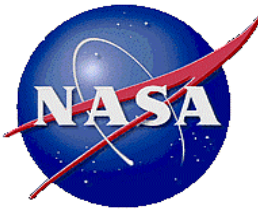


A VISION FOR SYSTEM SAFETY

Position Paper

September 30, 2013

_____ _____

Homayoon Dezfuli, Ph.D.
NASA Technical Fellow for System Safety
(Project Manager)

Date

Acknowledgements

The project manager expresses his gratitude to: 1) the management of the NASA Headquarters Office of Safety and Mission Assurance (especially Bryan O'Connor and Terrence Wilcutt) for their long-term support made possible the many advancements that have set the stage for the future of System Safety practice as envisioned in this document, and (2) the NASA System Safety Steering Group for their support and contribution to the development of this paper.

NASA System Safety Steering Group Members (including Alternates and Support Contractors)

Michael Blythe, NESC (JSC)	M
Roger Boyer, JSC	M
Bruce Bream, GRC	M
Jonathan Brown, DFRC	M
Alfredo Colon, HQ	M
Chet Everline, JPL	A
Martin Feather, JPL	M
Ron Gillett, KSC	A
Frank Groen, HQ	M
K.C. Johnson, LaRC	M
Crystal Jones, KSC	M
Mark Kowaleski, NSC	M
Jesse Leitner, GSFC	M
Donovan Mathias, ARC	M
Don Porter, LaRC	A
Bill Schoren, GRC	A
Cliff Watson, MSFC	M
Roselynne Strickland[1], MSFC	
Christopher Everett, ISL Inc.	S
Robert Youngblood, INL	S
Peter Rutledge, QA@RMS	S

[1] Software Assurance Working Group Representative

A VISION FOR SYSTEM SAFETY

Position Paper

1. Introduction

This position paper builds on previous years' efforts to assess the state of System Safety at NASA [1, 2]. It articulates a vision of System Safety into which we would like to see current NASA practice evolve in roughly a ten-year timeframe. The vision presented in this paper is informed by current best practices in System Safety within NASA [3], within other government agencies, and in the private sector. It is informed by the assessment and evaluation of System Safety called for by the recent Program/Discipline Questionnaire [4]. It reflects input from NASA stakeholders, most notably from the NASA System Safety Steering Group (S3G) [5], and is consistent with recent and ongoing OSMA initiatives in System Safety and Risk Management generally [6, 7, 8, 9, 10].

The System Safety vision presented in this paper establishes a mature future "target environment" for System Safety against which current NASA System Safety practice can be assessed. With a mature future target environment defined, implementation plans (IPs) can be rationally developed to move NASA most effectively towards System Safety maturity over the near-, mid-, and long-term (3 to 10 years). Such IPs are beyond the scope of this paper, but will be a necessary part of the overall effort to realize this System Safety vision.

2. What is System Safety and What is System Safety For?

Pragmatic Definition of "System Safety" at NASA

System safety is the application of scientific, engineering, and management principles, criteria, and techniques to optimize safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system life cycle. System Safety takes an integrated, system-level perspective towards safety, recognizing that safety is an emergent property that is defined only in the context of the whole system operating within a specified performance envelope. System Safety is an integral part of Systems Engineering and Risk Management that informs all decisions having the potential to affect safety.

Generally, System Safety practitioners will serve in one of two primary roles—either as an in-line member of a program/project team responsible for *ensuring* safety (e.g., supporting design-related activities), or in an independent safety *assurance* role, evaluating the System Safety work products of others [11].

In their safety ensurance role, System Safety practitioners will be organizationally situated so as to be able to work closely with Systems Engineers and Risk Managers as members of the team that is developing the system or service and providing it to the organization that formulated the

safety requirements for it and initiated the acquisition of it. System Safety practitioners will have primary responsibility for the Risk-Informed Safety Case (discussed below), either in their ensurance role of developing, presenting, and defending the RISC, or in their assurance role of evaluating the RISC on behalf of the acquiring organization for the benefit of its decision maker(s). System Safety practitioners serving in an ensurance role will likely be organizationally separated from System Safety practitioners serving in an assurance role.

A critical aspect of System Safety is support to Risk Management, especially risk acceptance decisions. In their safety ensurance role, System Safety practitioners will actively participate in design trade studies, providing a safety perspective through analytical inputs on design alternatives and through their knowledge of System Safety best practices. They will help to reduce or eliminate safety risks, properly characterize the risks that remain, and support processes to achieve and demonstrate that residual risk is "as low as reasonably practicable." In their safety assurance role, System Safety practitioners inform risk acceptance decisions through evaluation of the RISC on behalf of those responsible for them.

The technical authority function of OSMA relies crucially on the "assurance" role of System Safety, carried out to inform high-level concurrence on critical risk acceptance decisions [12].

3. What Is the Vision for System Safety?

> **Vision Statement**: NASA's vision for System Safety is that of a disciplined, unified, and efficient methodology and practice that enables the design and development, procurement, construction, operation, and retirement of aerospace systems for NASA that both meet imposed safety requirements and provide the highest reasonably practicable levels of safety to the public, the astronauts and pilots, the NASA workforce, the environment, and those valuable assets that the Nation entrusts to the Agency[2].

- Obligations to all stakeholders are met: high levels of safety are realized in practice.
- NASA System Safety practitioners are predominantly engineers experienced in aerospace technology and highly skilled in probability, statistics, mathematical modeling, and simulation. They understand and apply the principles of probabilistic thinking to their everyday work. They have a thorough understanding of the traditional safety and mission assurance (SMA) domains (safety, reliability and maintainability, quality assurance, and software assurance), as well as Risk Management and Systems Engineering.
- System Safety practice is carried out within a healthy safety culture: it is driven by a proactive concern for safety, which is achieved through rigorous application of best-

[2] Investigation of the Shuttle disasters generated comments about NASA organizational characteristics. This paper does not analyze the organizational implications of particular System Safety processes. The intent here is to delineate what good processes look like; this may have organizational implications, but those implications are beyond the present scope. System Safety processes are a necessary, but not in themselves sufficient, condition for safety.

available tools and methods, rather than complete reliance on process. System Safety process requirements are fulfilled not only in letter, but also in spirit. System Safety practitioners apply the scientific method to their work, and remain ever skeptical as they seek out new evidence for their safety arguments. Rather than passively accept the state of practice, they constantly seek ways to make the practice and methodology of System Safety better and more efficient. In accomplishing their important work to protect people, assets, and the environment, they do not lose sight of the Agency's goals and strategic direction. They are accomplished writers and speakers who will not hesitate to speak up for the risk-takers.

- The state of being "as safe as reasonably practicable" (ASARP) is attained through a collaboration of engineering disciplines comprising not only System Safety but also all other engineering disciplines that contribute to Mission Success.
- Uncertainties are understood as well as is practicable. Within an appropriately graded approach, dedicated efforts are made to obtain all relevant operating and test evidence. The implications of state-of-knowledge uncertainty for current decisions are understood. This includes uncertainty in model-based results, uncertainty regarding the applicability of available information, etc.
- Deviance is not normalized; penetrations of the analyzed performance envelope are investigated until they are understood.
- System Safety requirements strike the appropriate balance between "necessary" and "sufficient": requirements are sufficient to promote the desired outcomes, but no more burdensome than necessary. System Safety processes are streamlined relative to today's, but nevertheless cope successfully with the challenges discussed below.

This vision does not call for wholesale replacement of technical tools (such as Hazard Analysis) that have been applied for many years in System Safety practice at NASA and elsewhere. Continuous improvement in such technical analysis tools is desirable in principle, but is outside the scope of this vision. Rather, implementation of this vision is meant to apply such technical tools within an enhanced System Safety framework that better supports fulfillment of Agency needs, especially in light of the challenges articulated below.

4. Challenges to Be Met in Realizing the Vision

Achieving a high level of safety at NASA is challenging for several reasons:

- Space flight is inherently risky; safety margins are low because larger margins are impracticable.
- There is a significant diversity of technologies involved, many of them first-of-a-kind. System Safety requirements and System Safety practitioners are obliged to deal with both diversity and novelty.
- Development of NASA systems is often carried out by multiple organizations. Commercialization of certain developments is a recent special case.

- More generally, complex organizational structures and interfaces strongly affect the conduct of System Safety processes. Many different organizations are involved in all aspects of system development, and a key challenge is not to introduce new problems as requirements are flowed down, and systems are delivered across organizational interfaces. System interface issues have contributed to significant accidents at NASA.
- A high level of safety cannot, in general, be proven by a single demonstration. Flying a new system on a given day may prove that the system is *capable* of putting a payload into orbit, but a single flight cannot prove that the system is "adequately safe." Systems Engineering processes applied through the entire life cycle may eventually develop a system that achieves a good track record, but in general, even then, work is necessary to maintain that track record.
- Achieving safety calls for technical rigor. The key challenge is to develop processes that foster technical rigor rather than undermining it, in order to balance necessity with sufficiency in the promulgation of process requirements.

5. Strategy for Realizing the Vision

The technical essentials of risk acceptance decision-making are clear in principle. But because system development and operation involve many organizations, a special focus is needed on careful delineation of risk acceptance authority within each of those organizations and across organizational interfaces.

In many contexts, fulfillment of NASA's obligations requires consideration of aggregate risk. It may be appropriate to *manage* selected risks by defining risk-specific individual tasks, but *decision-making* needs to consider the bigger picture. In the past, System Safety practice has devolved to a focus on individual risks to the neglect of aggregate risk, and on the mechanics of fulfilling process requirements with concomitant neglect of technical rigor. It is difficult to solve "process" problems with new processes, and yet we are trying to do just that--we are trying to streamline System Safety-related processes, and yet improve results in critical ways.

For all the above reasons, System Safety must stress not only technical engineering methods and tools applied to safety engineering, but also System Safety processes. NASA already has many, many processes. As discussed below, some progress has been made in strengthening process requirements along these lines. In the coming years, the focus on process should be on streamlining processes, i.e., promulgating process requirements that promote technical rigor and clearly delineate risk acceptance authority, while not being so burdensome as to divert resources from the real technical job.

System Safety Practitioners Will:

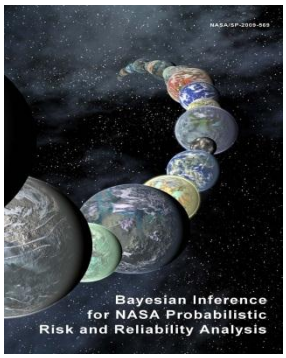
- Where appropriate, address AGGREGATE SAFETY PERFORMANCE at the system level, across the full scope of conditions that can cause death, injury, or illness to personnel, damage to or loss of equipment or property, or damage to the environment.
- Strive to comprehensively identify and analyze the full set of CREDIBLE SCENARIOS that have the potential to lead to adverse safety consequences, considering all hazard causes and propagation pathways through the system.
- Fully INTEGRATE with SYSTEMS ENGINEERING and RISK MANAGEMENT decision-making throughout the system lifecycle, to ensure the development and operation of systems that comply with levied safety performance requirements and are ASARP.
- Exploit SYNERGIES in the tools, techniques, and expertise used to ensure safety and those used to ensure Mission Success, such as those related to reliability, maintainability, quality assurance, and software assurance.
- Address UNCERTAINTY, using a “probabilistic mindset” to effectively reduce or eliminate identified uncertainties, and protect the system from unknown and underappreciated hazards.
- Be RESPONSIVE to new information, such as test and operational anomalies and performance trends, as well as successes and failures, in order to maintain a current understanding of the safety performance of the system and to proactively address emerging hazards.
- Be PRAGMATIC in the use of processes and techniques, adhering to a “graded approach” philosophy that matches the resources and depth of safety analysis to the complexity and importance of decisions being addressed, and accommodating the variety of insight/oversight acquisition models.
- Support SAFETY ASSURANCE activities by providing the oversight authorities with a coherent and compelling case for the adequacy of safety of the system that is substantiated by the best available evidence, and by assessing, on behalf of decision maker, the adequacy of cases provided by organizations supplying systems or services.
- Treat safety as a CORE VALUE by striving to learn new technical skills.
- EVOLVE in tandem with the evolution of the Agency, its strategic objectives, the nature of the technologies and systems addressed, and the System Safety state-of-the-art.

A linchpin of future System Safety practice will be the formulation and use of the Risk-Informed Safety Case (RISC), a NASA specialization of the idea of the "safety case," which has been widely applied in high technology situations around the world for many years. The safety case is a coherent, evidence-based argument that a given system is adequately safe for its intended application; formulation of the safety case requires more care and rigor from the system provider than does fulfillment of overly prescriptive process requirements, but the process of formulating and evaluating the RISC promotes better and more transparent risk acceptance decision-making, and a roadmap for managing risk in future lifecycle phases.

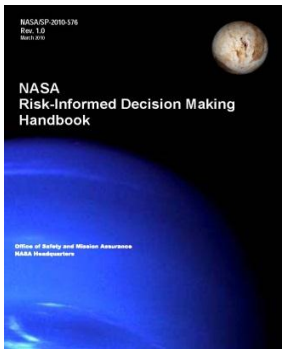
6. Recent Accomplishments

Following are accomplishments (listed in the chronological order) during the last five years that have set the stage for the further evolution of System Safety as proposed in this paper:

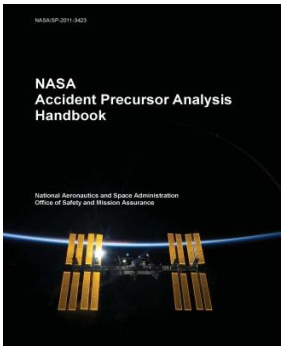
- Revision of NPR 8000.4, "Agency Risk Management Procedural Requirements" [13] – This NPR was significantly revised to require more explicit focus on risk-informed decision making (RIDM), and to delineate more clearly Risk Management processes in the context of organizational hierarchies, especially the coordination of Risk Management activities across organizational lines.



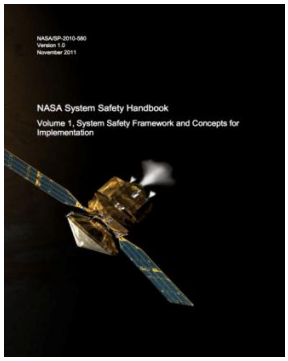
- Publication of NASA/SP-2009-569, "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis," [14] – This handbook covers the fundamentals of how data and information are used in risk and reliability analysis models and their potential role in decision-making. Understanding of these topics is essential to attaining a "probabilistic thinking mindset," which is the process of explicitly factoring the quality of a state-of-knowledge into models, analysis, and decision-making.



- Publication of NASA/SP-2010-576, NASA Risk-Informed Decision Making Handbook, [6] – This handbook describes processes for decision-making in the context of NASA Risk Management processes. It illustrates the use of decision analysis tools such as objectives hierarchies, influence diagrams, and decision trees through application to NASA examples.
- Establishment of the System Safety Steering Group (S3G) – The S3G was chartered by Bryan O'Connor, then NASA's Chief Safety and Mission Assurance Officer, on October 22, 2010 [15], "to develop Agency-wide plans and strategies" to improve System Safety and for its members to serve as champions at their Centers. The S3G has been meeting periodically and has been involved in the development of the System Safety Vision and associated products.

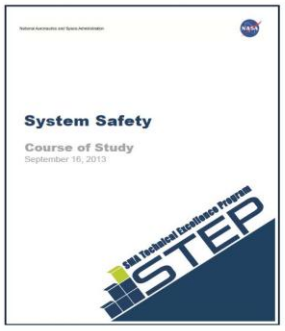


- Publication of NASA/SP–2011-3423, NASA Accident Precursor Analysis Handbook, [16] – This handbook provides methods for Accident Precursor Analysis (APA) within NASA. APA is a method to promote organizational learning from operational experience, without which reliability growth will occur more slowly, if at all. NASA has long had processes for collecting and analyzing operating experience; APA evaluates operating experience more systematically, in light of the performance envelope established in the RISC.

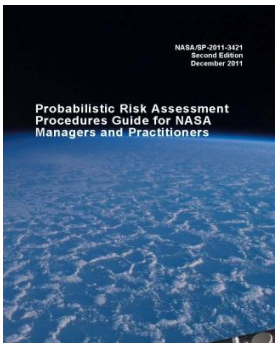


- Publication of NASA/SP-2010-580, NASA System Safety Handbook – Volume 1: System Safety Framework and Concepts for Implementation, [8] – This System Safety Handbook volume presents a System Safety framework that provides a coherent structure for organizing and unifying System Safety activities towards the achievement and demonstration of adequate safety throughout the system life cycle. Within the framework, System Safety activities are organized around the accomplishment of clearly stated safety objectives that collectively define adequate safety for the system, and are communicated to decision makers via the construct of the RISC.

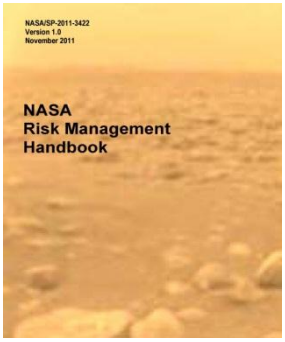
- Development of the white paper, "The Role of NASA Safety Thresholds and Goals in Achieving Adequate Safety," [17] – This paper provides a framework for implementing safety thresholds and goals in a way that reflects expectations that the safety of a new system will improve over time, and is consistent with the technical challenges inherent in assessing the safety of such systems. It is responsive to the need raised by the Aerospace Safety Advisory Panel (ASAP) [18] and others to consider the gap between actual risk and explicitly quantified risk, that gap being the so-called unknown and/or underappreciated (UU) risk.



- Development and Offering of More than a Dozen Training Courses for the System Safety Curriculum of the SMA Technical Excellence Program (STEP) – These courses are collectively designed to broaden the classical conception of System Safety, which is centered around qualitative hazard analysis and rule-based safety requirements to include modern and risk-informed approaches to safety analysis and management. The entire System Safety curriculum is now available online 24/7 through the System for Administration, Training, and Educational Resources for NASA (SATERN).



- Publication of NASA/SP-2011-342, Probabilistic Risk Assessment Procedures (PRA) Guide for NASA Managers and Practitioners, [19] – This edition of the PRA Guide expands coverage of the previous publication by including procedures for probabilistic modeling of physical processes and structural failures, and how PRA should be incorporated into Systems Engineering and Risk Management processes to support design and risk acceptance decisions.



- Publication of NASA/SP-2011-3422, NASA Risk Management Handbook, [7] – This handbook addresses the entirety of the NASA Risk Management process, including RIDM and Continuous Risk Management (CRM). The CRM process described is an enhanced version of NASA's traditional CRM paradigm. While it maintains the traditional core elements of CRM as practiced in the past, it builds upon the solid foundation of quantitative parameters and data made possible by the RIDM front-end of Risk Management.
- Engagement with Related Disciplines – As part of improving the knowledge and the integration of System Safety with other related disciplines, the S3G and the System Safety community were encouraged to review, comment on, and contribute to the NASA RM Handbook (NASA-SP-2011-3422) [7] and the PRA Procedures Guide (NASA-SP-2011-3421) [19]. Risk Management and PRA represent increasingly important areas of knowledge and skill for practicing System Safety professionals.

- Publication of NASA/CR-2013-218111, Context-based Software Risk Model Application Guide [20] – This handbook provides guidance for the Context-based Software Risk Model (CSRM) framework and process of software risk modeling and assessment. The CSRM framework has been specifically conceived and formulated to model and address the risk resulting from potentially mission-impairing software faults and failures that may affect the critical functions of space systems.

7. Current Activities

Current efforts to advance the practice of System Safety at NASA include:

- Development of a NASA System Safety Standard – A draft System Safety Standard has been produced and has been submitted for review to the S3G [10]. This standard does not try to reinvent fundamental System Safety processes that have been in place for many years; rather, the NASA System Safety Standard provides protocols that implement a systematic approach to System Safety as an integral part of Systems Engineering and Risk Management.
- Development of "NASA System Safety Handbook – Volume 2: Application of System Safety Concepts and Examples." [9] – A draft System Safety Handbook Volume 2 has been produced and is nearly ready for review by the S3G. This volume of the System Safety Handbook provides guidance in implementing the requirements and recommendations in the NASA System Safety Standard in a manner that builds upon the principles provided in Volume 1 of the Handbook. It provides detailed guidelines and associated examples for deriving and allocating safety requirements, developing a RISC, providing evidence to support the RISC, and inferring from the RISC and accompanying evidence whether or not the system is adequately safe.

- Development of a “System Safety II” training course for STEP – This two-day level 2 course presents the NASA System Safety framework and its elements. It addresses the relationship of System Safety to Risk Management and Systems Engineering, with a focus on the conduct of integrated safety analysis and its application to RIDM.

8. Plans to Implement the System Safety Vision

The following activities are currently planned for FY 14:

- Development of a System Safety Implementation Plan – NASA will assess the current System Safety baseline at the Agency and conduct a gap analysis relative to the System Safety Vision articulated in this document. NASA will use this gap analysis to develop an IP that addresses the 3-, 5-, and 10-year timeframes. The IP will build on the work that has been accomplished to date and that which is currently in progress.
- Integration of System Safety and Mission Success – Because of the large degree of overlap between the technical content of System Safety and that of Mission Success, they will be integrated into the combined methodology and practice of System Safety and Mission Success. This integration will take advantage of the high degree of synergy between System Safety and Mission Success, such as in the areas of scenario development, design and operation support, Risk Management, and assurance activities.

Finally, and perhaps most importantly, efforts will continue to engage the System Safety community throughout the NASA organizational structure in partnership to:

- Communicate the System Safety vision contained herein and modify it as necessary based on input from NASA stakeholders (i.e., to realize a shared vision), and
- Establish and maintain the objective of achieving the System Safety vision along the timeline set forth in the IP, working with NASA stakeholders towards a common goal of achieving the highest practicable levels of safety for NASA systems.

We are committed to fulfillment of NASA’s obligations to our stakeholders, despite evolving challenges in budget and in institutional arrangements (e.g., commercialization). The System Safety community of practice cannot fulfill this vision alone, but, as explained above, we believe that we understand what needs to be done in order to fulfill its obligations. Significant steps have already been taken, others are currently underway, and more are planned.

9. References

1. NASA, “System Safety State of the Discipline (SoD): Areas for Improvement,” January 12, 2011.
2. NASA, “NASA System Safety - State of the Discipline (SoD) 2012,” August 23, 2012.
3. NASA/SP-2011-6127-VOL-2, Constellation Program Lessons Learned, Volume 2: Detailed Lessons Learned, Washington, DC, Spring 2011.
4. NASA, “Discipline/Program Questionnaire - System Safety,” May 23, 2013.

5. NASA, “System Safety Vision Questionnaire,” presented to the S3G on July 10, 2013.
6. NASA, NASA/SP-2010-576, *NASA Risk-Informed Decision Making Handbook*, Washington, DC. April 2010.
7. NASA, NASA/SP-2011-3422, *NASA Risk Management Handbook*, Washington, DC. November 2011.
8. NASA, NASA/SP-2010-580, *NASA System Safety Handbook Volume 1, System Safety Framework and Concepts for Implementation,* Washington, DC. November 2011.
9. NASA, NASA/SP-XXXX-XXX, *NASA System Safety Handbook Volume 2, Application of System Safety Concepts and Examples,* Washington, DC. (Draft).
10. NASA, NASA STD-XXXX, *NASA System Safety Standard,* Washington, DC. (Draft).
11. Vesely, W., “Systematic Quantification of the Prior Risk Assurance of a New System Using Bayesian Evidence Analysis,” International Journal of Performability Engineering, Vol. 9, No. 6, November 2013.
12. NASA, NPD 1000.0, *Governance and Strategic Management Handbook*, Washington DC, August 2008.
13. NASA, NPR 8000.4, *Agency Risk Management Procedural Requirements*, Washington, DC, 2008.
14. NASA, NASA/SP-2009-569, *Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis*, Washington, DC, June 2009.
15. NASA, “NASA System Safety Steering Group Charter,” October 22, 2010.
16. NASA, NASA/SP-2011-3423, *NASA Accident Precursor Analysis Handbook*, Washington, DC, 2011.
17. NASA, “The Role of NASA Safety Thresholds and Goals in Achieving Adequate Safety,” June 20, 2012.
18. ASAP, *Aerospace Safety Advisory Panel Annual Report for 2011*, Washington, DC. 2012.
19. NASA, NASA/SP-2011-3421, *Probabilistic Risk assessment Procedures Guide for NASA Managers and Practitioners, Second Edition*, Washington, DC, December 2011.
20. NASA, NASA/CR-2013-218111, *Context-Based Software Risk Model (CSRM) Application Guide*, Washington, DC, October 2013.