health (ESOH) hazards?"	1 Program Organization & Initiation
8	How often, long-term average, has the program made system safety organizational/personnel changes?	1 Program Organization & Initiation
9	Are well-trained safety engineering personnel involved in the specification and design process? Do the design specifications reflect the impact of safety inputs?	1 Program Organization & Initiation
10	What level of training in system safety, risk management, & QRA (including hardware, software, and human factors) have you achieved?	1 Program Organization & Initiation
11	How many years of direct, full-time equivalent experience have you had in system safety, risk management, & QRA (including hardware, software, or human factors) practice?	1 Program Organization & Initiation
12	What applicable credentials do you hold?	1 Program Organization & Initiation
13	How would you characterize the system-specific knowledge of system safety staff members?	1 Program Organization & Initiation
14	How would you characterize organizational safety culture?	1 Program Organization & Initiation
15	How is the system safety program established and documented? How thorough is the System Safety Program Plan?	1 Program Organization & Initiation

1 Program Organization & Initiation	2 Hazard Identification & Tracking	3 Risk Assessment	4 Risk Reduction	5 Risk Acceptance	6 A Priori Standard

#	Query	Program Element
16	Is requirements tailoring applied? If so, at what level? What is the rationale for tailoring?	1 Program Organization & Initiation
17	Are the four desirable attributes (as defined in the ANSI STD) included in the safety program?	1 Program Organization & Initiation
18	What assets are protected by the system safety program?	2 Hazard Identification & Tracking
19	How are hazards identified?	2 Hazard Identification & Tracking
20	What hazard inventory-type analytical techniques are used?	2 Hazard Identification & Tracking
21	What logic tree analytical techniques are used?	2 Hazard Identification & Tracking
22	How are hazards understood by those working in the program?	2 Hazard Identification & Tracking
23	For software-intensive systems, how are the software personnel involved as contributors in identifying the hazards and mitigators?	2 Hazard Identification & Tracking
24	How is system safety practice linked to the “ilities” – e.g., Reliability, Availability, Maintainability?	2 Hazard Identification & Tracking
25	How are hazard tracking and safety requirement traceability implemented for system safety (including hardware, software, and human factors)?	2 Hazard Identification & Tracking
26	Are safety hazard data maintained up-to-date?	2 Hazard Identification & Tracking
27	Are explosives properly classified?	2 Hazard Identification & Tracking
28	Is risk managed at the hazard level (r) and the total system level (R)?	2 Hazard Identification & Tracking
29	How are hazards tracked? Is the SMO protocol used?	2 Hazard Identification & Tracking

1 Program Organization & Initiation	2 Hazard Identification & Tracking	3 Risk Assessment	4 Risk Reduction	5 Risk Acceptance	6 A Priori Standard

#	Query	Program Element
30	At what point in the system development cycle is a list of potential hazards defined?	2 Hazard Identification & Tracking
31	Has a comprehensive set of hazards been defined?	2 Hazard Identification & Tracking
32	Which hazard analysis techniques are used (PHA, FTA, FMECA, SHA, QRA, HHA, EHA, SAR etc.)? How are hazard analysis results tracked, recorded, documented, updated, and closed?	3 Risk Assessment
33	How is risk assessed for a single hazard that threatens multiple protected assets? Use clarifying example.	3 Risk Assessment
34	How is exposure interval selection made?	3 Risk Assessment
35	How is risk assessment matrix tailoring done?	3 Risk Assessment
36	Is analytical tool selection tailored to the needs of individual system peculiarities and needs?	3 Risk Assessment
37	How is the analysis of Government-off-the-Shelf (GOTS)/Non-Developmental-Items (NDI)/ Commercial-off-the-Shelf (COTS)/software reuse addressed in the system safety program (including hardware, software, and human factors)?	3 Risk Assessment
38	What analytical approach is used to assess risk?	3 Risk Assessment
39	A Software Criticality Index (SCI) is determined and used to guide the Level of Rigor (LOR) tasks or requirements?	3 Risk Assessment
40	Are range safety systems that are designed to reduce risk also evaluated to ensure they do not increase risk? Are they reliable? Do they balance alpha and beta errors? To what degree does the flight safety system demonstrate proof that it is reliable and balances both alpha and beta errors?	3 Risk Assessment
41	How is post-flight data used to validate pre-mission risk analysis?	3 Risk Assessment
42	In assessing risk, how is uncertainty addressed or characterized?	4 Risk Reduction
43	How is the hierarchy of mitigation precedence treated?	4 Risk Reduction
44	Are risk assessments quantified?	4 Risk Reduction
45	Are newly discovered hazards reported and mitigation plans formulated promptly?	4 Risk Reduction
46	How is the ALARP principle applied?	4 Risk Reduction
47	How are risk reductions verified and validated during the life cycle?	4 Risk Reduction
48	Are probability, severity, and exposure determinations made prior to and after mitigations?	4 Risk Reduction
49	How are system safety (including hardware, software, and human factors) analyses reviewed? (At what organizational level; with what thoroughness?)	5 Risk Acceptance
50	How are waivers, exceptions, and other non-compliances managed by the system safety program?	5 Risk Acceptance
51	How is acceptance of residual risk documented/reported?	5 Risk Acceptance

1 Program Organization & Initiation	2 Hazard Identification & Tracking	3 Risk Assessment	4 Risk Reduction	5 Risk Acceptance	6 A Priori Standard

#	Query	Program Element
52	How are risk tolerance limits selected for programs?	5 Risk Acceptance
53	What system safety risk summation practices are employed?	5 Risk Acceptance
54	Is the risk acceptance authority properly designated and does that authority always make the decision?	5 Risk Acceptance
55	How is compliance with the quantitative standard demonstrated?	6 *A priori* standard

3.0 Scoring Scale

Responses to the queries are to be scored against a generic scale to gauge the "goodness" of the program aspect covered by the query. The SSMMSLS is designed to be used for self-improvement as well as an audit tool. The generic scoring scale is shown here as Table 2.

Table 2. Generic Scoring Scale

Score	Descriptor
5	Excellent: Superlative in both concept and performance
4	Good: Satisfying all needs, in letter and in spirit
3	Fair: Satisfying most needs, but with one or a few notable flaws
2	Marginal: Failing to satisfy one or more key needs
1	Minimal: Present, but having little or no value to the Program
0	Null or Absent: Virtually non-existent/not practiced

A unique challenge of a such scale is the inherent subjectivity in assigning a score. Therefore, specific scoring scales are provided for every query in Appendix A, labeled as measurement categories. The measurement categories are intended to be used as guidance for the evaluator.

4.0 Tabulating the Results

To tabulate the results, query scores for each program element are averaged[3]. In some cases, a specific query may be judged as not applicable (N/A). In those cases, N/A scores are excluded from the program element's average. The final score for the audit is the average of the six program elements. Figure 4 shows a graphical illustration of a sample tabulation. In this case, scores for all queries are given equal weight in determining program element scores, and the program elements are weighted equally in determining the overall program score. Should it be desired by FAA AST, both query scores and program element scores could be assigned a weighted value.

[3] This is the mathematical mean using linear math.

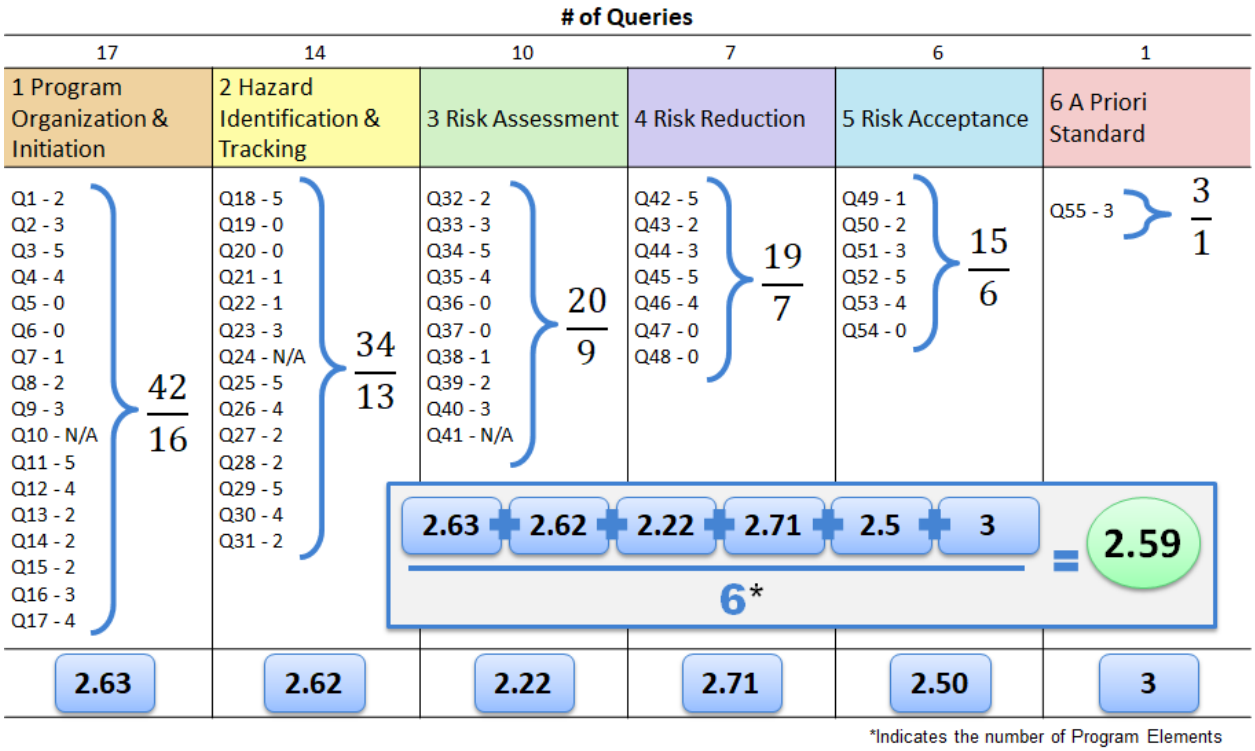


Figure 4: Sample Tabulation

5.0 Auditor Requirements

In the event that the SSMMSLS is used in the alternative path in obtaining a space launch license it is important that the individual(s) conducting the audit possess the correct qualifications, to limit scrutiny by industry. The following auditor education & experience qualifications are recommended.

- ***Experience:*** 20 years as a practicing system or range safety engineering professional
  - Prior program audits
- ***Education:*** Engineering, Science degree
  - 1-week auditor risk management course (as minimum)
  - Specialty education as needed for QRA, software safety, etc

Over time, the auditor pool can grow by having on-the-job auditor training. Initially the suggestion is made that every audit be a collaboration of at least two or more auditors.

5.1 Auditing Rules

The following is a list of suggested rules that should be followed when using the SSMMSLS as part of an alternative path in obtaining a space launch license.

1. Applicants are acquainted with the set of queries and invited to provide evidence to answer the question.

2. Before the initial audit, applicants are not provided the definitions of measurement categories. They may be provided with the source of the requirements.
3. If requested by the applicant, the audit may be conducted in two phases, with the first phase used as an audit preparation and improvement step.
4. Scores will be averaged in each element. Element scores will then be averaged for an overall score.
5. Some queries may not apply to the applicant's program. These queries will be excluded from the scoring and averaging.

IV. RECOMMENDATIONS / PATH AHEAD

1. Conduct a workshop with nationally recognized System Safety SMEs to review the SSMMSLS. A workshop would add value by increasing the pedigree. The product of the workshop would be an article that could be submitted to a peer-reviewed system safety journal.
2. Adopt the SSMMSLS as an audit tool to be used to calibrate the maturity of an applicant's system safety and risk management program.
3. Use the results of the audit as a metric of confidence in the safety solution offered by an applicant.
4. Define and develop a pool of SME auditors in accordance with the credentials defined in Section III.5.0.
5. Send qualified AST employees to auditor training in the use of the SSMMSLS.
6. Conduct a pathfinder demonstration with an actual license applicant to use the SSMMSLS to evaluate and improve their system safety program.

V. BIBLIOGRAPHY

"Standard Best Practices for System Safety Program Development and Execution," GEIA-STD-0010, SAE International, October 2008.

"Managing Space Launch and Re-Entry Risks", IAASS *Journal of Space Safety Engineering*, Volume 5, Issue 1, March 2018.

This page intentionally left blank.

APPENDIX A – THE SYSTEM SAFETY METRICS METHOD FOR SPACE LAUNCH SYSTEMS

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		1	
Query		How does system safety (including hardware, software, and human factors) manning allocation compare to actual needs?	
Measurement Categories	5	Level 4 + independent, 3rd party review of >5% samples, long-term average	
	4	Level 2 + 2nd level management or above	
	3	Level 2 + 1st level management (one group plus one manager)	
	2	Peer team (one group) or System Safety Working Group (SSWG)	
	1	Peer (1st level - one person)	
	0	None performed.	

Serial No.	PROGRAM ORGANIZATION & INITIATION	
	2	
Query	Are the five program elements and functions recognized and integrated into an overall System Engineering (or Program Engineering) process (i.e., program initiation, hazard identification & tracking, risk assessment, risk reduction, & risk acceptance)?	
Measurement Categories	5	All five are recognized, documented, and practiced.
	4	The fix discrete elements are practiced but without clear System Safety Program Plan (SSPP) documentation.
	3	Five elements recognized in program plan but poorly practiced (practice under-enforced or need under-appreciated).
	2	Some recognition apparent in program plan documentation, but five elements not fully practiced.
	1	Elements not documented in program plan; only a few elements recognized, and poorly practiced.
	0	The five elements are not recognized explicitly or in practice; no documentation specifies them as discrete program elements.

Requirements:

MIL-STD 882E

4.2: Identification and management of hazards and their associated risks

4.3.1: Document the system safety approach for managing hazards as an integral part of the SE process

4.3.1.a: Describing the risk management effort and how the program is integrating risk management into the SE process, the Integrated Product and Process Development process, and the overall program management structure.

4.3.8: Manage life-cycle risk

Task 102: Develop a System Safety Program Plan (SSPP) that documents the system safety methodology for the identification, classification, and mitigation of safety hazards as part of the overall Systems Engineering (SE) process

4.3.2: The hazard identification process shall consider the entire system life-cycle

ANSI STD

Section 4: This section prescribes the system safety program elements to be performed throughout the life cycle for any system. These guidelines are to ensure the identification and understanding of mishap hazards and their associated risks. The objective of system safety is to reduce mishap risk to an acceptable level (or alternatively as low as reasonably practical) through a systematic approach of hazard analysis, risk assessment, and risk management.

A.3.1: Element 1: Program initiation is the foundation of the safety program. It is important to establish the key elements and actions of the safety program in this element.

A.3.1.2: Plan a System Safety Program: The Developer should determine what system safety effort and specific tasks and activities are necessary to meet program and regulatory requirements.

A.3.1.3: System Safety Management Plan: This plan documents the Developer's approved system safety engineering and management approach

IAASS

2: establish a risk management framework

3: safety management program and processes should be established to identify, assess, reduce, and accept risks

3: It should include assigned responsibilities, a designation of risk acceptance authority, and other significant elements of the risk management program.

FAA Draft

- An operator must implement and document a system safety program throughout the complete operational lifecycle of the launch or reentry system
- An operator must establish procedures to evaluate the complete operational lifecycle of the launch or reentry system

Serial No.		PROGRAM ORGANIZATION & INITIATION
		3
Query		What authority does the system safety organization have?
Measurement Categories	5	"Must Change" and "Stop Work" authority documented and enforced.
	4	"Stop Work" or "Must Change" authority (in redesign), with evidence of application.
	3	Moderate design change authority, often overruled.
	2	Formal advisory.
	1	Observe and comment.
	0	None.

Requirements:

FAA Draft

- (e) Application requirements. An applicant must provide in its application the following: (1) A description of a safety organization, identifying the applicant's lines of communication and approval authority, both internally and externally, for all public safety decisions and the provision of public safety services; and (2) A summary of the processes and products identified in the system safety program requirements of § 450.xx.

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		4	**ANSI STD** 4: The PM should establish and maintain a system safety program to achieve the overall system safety objectives for the program. A.3.1.2.3: Establish a system safety organization or function and the required lines of communication with associated organizations
Query		Which model best describes system safety organization structure and reporting level?	**FAA Draft** • An operator must maintain and document a safety organization that has clearly defined lines of communication and approval authority for all public safety decisions. At a minimum, the safety organization must have the following positions: Mission director & Safety Official • Mission director. For each launch or reentry, an operator must designate a position responsible for the safe conduct of all licensed activities and authorized to provide final approval to proceed with licensed activities. The mission director must ensure that all of the flight safety official's concerns are addressed. • Safety Official. responsible for communicating potential safety issues and noncompliance issues to the mission director and authorized to examine (i) All aspects of the operator's ground safety operations and to independently monitor compliance with the operator's safety policies, safety procedures, and licensing requirements. This position, referred to as the ground safety official in this part, must have direct access to the mission director, who must ensure that all of the ground safety official's concerns are addressed. (ii) All aspects of the operator's flight safety operations and to independently monitor compliance with the operator's safety policies, safety procedures, and licensing requirements. This position, referred to as the flight safety official in this part, must have direct access to the mission director. • An operator must [document and implement] a system safety program that includes: (i) Methods to review and assess the validity of the preliminary safety assessment throughout the life of the operation, (ii) Methods for updating the preliminary safety assessment, and (iii) Methods for communicating and implementing the updates throughout the organization.
Measurement Categories	5	Staff organization reporting to general manager and/or program manager and has access to Integrated Product Teams (IPTs) (or equivalent).	
	4	Integrated with engineering and reporting to general manager.	
	3	Staff organization reporting to an engineering organization.	
	2	Staff organization reporting to an operations organization with regular informal communication with the engineering organization.	
	1	Staff organization reporting to an operations organization.	
	0	Staff organization reporting to Human Resources (HR) or other similar non-technical organization.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		5	
Query		Is management practice consistent with current standards?	
Measurement Categories	5	Management practice is fully consistent with applicable current standards; measures are in place to remain consistent and current.	
	4	Mostly consistent, with inconsistencies only in minor areas or during changes in standard version.	
	3	Regularly inconsistent in minor matters and occasionally inconsistent in key matters; widespread understanding of standards but lack of full enforcement.	
	2	Moderate inconsistency in key matters; lack of universal understanding/enforcement of standards.	
	1	Markedly inconsistent, with evidence of deliberate neglect or ignorance of applicable standards.	
	0	Entirely inconsistent, little or no understanding of applicable standards.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		6	**ANSI STD** A.3: Experience indicates that the degree of safety achieved in a system is directly dependent upon the emphasis given and the proper allocation of specific planning, requirements, analysis, testing, and verification tasks.
Query		What level of regard prevails for the system safety program description documents (including hardware, software, and human factors)?	**FAA Draft** • (a) An operator must implement and document a system safety process that identifies the hazards and assesses the risks to public health and safety and the safety of property arising from computing systems and software.
Measurement Categories	5	Program plan is a "Living Document," referred to frequently, updated as necessary, and used as a baseline guide to program operation.	
	4	Program plan is used as a guide in most program operations but needs updating.	
	3	Program plan exists, served to initiate program activities, but is no longer referred to or used to guide program operations.	
	2	Program plan is a "Dead Document," rarely referred to, and with many disregarded or outdated provisions.	
	1	If a program plan exists, practitioners are unacquainted with its provisions.	
	0	No program plan exists.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		7	**MIL-STD 882E** Task 108: Implement a Hazardous Materials Management Plan (HMMP) which shall be made available to the Government on request
Query		Does the system safety program specifically address public safety associated with Hazardous Material Management, Environmental, Safety, and Occupational Health (ESOH) hazards?"	
Measurement Categories	5	Hazards of occupational injury/illness and environmental hazards are recognized, and their risks assessed.	
	4	Hazards of occupational injury/illness and environmental hazards are usually recognized but their risks are often mis-assessed.	
	3	Hazards of occupational injury/illness and environmental hazards are usually recognized but only for hazards also threatening personnel or equipment.	
	2	ESOH hazards are moderately well recognized.	
	1	ESOH hazards are poorly recognized.	
	0	ESOH hazards are not recognized.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		8	
Query		How often, long-term average, has the program made system safety organizational/personnel changes?[4]	
Measurement Categories	5	Very rarely — less than once in four years.	
	4	Rarely — less than once in three years.	
	3	Occasionally — less than once in two years.	
	2	Often — about once in two years.	
	1	Frequently — about once a year.	
	0	Very often — more than twice a year.	

[4] For new programs, the spirit of this query needs to be applied by tailoring the measurement categories.

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		9	
Query		Are well-trained safety engineering personnel involved in the specification and design process? Do the design specifications reflect the impact of safety inputs?	
Measurement Categories	5	Designers are trained in system safety; immediate application of system safety principles is evident. Safety lessons learned considered.	
	4	Major influence in specifications and through practice of concurrent engineering or equivalent.	
	3	Influence through safety participation in determining specifications and in design reviews.	
	2	Influence through safety participation in infrequent design reviews.	
	1	Modest influence through inconsistent and infrequent design reviews.	
	0	Little or no evidence of influence on design.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		10	
Query		What level of training in system safety, risk management, & QRA (including hardware, software, and human factors) have you achieved?	
Measurement Categories	5	Level 3 + over 10 years domain knowledge.	
	4	Level 3 + five years applicable domain knowledge.	
	3	Level 1 + formal classroom training (≥30 classroom hours) specifically in system safety engineering, with CEUs or college credit.	
	2	Level 1 + formal classroom training (≥20 classroom hours) specifically in system safety engineering.	
	1	One year or more of on-the-job training (i.e., *not* one year of identical methodology/assignment).	
	0	No formal system safety training and less than 1 year of on-the-job training.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		11	
Query		How many years of direct, full-time equivalent experience have you had in system safety, risk management, & QRA (including hardware, software, or human factors) practice?	
Measurement Categories	5	>25 years direct experience in system safety or equivalent domain knowledge.	
	4	15-25 years direct experience in system safety or equivalent domain knowledge.	
	3	7-15 years direct experience in system safety or equivalent domain knowledge.	
	2	3-7 years direct experience in system safety or equivalent domain knowledge.	
	1	1-3 years direct experience in system safety or equivalent domain knowledge.	
	0	< 1-year direct experience in system safety or equivalent domain knowledge.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		12	
Query		What applicable credentials do you hold?	
Measurement Categories	5	Professional Engineer (PE) certification or advanced degree in engineering, physics, math, computer science, or related discipline + System Safety Society member (professional grade).	
	4	Level 3 + Certified Safety Professional (CSP) or Associate Safety Professional (ASP).	
	3	Level 2 + System Safety Society member (professional grade).	
	2	Bachelor of Science (BS) in engineering, physics, math, computer science, or related discipline.	
	1	High School diploma + specialized training in system safety (w/ certificate).	
	0	High school diploma or GED with no specialized training in system safety.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		13	
Query		How would you characterize the system-specific knowledge of system safety staff members?	
Measurement Categories	5	Full program knowledge; safety staff members have a well-developed understanding of the entire system and its requirements, general and specific.	
	4	A well-developed familiarity with the entire system and its requirements; capable of providing technical support in many system-specific areas.	
	3	Moderately developed familiarity with the entire system and its requirements; good understanding of selected system subparts.	
	2	Introductory familiarity with part of the system; moderate familiarity with some system specifics.	
	1	Introductory familiarity with part of the system; little or no familiarity with overall system specifics.	
	0	System knowledge poorly developed; personnel poorly informed or lacking in technical proficiency.	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		14	
Query		How would you characterize organizational safety culture?	
Measurement Categories	5	Demonstrated, full corporate involvement; system safety a highly esteemed part of any project.	
	4	Assigned management is knowledgeable and effective; system safety contributions are well-appreciated.	
	3	System safety considered a part of systems engineering or on a similar engineering level; management is moderately well-informed of the system safety role.	
	2	System safety is considered below engineering in importance or authority and is underappreciated, but performs notable function, though hampered.	
	1	System safety role is poorly defined /understood; engineers have negative bias toward system safety personnel and function.	
	0	Culture undeveloped or requirement not understood by program personnel; "system safety" function unrecognized or viewed negatively by many.	

Serial No.		PROGRAM ORGANIZATION & INITIATION
		15
Query		How is the system safety program established and documented? How thorough is the System Safety Program Plan?
Measurement Categories	5	A comprehensive Safety Program Plan (SSPP) including adequate system safety staff is fully executed by the top program executive before system design begins. Plan includes comprehensive risk management program and all elements
	4	Same as level 5, with minor shortfalls
	3	Same as level 5, with some noteworthy shortfalls
	2	Most elements of level 5 with some significant shortfalls
	1	The program consists only of the most hazardous procedures.
	0	No formal safety documentation, no full-time safety professionals.

Requirements:

ANSI STD

A.3.1.1: Define Program Authorizations and Charters: The Managing Authority(ies) should establish and execute system safety programs

A.3.1.1: Properly initiated programs should be formalized in documentation approved by the Managing Authority indicating the actions to be taken by the safety organization.

PROGRAM ORGANIZATION & INITIATION Requirements:

4.1.1: Program Initiation: The Managing Authority should document the approved system safety engineering approach and other actions needed to establish a fully functional system safety program

Task 101: Establish the foundation for a system safety program. The total system safety program consists of this task plus any other tasks from Sections 100, 200, 300, 400, or other source designated by the Managing Authority.

Task 102.1: The purpose of Task 102 is to develop a System Safety Program Plan (SSPP). It should describe, in detail, the tasks and activities of system safety management and system safety engineering that are required to identify, evaluate, and eliminate or control hazards, or reduce the associated risk to as low as reasonably practicable as determined by the Managing Authority throughout the system life-cycle.

IAASS

3: This program should be well documented and communicated to stakeholders.

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		16	**ANSI STD** A.3.1.2.1: Tailor the Program: Selective tailoring of a system safety program is necessary to effectively achieve all of the safety objectives within the constraints of performance, cost, schedule, and potential mishap loss
Query		Is requirements tailoring applied? If so, at what level? What is the rationale for tailoring?	
Measurement Categories	5	Tailoring is fully justified logical and strengthens the program without omitting requirements need for public safety.	
	4	Same as level 5, with incomplete justification	
	3	Valid tailoring is conducted, but not justified.	
	2	Partially valid tailoring is applied	
	1	Tailoring is needed but not used	
	0	Tailoring used to eliminate valid requirements or to cut corners (i.e., misued)	

Serial No.		PROGRAM ORGANIZATION & INITIATION	Requirements:
		17	**ANSI STD** A.3.1.6: Attributes of an effective system safety program include the following: 1) Management is always aware of the mishap risks associated with the system, and formally documents this awareness. Hazards associated with the system are identified, assessed, tracked, monitored, and the associated risks are either eliminated or mitigated to an acceptable level throughout the life cycle. Identify and archive those actions taken to eliminate or reduce mishap risk for tracking and lessons learned purposes; 2) Historical hazard and mishap data, including lessons learned from other systems, are considered and used; 3) Mishap risk resulting from harmful conditions (e.g., temperature, pressure, noise, toxicity, acceleration, and vibration) and human error in system operation and support is minimized. Design factors likely to contribute to human error are identified and mitigated; 4) System users and operating personnel are kept abreast of the safety of the system and included in the safety decision process. 301.1: perform and document a comprehensive evaluation of the mishap risk being assumed prior to test or operation of a system, prior to the next contract phase or at contract completion A.3.2: Historical hazard and mishap data, including lessons learned from other systems, should be considered and used.
Query		Are the four desirable attributes (as defined in the ANSI STD) included in the safety program?	
Measurement Categories	5	Safety program plan and safety culture present clear evidence that all four attributes are present	
	4	Same as level 5, with partial evidence available	
	3	Same as level 5, but evidence lacking	
	2	Most elements present	
	1	Some elements present	
	0	No evidence of these attributes	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		18	
Query		What assets are protected by the system safety program?	
Measurement Categories	5	Level 4 + program impact	
	4	Includes 5 of 5 (personnel, equipment, environment, public, public property).	
	3	Includes 4 of 5 (personnel, equipment, environment).	
	2	Includes 3 of 5	
	1	Includes public and personnel	
	0	No distinctions made.	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		19	**MIL-STD 882E** Task 101: Integrate hazard identification and mitigation using the system safety methodology. 4.3.2: Identify and document hazards.
Query		How are hazards identified?	**ANSI STD** A.3.2.1: Hazard identification can be achieved by a variety of mutually complementary methods including the use of checklists, prior work with similar systems, and operating scenario walkthroughs. A.3.2: Identify and track hazards through a systematic hazard analysis process encompassing detailed analysis of system hardware and software, the environment (in which the system will exist), and the intended usage or application. A.3.2: Identification of hazards is a responsibility of all program members. A.3.2: During hazard identification and tracking; consider hazards that could occur over the system life cycle. Products of this element may include a PHL and/or a functional hazard assessment and a hazard tracking system (HTS).
Measurement Categories	5	Formally prescribed balance of brainstorm, checklists, walkthroughs, and hazardous operations (HAZOP), Failure Modes and Effects Analysis (FMEA), or Failure Hazard Analysis (FHA).	**IAASS** 4: Identify risks and its two essential elements: probability of an undesired event (a hazard) and the resulting consequences. 4: Identify situations and scenarios wherein people could be hazarded, including not only the planned or nominal scenario, but also off-nominal, unplanned, and malfunction scenarios.
	4	Level 3 + use of HAZOP, FMEA, or FHA, or equivalent; or use of prior experience with like systems.	
	3	Level 2 + supported by checklist(s) and/or energy source inventory and/or operational walkthroughs.	**FAA Draft** • An operator must conduct a preliminary safety assessment • An operator must [document and implement] a system safety program that includes: (i) Methods to review and assess the validity of the preliminary safety assessment throughout the life of the operation, (ii) Methods for updating the preliminary safety assessment, and (iii) Methods for communicating and implementing the updates throughout the organization.
	2	Organized, formally led brainstorming.	
	1	Informally guided brainstorming; "what if."	
	0	No formally required or documented techniques.	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		20	**MIL-STD 882E** Task 201: PHL: compile a list of potential hazards early in development
Query		What hazard inventory-type analytical techniques are used?	**ANSI STD** 202.1: perform and document a Preliminary Hazard Analysis (PHA) to identify safety critical areas, to provide an initial assessment of hazards, and to identify requisite hazard controls and follow-on actions.
Measurement Categories	5	One or more top-down methods and one or more bottom-up methods, formally documented, with software databasing.	
	4	Formally required FMEA or FHA, or equal; requirement is documented.	
	3	Formally required Preliminary Hazard Analysis (PHA) or HAZOP, with tailored matrix use; requirement is documented.	
	2	Formally required PHA, without tailored matrix use; requirement is documented.	
	1	Formally required PHL, requirement is documented.	
	0	Informal brainstorm list-making.	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		21	
Query		What logic tree analytical techniques are used?	
Measurement Categories	5	Probabilistic risk assessment, fully quantified with sound understanding of uncertainty.	
	4	Level 3 + Cause-Consequence Analysis (CCA) or equal (quantified) with a very sound understanding of calculating risk from probability and severity assessments.	
	3	FTA and/or Event Tree Analysis (ETA) with a very sound understanding of probability assignments and calculations.	
	2	Level 1 + ETA (unquantified) (or another logic tree method) with a sound understanding of modeling events with binary outcomes.	
	1	FTA (unquantified) with a sound understanding of "AND" and "OR" logic gates.	
	0	No formal logic tree analytical techniques are used.	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		22	
Query		How are hazards understood by those working in the program?	
Measurement Categories	5	Thorough understanding: a hazard constitutes a threat of harm to one or more assets and is expressed as a source, mechanism, and outcome.	
	4	N/A	
	3	Hazards are moderately well understood but are described inconsistently and don't specify threatened assets.	
	2	N/A	
	1	Hazards are often described, simply as a source, or a mechanism, or an outcome, alone.	
	0	Widespread misunderstanding as to what constitutes a hazard.	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		23	
Query		For software-intensive systems, how are the software personnel involved as contributors in identifying the hazards and mitigators?	
Measurement Categories	5	Fully involved in System Safety Working Group (SSWG) and integrated into the various IPTs.	
	4	Level 3+ involvement in developing mitigation features.	
	3	Involved in SSWG.	
	2	Involved in IPTs (or equivalent) only.	
	1	Involved in limited IPTs (or equivalent) only.	
	0	No involvement.	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		24	
Query		How is system safety practice linked to the “ilities” – e.g., Reliability, Availability, Maintainability?	
Measurement Categories	5	Full-bore, readily-auditable linkage to reliability, availability, and maintainability.	
	4	Formal, mandatory cross-feed with reliability and another “ility.”	
	3	Formal, mandatory cross-feed with reliability or availability, or maintainability.	
	2	Modest, moderately formal cross-feed with reliability or availability, or maintainability.	
	1	Infrequent, informal cross-feed with reliability or availability, or maintainability.	
	0	No linking practiced.	

Serial No.		HAZARD IDENTIFICATION & TRACKING
		25
Query		How are hazard tracking and safety requirement traceability implemented for system safety (including hardware, software, and human factors)?
Measurement Categories	5	Level 4 + auditable evidence that the hazard has been mitigated to an acceptable level of risk and there is an audit trail of safety requirements.
	4	Level 3 + coupled with configuration, management, or quality program.
	3	Procedure-driven and documented in well maintained records, uniform format, and with a well-established process. Safety requirements derived from hazards.
	2	Practiced according to loosely interpreted standards and procedures.
	1	Informally practiced.
	0	Not practiced.

Requirements:

FAA Draft

- (b) An operator must identify all safety-critical functions associated with its computing systems and software. Safety-critical computing system and software functions must include at least the following: (1) Software used to control or monitor safety-critical systems. (2) Software that transmits safety-critical data, including time-critical data and data about hazardous conditions. (3) Software used for fault detection in safety-critical computer hardware or software. (4) Software that responds to the detection of a safety-critical fault. (5) Software used in a flight safety system. (6) Processor-interrupt software associated with safety-critical computer system functions. (7) Software that computes safety-critical data. (8) Software that accesses or manages safety-critical data. (9) Software that displays safety-critical data. (10) Software used for wind weighting.

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		26	**MIL-STD 882E** 4.3.1.d: Documenting hazards with a closed-loop Hazard Tracking System (HTS) Task 106: Establish and maintain a closed-loop Hazard Tracking System (HTS).
Query		Are safety hazard data maintained up-to-date?	**ANSI STD** A.3.2.3: Maintain a HTS that includes hazard descriptions, mishap severity and probability, hazard causes (which may relate to hardware, software, or human-systems interface), mitigators for each cause, and verification for each mitigator, their closure actions, and mishap risk throughout the system life cycle. The HTS should be maintained throughout the system life cycle.
Measurement Categories	5	Updating required and practiced in response to: mishaps/near misses, design changes, or progress in modeling, analysis, or simulation.	106.2.1: The Developer should develop a method or procedure to document and track hazards and their controls thus providing an audit trail of hazard resolutions. A centralized file, computer data base, or document called a “Hazard Log” should be maintained.
	4	New experiences with same or similar systems prompt updating.	**FAA Draft** (b) An operator must establish and document the criteria and techniques for identifying new hazards throughout the life of the launch or reentry system; (d) The hazard analysis must be continually updated throughout the complete operational lifecycle of the launch or reentry system using configuration management principles.
	3	Major developments or findings of potential loss events, including near misses and incidents, prompt updating.	
	2	Major and minor loss events prompt updating; updating is not always timely.	
	1	Major loss events prompt updating; updating is not always timely.	
	0	Data are rarely updated or not updated at all; updating requirements do not exist.	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		27	**MIL-STD 882E** Task 402: Perform tests and analyses, develop data necessary to comply with hazard classification regulations
Query		Are explosives properly classified?[5]	
Measurement Categories	5	All explosives items have been classified in accordance with proper protocols and authority.	
	Scoring is limited to 0 or 5 only.		
	0	Some explosives items are not classified.	

[5] Evidence of classification needs to be validated by audit.

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		28	**ANSI STD** A.3.1.1: manage the risk of each single hazard (r) as well as the total system risk (R). 4.1: System Safety Program Elements. The Managing Authority should establish and execute system safety programs that manage the risk of each single hazard (r) as well as the total system (R). The following five elements are necessary to conduct a complete system safety program. Within each of the elements, the Managing Authority and developer should tailor the system safety program to fit the system context, unique hazards, and fiscal limitations. The Managing Authority should allocate sufficient resources to accomplish each safety element.
Query		Is risk managed at the hazard level (r) and the total system level (R)?	
Measurement Categories	5	Both. Individual hazards are summed using principles in risk summing guidebook. *Risk summing guidebook published by DoD.	**IAASS** 5: Aggregation of the total set of launch risks is recommended
	4	Risks are summed using simple addition.	
	3	Comprehensive risk list is quantified	
	2	Risks managed by comprehensive list of individual hazards.	
	1	Risk managed by incomplete list of individual hazards.	
	0	Risk is not managed.	

Serial No.		HAZARD IDENTIFICATION & TRACKING
		29
Query		How are hazards tracked? Is the SMO protocol used?
Measurement Categories	5	Automated tracking system is used and updated frequently throughout the life cycle as a living document. Tracking is available to system engineers, stakeholders, and safety personnel. SMO protocol is used to define comprehensive list of hazards, initiated at outset of system design.
	4	Same as level 5, but to a lesser degree
	3	Majority subset of level 5
	2	Partial subset of level 5
	1	Tracking is not automated, and ad hoc
	0	Hazards are not tracked

Requirements:

ANSI STD

4.1.2: Hazard Identification and Tracking: System safety includes a complete identification of the hazards associated with a system. In general, this is accomplished by identifying the source-mechanism-outcome of each hazard. This element also includes use of a hazard tracking system (HTS) and continuous tracking of the hazards throughout the life cycle.

A.3.2.2: Hazards should be described in terms that identify: a potential source of harm, the mechanism whereby the harm may be caused, and the outcome of the harm itself.

FAA Draft

- For operators that must conduct a hazard analysis, as required by § 450.xx, the system safety program must include: (A) Methods to review and assess the validity of the hazard analysis throughout the life of the operation, (B) Methods for updating the hazard analysis, (C) Methods for communicating and implementing the updates throughout the organization, and (D) A process for tracking hazards, risks, mitigation and risk control measures, and verification activities.
- (c) Configuration management and control. An operator must—(1) Employ a process that tracks configurations of all safety critical systems related to the operation, (2) Employ a process that tracks configurations of all safety critical documentation related to the operation, (3) Ensure the use of correct and appropriate versions of systems tracked in paragraph (c)(1) and (c)(2) of this section, and (5) Maintain records of launch or reentry system configurations and document versions used for each licensed activity, as required by § 450.xx (Records).

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		30	**ANSI STD** 201.1: Compile a list of potential hazards, very early in the system development cycle, on which management emphasis needs to be placed. **IAASS** 10: Launch system changes: At the system design phase, many options are available in selecting the materials, propulsion, and on-board constituents that directly affect the resultant hazards. Therefore, the assessment of potential (hazards leading to) risks should begin during this phase.
Query		At what point in the system development cycle is a list of potential hazards defined?	
Measurement Categories	5	Before preliminary design	
	4	During preliminary design	
	3	After preliminary design and before final design	
	2	During final design	
	1	After final design	
	0	Not accomplished during design phase	

Serial No.		HAZARD IDENTIFICATION & TRACKING	Requirements:
		31	**FAA Draft** • Identify the potential hazards associated with the system relevant to public safety and safety of property, including: (i) Vehicle operation, including staging and release; (ii) System, subsystem, and component failures or faults; (iii) Software operations as required by 450.xx (software reg); (iv) Environmental conditions; (v) Human factors; (vi) Design inadequacies; (vii) Procedures; (viii) Functional and physical interfaces between subsystems, including vehicle payload(s); (ix) Reuse of components or systems; and (x) Interactions of any of the above.
Query		Has a comprehensive set of hazards been defined?	
Measurement Categories	5	Hazard sources include a comprehensive list including: (i) Vehicle operation, including staging and release; (ii) System, subsystem, and component failures or faults; (iii) Software operations as required by 450.xx (software reg); (iv) Environmental conditions; (v) Human factors; (vi) Design inadequacies; (vii) Procedures; (viii) Functional and physical interfaces between subsystems, including vehicle payload(s); (ix) Reuse of components or systems; and (x) Interactions of any of the above.	
	4	More than seven of the categories are thoroughly evaluated.	
	3	More than five of the categories are thoroughly evaluated.	
	2	Some of the categories are thoroughly evaluated.	
	1	Only nominal scenarios are assessed.	
	0	No specific hazards are identified.	

Serial No.		RISK ASSESSMENT
		32
Query		Which hazard analysis techniques are used (PHA, FTA, FMECA, SHA, QRA, HHA, EHA, SAR etc.)? How are hazard analysis results tracked, recorded, documented, updated, and closed?
Measurement Categories	5	Recorded in uniform format software with search function and software-compiled summaries accessible by all system safety personnel.
	4	Recorded with uniform format for entire program in software with search/sort capability.
	3	Recorded using software with database search/sort capability.
	2	Recorded using software without database search/sort capability.
	1	Handwritten data sheets.
	0	Analysis documentation is not developed; no requirement exists for documentation or its method.

Requirements:

MIL-STD 882E

Task 202: PHA: perform and document a Preliminary Hazard Analysis (PHA) to identify hazards, assess the initial risks, and identify potential mitigation measures

Task 205: Perform and document a System Hazard Analysis (SHA) to verify system compliance with requirements to eliminate hazards or reduce the associated risks; to identify previously unidentified hazards

Task 207: Perform and document a Health Hazard Analysis (HHA) to identify human health hazards, to evaluate proposed hazardous materials and processes using such materials, and to propose measures to eliminate the hazards or reduce the associated risks when the hazards cannot be eliminated

Task 301: Perform and document a Safety Assessment Report (SAR) to provide a comprehensive evaluation of the status of safety hazards and their associated risks prior to test or operation of a system

ANSI STD

4.1.3: Risk Assessment: For each identified hazard, the mishap severity and probability or frequency are established. The assessment methods may include models, numerical analyses, and subjective judgments based on history and system knowledge.

205.1: perform and document a System Hazard Analysis (SHA) to: verify system compliance with safety requirements contained in system specifications and other applicable documents; identify previously unidentified hazards associated with the subsystem interfaces and system functional faults; assess the risk associated with the total system design, including software, and specifically of the subsystem interfaces; and recommend actions necessary to eliminate identified hazards and/or control their associated risk to acceptable levels.

207.1: perform and document a Health Hazard Assessment (HHA) to identify health hazards, evaluate proposed hazardous materials, and propose protective measures to reduce the associated risk to a level acceptable to the Managing Authority.

FAA Draft

n(a) A hazard analysis must identify, describe and analyze all reasonably foreseeable flight hazards to public safety and safety of property resulting from the vehicle operation, vehicle components, and payload and its integration. The hazard analysis must include a designation of risk, specifically the expected severity and likelihood of occurrence associated with each hazard. Each hazard analysis must:

(2) Assess each hazard's likelihood and severity;

(3) Determine each hazard's risk to public safety and safety of property;

Serial No.		RISK ASSESSMENT
		33
Query		How is risk assessed for a single hazard that threatens multiple protected assets? Use clarifying example.
Measurement Categories	5	Risk is individually assessed for each of multiple assets.
	4	Assessments for multiple assets are aggregated using a defined rule.
	3	Assessments for multiple assets are aggregated consistently by a rule developed by the individual practitioner.
	2	Assessments for multiple assets are "lumped" to a single risk declaration without disciplined aggregation.
	1	Risk is assessed/reported only for the single asset that is judged to have greatest risk.
	0	Assessment method not known or not understood by interviewee.

Requirements:

ANSI STD
A.3.2.2: Hazards should be described in terms that identify: a potential source of harm, the mechanism whereby the harm may be caused, and the outcome of the harm itself. An effective way to deal with these multiple outcomes from one source and mechanism is to treat each outcome, each harmful impact on an asset, as a separate hazard.

Serial No.		RISK ASSESSMENT	Requirements:
		34	
Query		How is exposure interval selection made?	
Measurement Categories	5	Exposure Interval is explicitly stated, with due regard for the overall time interval and adjusted for less-than-full-time functions.	
	4	Exposure Interval is explicitly stated, with due regard for the overall time interval, but not adjusted for less-than-full-time functions.	
	3	Exposure Interval is explicitly stated, but miscalculated.	
	2	Exposure Interval is known to play a role in determining Hazard Probability but is unstated or is assigned from a standard, not adjusted to true Program needs.	
	1	Exposure Interval is vaguely/indefinitely stated (e.g., "life cycle").	
	0	Need for expressing an explicitly stated Exposure Interval is not recognized.	

Serial No.		RISK ASSESSMENT	Requirements:
		35	**ANSI STD** A.3.1.4.2: Describe the mishap risk assessment procedures, including the mishap severity categories, mishap probability categories A.3.1.2.6: Establish an acceptable level of mishap risk, mishap probability or frequency, and mishap severity thresholds, and documentation requirements (including but not limited to hazards and mishap risk). A.3.1.3.4.2: Developing Risk Assessment Matrix using ANSI Std guidance A.3.1.4.2: Describe the mishap risk assessment procedures, including the mishap severity categories, mishap probability categories,
Query		How is risk assessment matrix tailoring done?	
Measurement Categories	5	Full matrix (indices/spans/resolution) quantitatively tailored, asset-by-asset.	
	4	Quantitative partial matrix scaling/tailoring.	
	3	Subjective matrix scaling/tailoring of exposure interval and multiple assets.	
	2	Tailored severity scale for only one asset (e.g., equipment or personnel).	
	1	Need recognized, but none performed.	
	0	Need not recognized.	

Serial No.		RISK ASSESSMENT	Requirements:
		36	
Query		Is analytical tool selection tailored to the needs of individual system peculiarities and needs?	
Measurement Categories	5	Optimized selection of tools according to need from wide range of options.	
	4	Tools generally selected to fit the task, but sometimes chosen according to analyst's capability rather than system need.	
	3	Moderate tailoring of selection from standard list of tools for all systems/subsystems.	
	2	No tailoring; standard, modest selection of tools for all systems/subsystems.	
	1	One tool used without modification for all analyses.	
	0	Need for tailored selection not recognized.	

Serial No.		RISK ASSESSMENT	Requirements:
		37	
Query		How is the analysis of Government-off-the-Shelf (GOTS)/Non-Developmental-Items (NDI)/ Commercial-off-the-Shelf (COTS)/software reuse addressed in the system safety program (including hardware, software, and human factors)?	
Measurement Categories	5	Fully defined with appropriate variety of techniques for certification of proposed use, monitoring and selection.	
	4	Limited safety approval process.	
	3	Monitoring safety of use.	
	2	Defined using appropriate techniques.	
	1	Defined methods for item selection.	
	0	Not addressed.	

Serial No.		RISK ASSESSMENT	Requirements:
		38	**MIL-STD 882E** 4.3.3: Assess and document risk 4.3.3.b.1: When available, the use of appropriate and representative quantitative data that defines frequency or rate of occurrence for the hazard, is generally preferable to qualitative analysis. 4.3.3.e: The Program shall document all numerical definitions of probability used in risk assessments as required by 4.3.1. **IAASS** 5: These assessments combine physical sciences, engineering disciplines, and reliability information with math, statistical, and in some cases, uncertainty calculations to produce an assessment of each risk. 5: Risk assessments should be objective, scientifically supported with academically acceptable math, and based on data rather than conjecture.
Query		What analytical approach is used to assess risk?	
Measurement Categories	5	Full QRA (including uncertainty) analysis using academically acceptable methods and fully supported input data. Input data based on test data, historical data, reliability calculations. Assumptions fully explained and justified. QRA is peer reviewed by external SME.	
	4	Same as level 5, but to a lesser degree	
	3	Same as level 5, but to a partial degree	
	2	Same as level 1, with independent peer review	
	1	Subjective analysis by SMEs	
	0	Ad hoc subjective judgements by single untrained individual.	

Serial No.		RISK ASSESSMENT
		39
Query		A Software Criticality Index (SCI) is determined and used to guide the Level of Rigor (LOR) tasks or requirements?
Measurement Categories	5	A Software Criticality Matrix (SCM) is documented and used to define the SCI. A LOR table has been developed and used to guide tasks or requirements. Equally rigorous methods may be substituted. Rigor of V&V testing is proportional to criticality of software.
	4	Same as level 5, but to a lesser degree
	3	Same as level 5, but to a partial degree
	2	Critical software is tested more rigorously
	1	Critical software is not tested to a more rigorous level
	0	Software criticality is not defined

Requirements:

MIL-STD 882E
4.4: [Note 882 software requirements are not state of the art and therefore not included (see Joint Services Software Safety Authorities JS-SSA-IG Rev B)]

ANSI STD
A.3.1.3.2.d: Identification of the software hazard criticality assessment process to include establishment of the software criticality index matrix for each safety critical software function and safety critical requirement and how it will be used to assign software integrity assurance tasks necessary to verify and validate the safety critical functions and requirements;
A.3.1.3.2.c: Identification of safety critical software functions and safety critical software requirements;
A.3.3.2: For systems with safety critical software (i.e., software controls safety critical functions), each safety critical software function and requirement should be assigned a software criticality index (SCI).

FAA Draft
(c) Safety-critical functions must be identified by consequence and the degree of control exercised by the software component as defined by paragraphs (d) through (h) of this section.
(d) Autonomous software. This section applies … criteria: *To include (1)(2)(3)(4)(5) & (i)(ii)(iii)(iv)(v)*
(e) Semi-autonomous software. This section applies … criteria: *To include (1)(2)(3)(4)(5) & (i)(ii)(iii)(iv)(v)*
(f) Redundant fault-tolerant software. This section applies … criteria: *To include (1)(2)(3)(4)(5) & (i)(ii)(iii)(iv)(v)*
(g) Influential software. This section applies … criteria: *To include (1)(2)(3) & (i)(ii)(iii)(iv)(v)*
(h) Application requirements. An applicant must document and include in its application the following: *To include (1)(i)(ii)(iii)(iv), (2)(i)(ii)(iii)(iv), (3)(i)(ii), (4)(i)(ii), and (5).*

Serial No.		RISK ASSESSMENT	Requirements:
		40	**IAASS** 11: Range flight safety systems. Many launch vehicles carry on-board systems designed to limit the risk if the launch system malfunctions during the propulsion phase and poses a hazard. The design of these systems can vary widely and include thrust termination, vehicle separation or destruction, or intact ditch of the vehicle. In some scenarios, the use of a range flight safety system may add additional risks to the mission and protected population. Therefore, the application of a range flight safety system must be thoroughly analyzed as part of the risk assessment.
Query		Are range safety systems that are designed to reduce risk also evaluated to ensure they do not increase risk? Are they reliable? Do they balance alpha and beta errors? To what degree does the flight safety system demonstrate proof that it is reliable and balances both alpha and beta errors?[6]	
Measurement Categories	5	System is uncomplicated with few failure modes. System is tested thoroughly for both alpha and beta errors. Risk analyses use physics-based consequence approach to determine all risks to the public. All reasonable malfunctions are considered based on probability. Assumptions are defined and documented. System clearly reduces risk to public in all reasonable scenarios.	
	4	Same as level 5, but to a lesser degree	
	3	Same as level 5, but to a partial degree	
	2	System reduces risk in most scenarios	
	1	System does not effectively reduce inherent risks	
	0	System can add unwarranted risk	

[6] Alpha error is the probability that an FSS in a given scenario will erroneously fail to terminate an off nominal or malfunctioning flight. Beta error is the probability that an FSS in a given scenario will erroneously terminate a nominal flight.

Serial No.		RISK ASSESSMENT	Requirements:
		41	**FAA Draft** (d) Post-flight data review. An operator must establish a process for evaluating post-flight data to— (1) Ensure consistency between the assumptions used for the preliminary safety assessment and operational restrictions, (2) Identify anomalies that may impact the flight safety analysis, (3) Identify anomalies that may impact the hazard analysis, if a hazard analysis is required, (4) Resolve any identified inconsistencies prior to the next flight of the vehicle, (5) Include and address any identified anomalies in the flight safety analysis used for the next flight of the vehicle, and (6) Include and address any identified anomalies in updates to the hazard analysis, as required by § 450.xx.
Query		How is post-flight data used to validate pre-mission risk analysis?	
Measurement Categories	5	All 6 steps for evaluating post-flight data are completed and well documented	
	4	Most are completed	
	3	Some are completed	
	2	Review is completed. Documentation is ad hoc.	
	1	Review is conducted, but not documented.	
	0	Not used at all.	

Serial No.		RISK REDUCTION	Requirements:
		42	
Query		In assessing risk, how is uncertainty addressed or characterized?	
Measurement Categories	5	Uncertainty is evaluated with rigor, on a case-by-case basis, according to a prescribed, documented plan.	
	4	Uncertainty is assessed either subjectively or quantitatively but without a standardized, documented plan.	
	3	"Standard" uncertainties are assigned to subjective severity and probability evaluations then projected to a value for risk.	
	2	Risk uncertainties are subjectively judged from a standardized scale as are levels of hazard probability and severity.	
	1	No consideration is given to evaluating uncertainty, or uncertainty is very poorly conceptualized.	
	0	Uncertainty as a concept is inadequately understood to be applied.	

Serial No.		RISK REDUCTION
		43
Query		How is the hierarchy of mitigation precedence treated?
Measurement Categories	5	Level 4 + proper use of design change is generously evident.
	4	Level 3 + requirement for use is documented/enforced.
	3	Hierarchy is properly used, and use is monitored/reviewed.
	2	Hierarchy is properly used, but use is ill-enforced.
	1	Hierarchy is recognized but use is not monitored or enforced; mitigation measures are often mis-ranked.
	0	Effectiveness hierarchy not recognized, not used.

Requirements:

ANSI STD

A.3.1.4.2: Describe the system safety mitigation order of precedence that should be followed to satisfy the safety requirements of the program.

4.1.4.1: System Safety Mitigation Order of Precedence: 1) Eliminate Hazard Through Design Selection; 2) Reduce Mishap Risk Through Design Alteration; 3) Incorporate Engineered Safety Features; 4) Incorporate Safety Devices, 5) Provide Warning Devices; and 6) Develop Procedures and Training,

A.3.4: Risk reductions are achieved by understanding the risk drivers, reducing risk according to the system safety mitigation order of precedence, and then reassessing the risks. Mitigators for reducing risk include design changes, engineered safety features, safety devices, warning devices; and procedures or training. Mitigators may serve to eliminate the hazard or reduce severity or probability of potential mishaps.

IAASS

6: Possible Proven Risk Reduction measure approaches: 1. Containment, 2. Evacuations and Sheltering, 3. Scenario Changes, 4. Launch System Changes, 5. Range Flight Safety Systems

7: Containment: limit personnel access within an area that contains these pre-launch and launch risks. The appropriate area for limited access is determined as part of the risk assessment.

8: Evacuations and Sheltering: evacuate (or shelter) personnel from potential hazard areas for launch or other associated hazard operations.

9: Scenario changes: Varying the flight profile to identify the minimum risk scenario should be a part of the risk reduction approach.

12: Risk-reduction measures for re-entry: demise, collision avoidance, planned re-entry, scheduling, and orbital inclination tailoring can help avoid population centers

FAA Draft

- (5) Identify and describe the risk elimination and mitigation measures required to satisfy paragraph (a)(4) of this section. The measures must include one or more of the following: Designing for minimum risk, Incorporating safety devices, Providing warning devices, or Implementing procedures and training.
- (e) Application requirements. An applicant must provide in its application the following: (1) The hazard analysis products of § 450.xx, including data that verifies the risk elimination and mitigation measures resulting from the applicant's hazard analyses required by paragraph § 450.xx(a)(6).

Serial No.		RISK REDUCTION	Requirements:
		44	**ANSI STD** A.3.1.4.2: State any subjective or quantitative measures of safety to be used for the mishap risk assessment process including any associated criteria.
Query		Are risk assessments quantified?	
Measurement Categories	5	All risk assessments are quantified using academically accepted methods and peer review.	
	4	Most risk assessments are quantified using academically accepted methods and peer review.	
	3	Some risk assessments are numerically expressed using sound methods.	
	2	Some risk assessments using subjective methods.	
	1	An underdeveloped effort has been made to numerically express/quantify risk, based on subjective assessments.	
	0	No risk assessments are numerically expressed.	

Serial No.		RISK REDUCTION	Requirements:
		45	
Query		Are newly discovered hazards reported and mitigation plans formulated promptly?	
Measurement Categories	5	Discovery/hazard reporting and risk assessment by collaborating safety/engineering team; prompt mitigation development/implementation.	
	4	Hazard/risk assessment reporting by system safety personnel with immediate reporting to engineering and/or Program Management (PM) level; mitigation follows shortly.	
	3	Infrequent reporting at periodic meetings dedicated to that purpose; mitigation follows, usually with no particular urgency.	
	2	Reporting done only during widely spaced formal design reviews; mitigation follows.	
	1	Reporting significantly lags discovery, delaying mitigation.	
	0	No formal reporting method exists; mitigation of a newly discovered hazard may not occur until a near miss or loss event is experienced.	

Serial No.		RISK REDUCTION	Requirements:
		46	**MIL-STD 882E** 4.3.4: When a hazard cannot be eliminated, the associated risk should be reduced to the lowest acceptable level within the constraints of cost, schedule, and performance by applying the system safety design order of precedence. 4.3.5: Reduce risk. 4.3.5: Mitigation measures are selected and implemented to achieve an acceptable risk level. **ANSI STD** 402.1: perform and document an assessment to identify and verify compliance with military, federal, national, international, and industry codes to ensure design of a system whose mishap risk is as low as reasonably practicable, and to comprehensively evaluate the mishap risk being assumed prior to test or operation of a system or at contract completion. A.3.4: The mitigators for each hazard should be selected based on effectiveness, cost, and feasibility. Feasibility includes consideration of both means and schedule for accomplishment. After mitigators have been selected, the residual mishap risks should be reassessed to ensure that risks are ALARP. A.3.5: The designated risk acceptance authority determines whether or not the mishap risks have been reduced to ALARP within the constraints of operational effectiveness and suitability, time, and cost (or that the risk is acceptable).
Query		How is the ALARP principle applied?	
Measurement Categories	5	ALARP is always the goal in risk reduction. Judgments are peer reviewed and documented.	
	4	Same as level 5, but to a lesser degree	
	3	Same as level 5, but to a partial degree	
	2	ALARP is a concept	
	1	Mitigation measures are selected and implemented only to meet acceptable risk levels.	
	0	ALARP is not understood.	

Serial No.		RISK REDUCTION	Requirements:
		47	**MIL-STD 882E** 4.3.4: Identify and document risk mitigation measures Task 401: Define and perform tests and demonstrations or use other verification methods on safety-significant hardware, software, and procedures to verify compliance with safety requirements **ANSI STD** 4.1.4: Risk reduction is achieved by accomplishing the following steps: a) Understand the risk drivers; b) Develop and document candidate mitigators; c) Select and implement mitigators in accordance with the system safety mitigation order of precedence; and d) Verify that the risk has been reduced. 401.1: define and perform tests and demonstrations or use other verification methods on safety critical hardware, software, and procedures to verify compliance with safety requirements
Query		How are risk reductions verified and validated during the life cycle?	
Measurement Categories	5	Multiple methods are used, including: frequent monitoring; QRA calculations updated frequently with new information; physical inspections of hardware; testing of software; post-test examinations of mitigation performance; documentation of above	
	4	Same as level 5, but to a lesser degree	
	3	Same as level 5, but to a partial degree	
	2	Implemented, but infrequent follow-up	
	1	Implemented, but no follow-up	
	0	Not done	

Serial No.		RISK REDUCTION	Requirements:
		48	**ANSI STD** A.3.3: After hazards are identified in Element 2, the identified hazards are reviewed and mishap severities, and probabilities or frequencies are assessed and documented. The products of this element may include a PHA, O&SHA, SSHA, SCF list, CSI list, and an SHA. **IAASS** 5: Assessment of risks: a scientific and engineering assessment of the level of seriousness of each identified risk 5: Assessments are normally conducted before and after the incorporation of risk reduction measures. **FAA Draft** • (6) Demonstrate that the risk elimination and mitigation measures achieve the risk levels of paragraph (a)(4) of this section through validation and verification. Verification includes: (i) Test data, (ii) Analysis, or (iii) Inspection results.
Query		Are probability, severity, and exposure determinations made prior to and after mitigations?	
Measurement Categories	5	Probability and severity determination after mitigation implementation is only applied after the mitigation methods have been verified using one of the four fundamental methods of verification (Inspection, Demonstration, Test, or Analysis). Includes comprehensive QRA.	
	4	Same as level 5, but to a lesser degree	
	3	Same as level 5, but to a partial degree	
	2	Same as level 5, but only where risk change is considered significant	
	1	Probability and severity determination after mitigation; implementation is based on the subjective opinion of an individual as an adjustment to a previous QRA.	
	0	No post-mitigation adjustment made	

Serial No.		RISK ACCEPTANCE	Requirements:
		49	
Query		How are system safety (including hardware, software, and human factors) analyses reviewed? (At what organizational level; with what thoroughness?)	
Measurement Categories	5	Level 4 + independent, 3rd party review of >5% samples, long-term average	
	4	Level 2 + 2nd level management or above	
	3	Level 2 + 1st level management (one group plus one manager)	
	2	Peer team (one group) or System Safety Working Group (SSWG)	
	1	Peer (1st level - one person)	
	0	None performed.	

Serial No.		RISK ACCEPTANCE	Requirements:
		50	
Query		How are waivers, exceptions, and other non-compliances managed by the system safety program?	
Measurement Categories	5	Waivers are time-limited and are tracked to soundly justified resolution and closeout without renewal.	
	4	Waivers are properly requested /approved, and tracked, but occasionally are insufficiently time-limited, or closeout deadlines are extended with little question/no stated justification.	
	3	Waivers are properly requested/approved but many persist indefinitely, or are arbitrarily closed out with questionable justification (e.g., "it hasn't happened yet, so it's not a hazard").	
	2	Waivers are requested/approved perfunctorily, without probing the rationale for granting them and are arbitrarily closed or persist indefinitely.	
	1	Waiver practice requirements are very poorly understood by line personnel and/or are poorly documented/implemented.	
	0	Program has no provisions for waivers - none are used.	

Serial No.		RISK ACCEPTANCE
		51
Query		How is acceptance of residual risk documented/reported?
Measurement Categories	5	Signed risk assessment document, electronically archived in searchable database.
	4	Signed risk assessment document, with archived paper copy.
	3	Verbal (spoken), transcribed/documented in hazard tracking software.
	2	Verbal (spoken) transcribed informally on handwritten sheet.
	1	Verbal (spoken) with no documentation of residual risk having been accepted.
	0	No recognition or flawed recognition of residual risk as a concept.

Requirements:

MIL-STD 882E
4.3.1.c: Defining how hazards and associated risks are formally accepted by the appropriate risk acceptance authority

ANSI STD
A.3.1.2.8: Establish the method for the formal acceptance and documentation of mishap risks and the associated hazards.
4.1.5: Risk Acceptance: The Developer PM should provide the Managing Authority with sufficient information to make informed decisions regarding the acceptability of residual mishap risk

FAA Draft
- (4) Ensure that the risk associated with each hazard meets the following criteria: (i) The likelihood of any hazardous condition that may cause death or serious injury to the public must be extremely remote. (ii) The likelihood of any hazardous condition that may cause substantial property damage to the public must be remote.
- (c) For every mission, the hazard analysis must be accurate and complete, and all hazards must be mitigated to an acceptable level in accordance with paragraph (a)(4) of this section.

Serial No.		RISK ACCEPTANCE	Requirements:
		52	
Query		How are risk tolerance limits selected for programs?	
Measurement Categories	5	Hazard probability and severity levels, exposure interval, and risk acceptance contour tailored by management to satisfy program needs; requirement is documented and enforced.	
	4	Tailored by adjusting hazard severity and hazard probability level definitions, adjusting risk tolerance contours within matrix, and adjusting exposure interval.	
	3	Tailored by adjusting hazard severity and/or probability scale definitions or exposure interval.	
	2	Applied directly from a carefully selected standard (e.g., MIL-STD-882), with no tailoring, with fixed, documented exposure interval.	
	1	Pro-forma, directly from a standard (e.g., MIL-STD-882) without change and without regard for exposure interval.	
	0	Risk tolerance concepts are not recognized; standards-based code worthiness is the sole risk tolerance determinant.	

Serial No.		RISK ACCEPTANCE
		53
Query		What system safety risk summation practices are employed?
Measurement Categories	5	Risk summation is required and enforced with rigorous quantitative calculations and software support; total system risk versus partial risk is well recognized.
	4	Summing risks is required; quantitative calculations are well understood, and the concept of total risk versus partial risk is well recognized.
	3	Summing risks is a required practice; subjective application is widely recognized, and quantitative application is moderately understood.
	2	Risk summation is moderately understood; subjective application is often used, but quantitative calculation is poorly understood.
	1	Risk summation is modestly understood; the concept is loosely interpreted and practiced subjectively.
	0	Risk summation is insufficiently understood to be used by the program; partial risks are treated individually.

Requirements:

ANSI STD

A.3.3.4: Most hazard analysis techniques are designed to identify and assess the risk of individual hazards, considered one at a time. Risk acceptance authorities, however, should also consider the overall, or total system, risk presented by the system in its entirety. Consideration of total system risk is useful because the aggregation of a number of otherwise acceptable individual risks may present an unacceptable risk when considered in total

A.3.4.1: For the system, determine which hazards are the drivers of the total system risk (R). For each hazard, determine which sources and mechanisms are the drivers of the single hazard risk (r). A good understanding of these risk drivers facilitates effective development, selection and prioritization of risk mitigators.

A.3.5: Review and acceptance of each interim and residual single hazard risk (r) by the appropriate authority is a necessary action in the risk management process. Consideration should also be given to requiring the review and acceptance of total system risk (R) by the appropriate authority. The designated risk acceptance authority should be kept informed regarding identified hazards and mishap risks.

Serial No.		RISK ACCEPTANCE	Requirements:
		54	**MIL-STD 882E** 4.3.7: Accept risk and document. The risks shall be accepted by the appropriate authority.
Query		Is the risk acceptance authority properly designated and does that authority always make the decision?	**IAASS** 13: Acceptance of risks by a properly designated authority. A risk management framework is not complete without a well-defined and documented approach to accept known risks prior to launch. The legal principle supporting this element requires three parts: a) a properly designated official, b) make a risk informed decision, c) that all of the known risks are within acceptable standards. If each element is adequately met, a degree of liability protection can be afforded. 14: Risk criteria/standards. To support risk acceptance decisions, a set of criteria/standards should be developed and used
Measurement Categories	5	A risk acceptance authority is clearly designated and documented in a SSPP or SSMP. This authority always makes the risk acceptance decision and never delegates. An independent, third-party SME is used to review all risk calculations. Process is fully transparent to FAA AST	
	4	Same as level 5, but to a lesser degree	
	3	Same as level 5, but to a partial degree	
	2	Documented process not fully followed	
	1	Ad hoc acceptance process used. Authorities undocumented.	
	0	Risk acceptance is not done.	

Serial No.		A PRIORI STANDARD	Requirements: Applicants must compute E_c and P_c based on QRA analysis.
		55	
Query		How is compliance with the quantitative standard demonstrated?	
Measurement Categories	5	Same as four (measurement category) with uncertainty applied at each element of risk equation using peer reviewed methods and validated by Monte Carlo or academically acceptable closed-form analysis.	
	4	Same as three (measurement category) with addition of properly defined risk summing. Uncertainty applies as applique.	
	3	Dendritic analyses define both failures and nominal scenarios that pose risks. Reliability data, statistical data, and a comprehensive set of conditions are considered.	
	2	Dendritic analyses define failure modes. Subjective analyses support each failure mode assumptions are defined.	
	1	Simplistic quantitative analyses are performed based on subjective assessments.	
	0	QRAs are not performed.	

This page intentionally left blank.

APPENDIX B – SOW TASK 1

2.0 STATEMENT OF WORK

FAA/AST seeks to define a safety regime that varies safety requirements as a function of the operating class of a vehicle. The operating class should define the required Level of Rigor (LoR) of an applicant's system safety process and AST's evaluation of the process, as a function of various safety performance metrics such as:

- the public safety consequences of a System failure,
- the probability of a System failure,
- the robustness of a Flight Safety System (FSS) and the associated activation criteria,
- the fault tolerance of safety critical system(s), and
- the fidelity of the Flight Safety Analysis (FSA).

In A-P-T Report CDSP-FL004-17-00200 (incorporated in ACTA Report #17-1001/2-01), APT's System Safety Performance Level Model (SSPLM) framework was proposed to evaluate the level of rigor for a system safety process. FAA/AST desires to update and tailor the SSPLM framework for application to launch and reentry vehicles, including examining current system safety standards, tailoring the SSPLM queries, and developing the "grading" criteria standards for assessing an applicant's system safety program maturity and adequacy. The goal of this subtask includes development of procedures for the application of the SSPLM by AST.

Under this subtask the contractor shall:

1) Facilitate a face-to-face Technical Interchange Meeting to:
    a. Describe APT's System Safety Metrics Method (SSMM)
    b. Discuss FAA/AST vision for system safety level of rigor
    c. Introduce training options
2) Review industry System Safety standards, including the current version of MILSTD-882
3) Validate the applicability of SSPLM queries as related to space systems,
4) Tailor SSPLM queries and assessment criteria
    a. Tailor queries for space system applications
    b. Modify assessment criteria targeting space systems
5) Develop options for AST implementation of the SSMM, and hone the options based on AST feedback,
6) Present proposed path forward to FAA/AST,
7) Recommend updates to the SSPLM as necessary based on AST feedback,
8) Document the path ahead for full or partial implementation of the SSPLM to the Level of Rigor Framework. This should include a sample scenario of a medium Level of Rigor for exemplary purposes, itemization of the procedures to be developed, and definition of the training and credentials needed to conduct audits.

This page intentionally left blank.

APPENDIX C – AUTHORS

The primary authors for Task 1 are Tom Pfitzer and Megan Stroud. Contributing authors include Katie Byers, Bob Baker, Tom Delong, Saralyn Dwyer, Barry Hendrix, Tim Middendorf, and Dr. Fayssal Safie.

Tom Pfitzer

A career-long safety engineer since 1971, Tom Pfitzer founded A-P-T Research, Inc., a company that currently holds the safety support contracts for NASA Kennedy Space Center and the Missile Defense Agency (MDA), the Department of Defense Explosives Safety Board (DDESB), as well as smaller contracts providing safety engineering analysis and support to over 40 U.S. government agencies.

Early in his career, he was a Range Safety Officer at one of the U.S. National Ranges overseeing the safety of over 200 launches. He was one of the primary authors of the first consensus range safety risk criteria document developed by the U.S. Range Commanders Council in 1997. From 1997 to 2005, he led a team of analysts supporting DDESB that developed the IARA (Identify, Assess, Reduce, Accept) risk management method and the Safety Assessment For Explosives Risk (SAFER) model. He is a Fellow member of the International System Safety Society (ISSS) and has been recognized by that society with their Pathfinder Award for lifetime achievements, one of only 10 persons to receive this award. From 2009-2017, he chaired the Launch and Re-Entry Committee of the IAASS, where he remains a board member. In 2004, he founded the Safety Engineering and Analysis Center (SEAC) in Huntsville, AL, where he currently serves as Subject Matter Expert (SME). He is a frequent speaker at safety conferences, including several keynote addresses. He holds a MS in Safety Engineering from Texas A&M University.

Megan Stroud

Megan Stroud is a Senior Engineer/Analyst at APT Research, Inc. in Huntsville, AL. She is currently a member of the SEAC and serves as the Program Manager for APT training initiatives, development & collaboration efforts. Prior to her current assignment, Ms. Stroud supported the MDA System Test and Evaluation Planning Lab in the area of Flight Safety, specifically including intercept debris analysis, flight termination system debris analysis, and the evaluation of risk contours and exclusion zones. In addition, Ms. Stroud has experience with analysis methods for explosives safety risk assessments and was a member of the Risk Based Explosive

Safety Criteria Team sponsored by the DDESB. Megan holds a B.S. in Engineering from Auburn University and a M.S. in Engineering Management from Florida Institute of Technology. She has been granted membership into the engineering honor society, Tau Beta Pi and the nation's most selective honor society for all academic disciplines, Phi Kappa Phi. She is also a member of the IAASS (International Association for the Advancement of Space Safety), serving as its Professional Training Chair.

Katie Byers

Katie Byers serves as APT's SME in written language and regulations. Her knowledge and expertise in clear writing principles help ensure products are clear, concise, and effective. Prior to her current assignment, she spent 20+ years in business journalism as a writer and editor. She has also served as a flight test data analyst/manager. She holds a B.A. in English from Davidson College and MBA from the University of Alabama in Huntsville.

Bob Baker

Bob Baker is the Chief Analyst at APT Research, Inc. Mr. Baker holds a B.S. in Applied Mathematics from Auburn University and a B.S. / M.S. in Aeronautical / Astronautical Engineering from the Air Force Institute of Technology. He has over 30 years of experience conducting/analyzing missile flight testing and developing quantitative models to evaluate the risks posed by a variety of hazards. Mr. Baker's background includes work with national committees in the areas of flight safety, system safety, and explosive safety and as a contributing author to risk standards in each area (RCC321, MIL STD 882, DoD 6055.09). He has supported over 25 major missile system tests conducted at eight U.S. and two foreign test ranges. Mr. Baker has supported the DoD Explosive Safety Board's Risk Based Explosive Criteria Team for over 20 years making key contributions to statistical model uncertainty estimation.

Tom DeLong

Tom DeLong holds a BSEE from Lehigh University and master's degree in IE (System Safety) from Texas A&M University. He graduated in the first U.S. Army Materiel Command Safety Engineering Intern Program and graduated from the Army Management Staff College. Prior to joining APT, Tom retired from civil service with nearly 35 years of service, where he received the Department of the Army Meritorious Civilian Service Award. He served as the government technical monitor on two safety

support contracts. Tom was the lead engineer for explosive hazard classification for the Army Missile Command and provided Army MACOM review of explosive site plans for USASMDC. He was a member of the Army Acquisition Corps with Level III certification in Systems Planning, Research, Development and Engineering. He chaired the Army's System Safety Technical sub panel for several terms and was the International System Safety Society Engineer of the Year in 2000 where he served in all offices of the local chapter. He was selected as 2010 Educator of the Year by the Tennessee Valley Chapter. Tom has been a guest instructor at the AMC Field Safety Activity's System Safety Course. He was a Certificated Flight Instructor for over 30 years. He currently is APT's lead system safety instructor.

Saralyn Dwyer

Ms. Dwyer currently serves as SEAC Director. She supports the day-to-day management of the SEAC as well as providing customer support. Ms. Dwyer has 25+ years of experience in supporting systems and design teams with Failure Modes, Effects and Criticality Analyses (FMECAs), Critical Items Lists (CILs), Fault Tree Analyses (FTAs), the development of system requirements, as well as providing overall safety and mission assurance support. She has supported safety analyses on launch vehicle safety systems to include Flight Termination Systems and reviewed and assessed contractor deliverables including FMECAs, FTAs, safety analyses, and hazard analyses. From 1996-2016, she served in a variety of local and national officer positions of the ISSS.

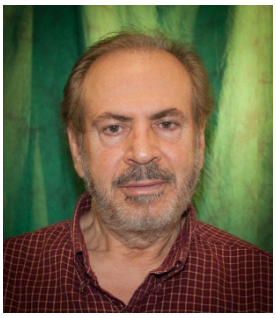
Barry Hendrix

Mr. Hendrix joined APT Research in 2015 after retiring from Lockheed Martin as Fellow Emeritus for System Safety. In Huntsville he has served as the System Safety Lead on the Integrated Battlefield Command System, the Principal Software Safety Engineer on the Multi-Mission Launcher, and the Software Safety Lead on C-RAM (Counter Rocket, Artillery, and Mortar). Barry's career in System Safety started 37 years ago at Vought Aircraft Company in Dallas, TX after serving 10 years in the United States Navy with attack squadrons aboard aircraft carriers. He is a Fellow member of the ISSS, former President of the North Texas Chapter, and past Director of Members Services. He was awarded the ISSS Manager of the Year in 2001 for system safety leadership in software safety on the F-22, F-35, C-130J, and C-5M AMP and RERP aircraft upgrades. He supported advanced missile programs at LTV and Texas Instruments. He was a system engineering team leader at the Superconducting Super Collider for Lockheed at the Department of Energy. He has trained over 1,000 engineers in software system safety and airworthiness.

Tim Middendorf

Mr. Middendorf has over 30 years of experience in space systems engineering, system safety, and space operations, to include Range Flight Safety, UAV flight analysis, propulsion technology system analysis, spacecraft engineering/ operations (GPS and DSCS II), and spacecraft launch operations (GPS). Mr. Middendorf has over 20 years of experience supporting the Office of Commercial Space Transportation.

Fayssal Safie



Dr. Safie is currently serving as a Principal Reliability Engineer at APT Research. He holds a Bachelor, a Master, and a Doctorate degree in Systems Engineering. Dr. Safie retired from NASA Marshall Space Flight Center in 2016 as the Agency Technical Fellow for Reliability and Maintainability (R&M) engineering with over 30 years of service. Prior to his assignment as the NASA Technical Fellow for R&M, he held several leadership positions in the areas of reliability, safety, Quality engineering, and Risk Assessment. Beside his many years of service at NASA, Dr. Safie served for over 20 years as an Adjunct Professor of Systems Engineering at the University of Alabama in Huntsville. Dr. Safie received over 50 honors and awards and published over 40 papers in Reliability Engineering, Probabilistic Risk Assessment, System Safety, and Quality Engineering.