Application of “Safety Case” at NASA

Presented at the Safety Case Workshop Sponsored by the G-48 Committee and A-P-T Research

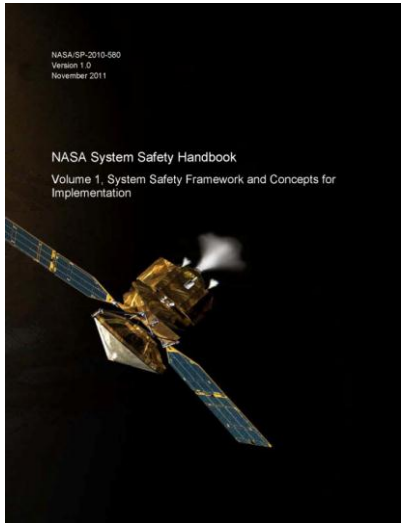
Huntsville, AL
January 14, 2014

Homayoon Dezfuli, Ph.D.
NASA Technical Fellow (System Safety)
Office of Safety and Mission assurance (OSMA)
NASA Headquarters

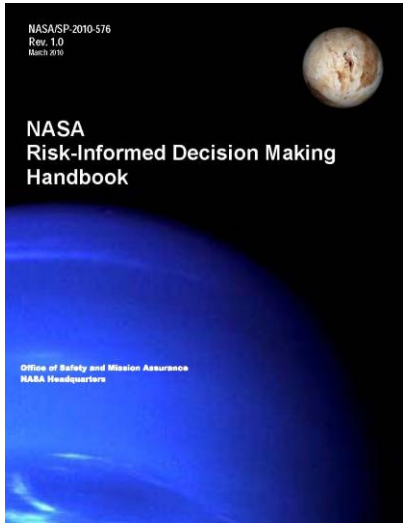
Disclaimer and Acknowledgments

This presentation reflects our current thinking regarding the future of system safety at NASA. The material contained herein is provided for informational purposes only, in the spirit of sharing our ideas with our industry partners, and should not be viewed as the official position of NASA.

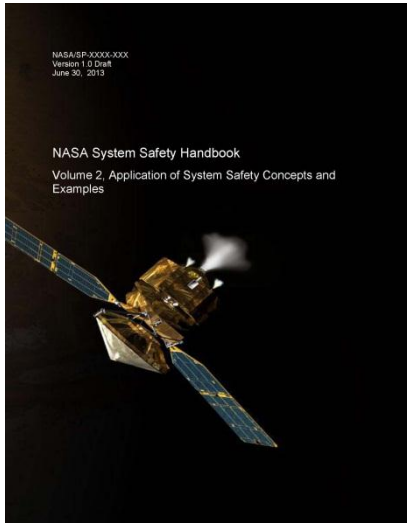
The following sources were used in the development of this presentation.



[NASA/SP-2010-580]



[NASA/SP-2010-576]

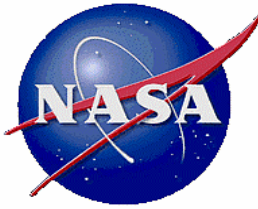


[NASA/SP-2013-XXX (Draft)]

Outline

- Driving Forces that Influenced the Evolution of System Safety at NASA
- Evolution of Risk Management
- The Concept of Risk Tolerance
- Evolution of System Safety
- The Concept of Adequate Safety
- The Issue of Risk Analysis Completeness
- The System Safety Framework (Risk-Informed Safety Case (RISC) Development and Evaluation)
- Summary
- Supplementary Slides

Setting the Stage for Why SS Evolution Cannot be Discussed in Isolation of Risk Management and Systems Engineering

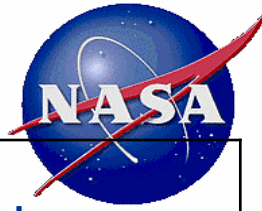


- **Risk Management (RM):**
  - Manage risks across all mission execution domains of safety, technical, cost, and schedule
- **Systems Engineering (SE):**
  - Do the best possible job of meeting overall mission / program / project goals, striking balance between competing objectives
- **System Safety (SS):**
  - Support development of systems that satisfy safety requirements and additionally are as safe as reasonably practicable, and substantiate the claim of "adequate safety" to decision-makers in contexts ranging from KDP reviews to operations

Driving Forces and Trends

1960s – 1970s	• Rush to land people on the moon (Apollo Program) • Money is no object • Testing and retesting • Apollo 1 launch pad fire (1967) leads to increased emphasis on a systematic safety program during the design process • Recognition of high risk and the need to succeed in spite of it ("Failure is not an option") • Emphasis on hazard analysis, FMEAs, CILs, and control of individual hazards
1980s – 1990s	• Increase in design complexity (Space Shuttle Program) • Money is more limited • Tendency toward process proliferation • Increase in complacency due to previous successes • Challenger accident occurs (1986) • Presidential Commission recommends more emphasis on safety culture and improved management practices and better trend analysis (Rogers Report, 1986) • The National Research Council of the National Academy of Sciences recommends a more integrated approach to safety assessment and CIL waivers (1988) • Renewed increase in complacency due to record of successes for crewed flights • NASA adopted "Faster, better, cheaper" philosophy • Failure of Mars robotic missions leads to concerns about "faster, better, cheaper" • Reliance on software (SW) starts to increase, along with the incidence of SW related failures

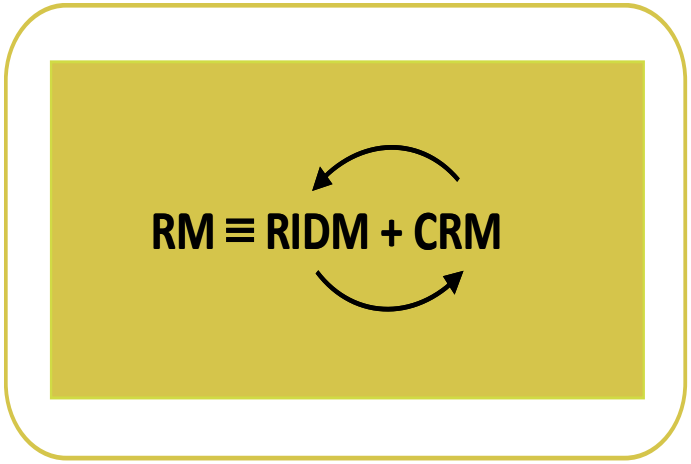
Driving Forces and Trends (cont.)



2000s – Present	• Columbia accident occurs (2003) • CAIB report highlights organizational and management problems and recommends conducting trend and risk analyses at multiple levels (subsystem, system, and enterprise) • Detailed probabilistic risk assessments for Shuttle and ISS • Increase in computational capabilities leads to increased use of physics modeling & simulation • Application of PRA to inform design decisions • Introduction of probabilistic safety thresholds and goals • Emphasis on tying safety requirements to safety performance objectives • Increased emphasis on holistic approaches (consider system/software/human interactions) • Questions raised about the reliability of PRA as a predictor of aggregate risk due to the historical importance of unknown and underappreciated (UU) scenarios
Present and Future	• Budget tightening • Emphasis on the need for graded analysis and for assessing the credibility of models • Increase of reliance on the commercial sector with emphasis on technology transfer and commercial crew certification • Increased emphasis on the regulatory side of system safety (e.g., risk acceptance) • Changes in acquisition models • Emphasis on NASA's role in developing new technologies independent of defined missions • Increasing emphasis on strategic risk, including tradeoffs between risk of mission failure and potential rewards, but with primary importance on protecting human lives and safety • Emphasis on better treatment of uncertainty & innovative means to protect against UU risks • Trend toward bringing organizational issues into safety evaluations • Movement toward model-based systems engineering • Integration of system safety and mission success

NPR 8000.4A Evolved NASA's Risk Management to entail two Complementary Processes

- **Risk-Informed Decision Making (RIDM)**
  - To inform systems engineering decisions through better use of risk and uncertainty information in selecting among alternatives and establishing baseline performance requirements
- **Continuous Risk Management (CRM)**
  - To manage aggregate performance risks over the course of the development and implementation phases of the life cycle to assure that requirements related to safety, technical, cost, and schedule are met



NPR 8000.4A Emphasizes Analysis of Decisions and Consideration of Aggregate Risk

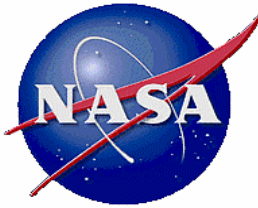
Inclusion of RIDM in RM has the effect of increasing emphasis on analysis and decision-making

- Development of requirements based on aggregate performance measures such as Probability of Loss of Crew (P(LOC)), Payload Capability (Kg), Time to Completion (Days), Total Program Cost ($)
- Risk measured in terms of uncertainty in being able to meet each performance requirement
- Uncertainties assessed in terms of their aggregated effect on the quantification of the performance measures

CRM was expanded to be a tool for managing aggregate performance risks

- Evaluation of the effects of individual “risks” on the aggregate performance measures and associated performance risks
- Determination of corresponding performance risk drivers that most significantly affect the likelihood of not meeting the aggregate performance requirement
- Application of risk management efforts to the mitigation of risk drivers

NPR 8000.4A Defines Risk in the Context of Performance Objectives or Requirements



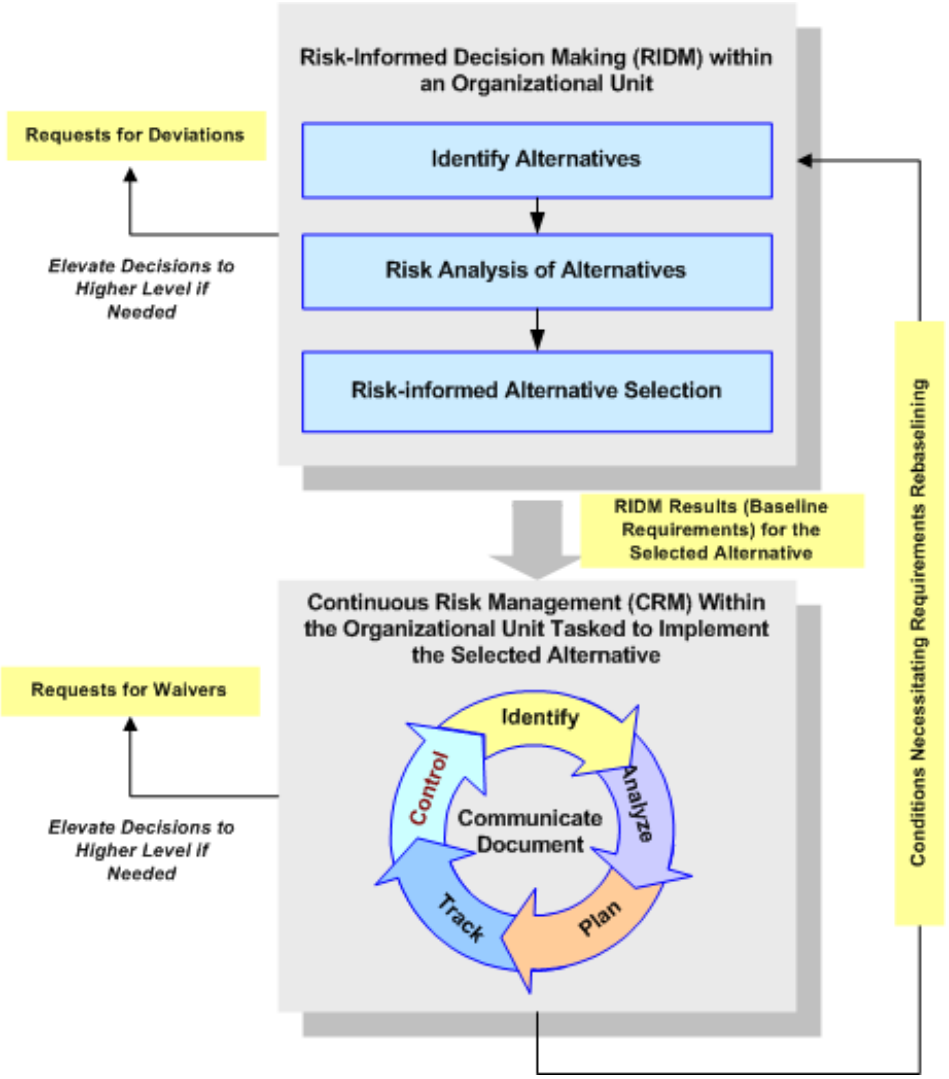
> **"Risk is the potential for performance shortfalls, which may be realized in the future, with respect to achieving explicitly established and stated performance requirements."**

Performance shortfalls may be related to institutional support for mission execution or to any one or more of the following mission execution domains:

- **Safety (e.g., avoidance of injury, fatality, destruction of key assets, environmental damage)**
- **Technical (e.g., thrust or output, amount of observational data acquired)**
- **Cost (e.g., execution within allocated cost)**
- **Schedule (e.g., meeting milestones)**

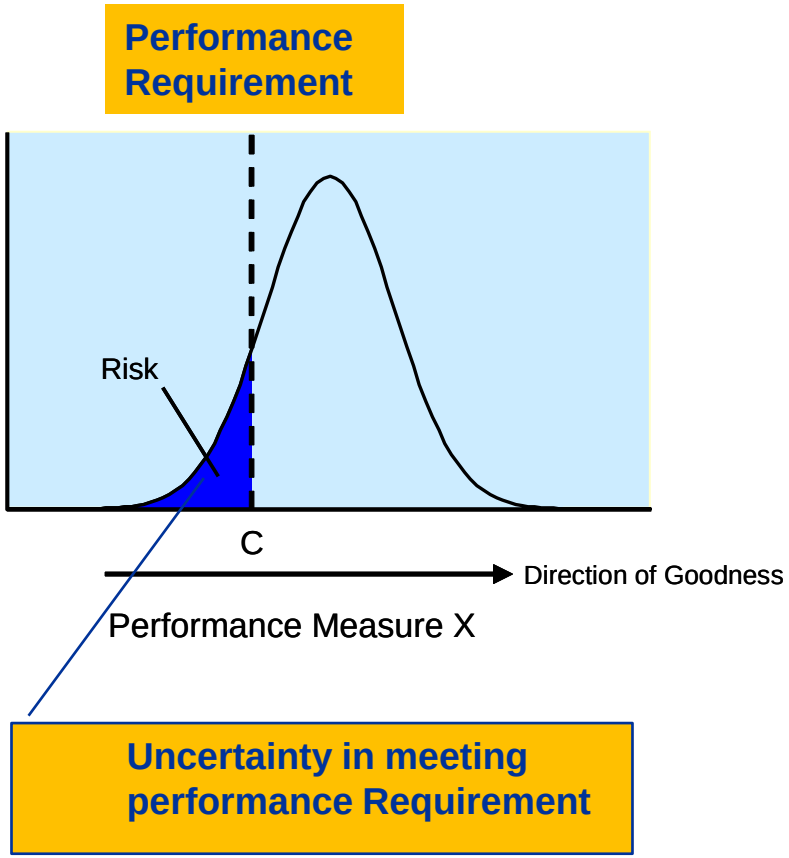
Relationship Between RIDM and CRM

- Selection of an alternative (e.g., a design concept) includes specification of baseline performance requirements
- CRM processes manage the risk of not achieving that performance baseline, until the baseline is changed
- Per 8000.4A, each organizational unit's authority for risk acceptance is to be spelled out in its Risk Management Plan, with the concurrence of the higher-level unit

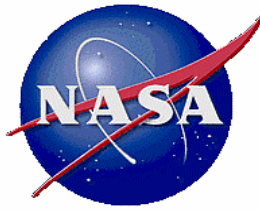


The Concept of "Risk Tolerance"

- **Within NASA's Risk Management framework, "risk tolerance" (a.k.a. acceptance) is the amount of uncertainty (or lack of confidence) accepted in the argument that the system meets an aggregate performance requirement**
- **There is a separate risk tolerance for each aggregate performance requirement**

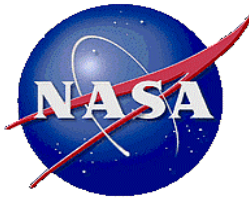


An Example



- Consider an acquisition of a launch system supposed to have a Probability of Loss of Crew (P(LOC)) < “threshold” (e.g., 1E-3) for a particular mission.
  - There has already been a high-level decision to accept P(LOC)<threshold.
  - Currently, acceptance of this P(LOC) is required of the risk-takers themselves and other stakeholders
- ***The risk being accepted by the Acquirer is the risk that P(LOC) > threshold.***
- In order to justify that risk acceptance decision, the Acquirer needs assurance (have enough confidence) that P(LOC) < “threshold”
- In the above example, P(LOC) is ONLY an example. Other kinds of requirements may also be imposed.
- The point of the example is that in general, the Acquirer needs to manage the risk that the actual performance falls short of requirements.

Evolutions in System Safety Practice

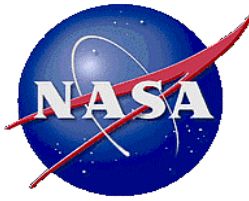


- **Specific evolutions in System Safety practice are warranted by the general "drivers" noted earlier. Additional key motivating factors include:**
  - **Promote an *objectives-driven* approach to system safety that explicitly focuses system safety efforts on the achievement of operationalizable safety objectives**
  - **Allow *flexibility* in the means by which system safety is analyzed and achieved, thereby accommodating next-generation engineering modalities and promoting *innovation***
  - ***Streamline* system safety activities (e.g., safety analysis activities) in order to reduce redundancies and potential inconsistencies, thereby achieving cost savings and lowered risk**
  - ***Unify* system safety with systems engineering and risk management, in order to ensure effective risk-informed decision making throughout the system life cycle**

Evolutions in System Safety Practice (cont.)

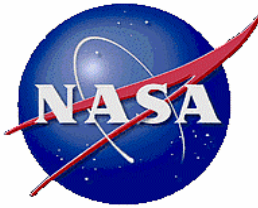
- **Priorities:**
  - **Management of safety risk across organizational interfaces (acquirer / provider), and at the integrated system level, especially in light of commercialization**
  - **Improved technical basis for risk acceptance decisions**
- **Unfortunately, "safety" is not observable in the same way as physical performance. *Evidence* of safety can be provided, but in complicated settings, safety cannot be conclusively *proven.***
- **Therefore, when we require "safety," what we get in practice is essentially a proxy for safety.**
- **For human space flight in particular, and high-risk / high-value undertakings in general, the proxy needs to be as good a proxy as it can be, because it is supporting an extremely important risk acceptance decision.**

Evolutions in System Safety Practice (cont.)



- For this reason, “safety cases” have been applied ever more widely for approximately half a century in many countries and in multiple technology domains.
- Whenever one organization needs to make a risk acceptance decision regarding a technology supplied by another organization, “safety case” is a useful idea
  - Regulators licensing a hazardous facility, making a risk acceptance decision on behalf of society
  - NASA making a risk acceptance decision regarding a launch system
    - Deciding whether to proceed to the next development phase
    - Deciding whether obligations to NASA’s risk takers have been / are being met
    - Deciding whether the system is (or will be) adequately safe
- Accordingly, the system safety framework of NASA/SP-2010-580 is predicated on specialization of this concept to the NASA environment, supporting Risk Management in general and prudent approaches to safety risk in particular

The Concept of "Adequate Safety"



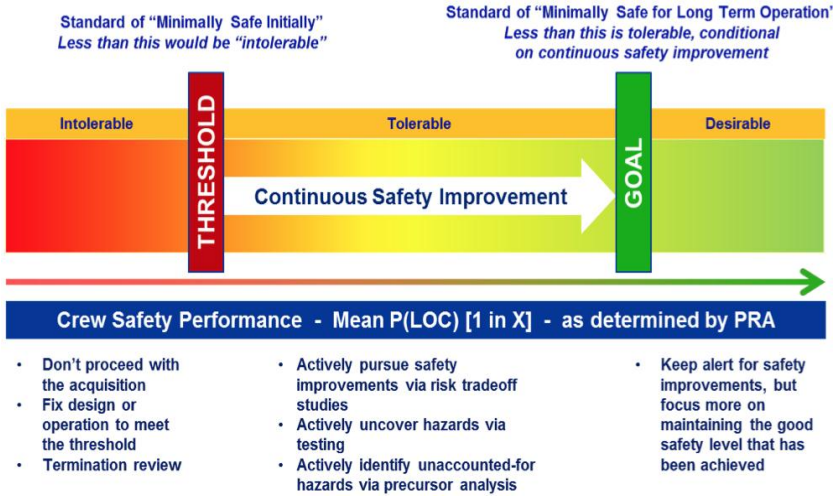
- **The trigger for dealing with the issue of "adequate safety" was the NASA Aerospace Safety Advisory Panel (ASAP) Recommendation 2009-01-02a:**

  "The ASAP recommends that NASA stipulate directly the acceptable risk levels—including confidence intervals for the various categories of activities (e.g., cargo flights, human flights)—to guide managers and engineers in evaluating "how safe is safe enough."

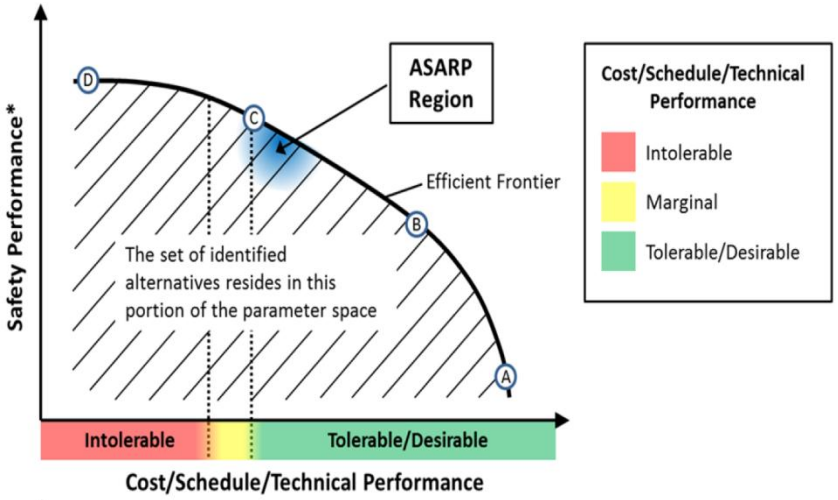
- **NASA accepted the ASAP recommendation and committed to establishing safety thresholds and goals for human space flight**
  - **Safety threshold expresses an initial minimum tolerable level of safety**
  - **Safety goal expresses expectations about the safety growth of the system in the long term**
- **NASA/SP-210-580 articulates two fundamental principles of safety that together constitute "adequate safety":**
  - **The system meets or exceeds a minimum tolerable level of safety; below this level the system is considered unsafe**
  - **The system is as safe as reasonably practicable (ASARP)**

Principles of Adequate Safety

- **An adequately safe system is one that adheres to the following fundamental safety principles:**
  - **Meeting minimum tolerable levels of safety (i.e., aggregate risk)**
    - Below the minimums the system is considered unsafe
    - Minimums may be applied to any safety performance measure, e.g., P(LOC), P(LOM), P(LOV), E_c, P(environmental contamination)
    - Minimums may evolve from initial thresholds to long-term goals
  - **Being as safe as reasonably practicable (ASARP)**
    - Decisions affecting safety are risk-informed
    - Safety is prioritized within constraints on operational effectiveness, schedule, and cost



Minimum Tolerable Levels of Safety



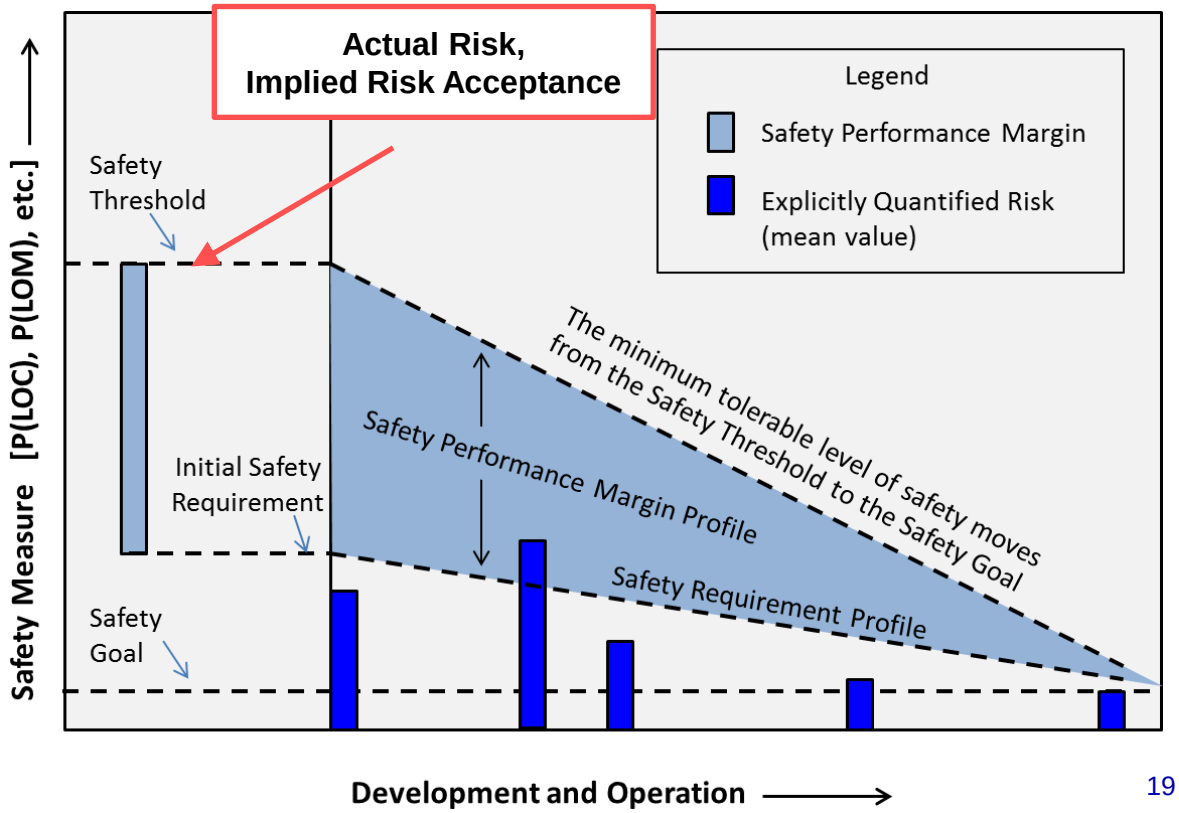
As Safe As Reasonable Practicable (ASARP)

The Issue of Risk Analysis Completeness

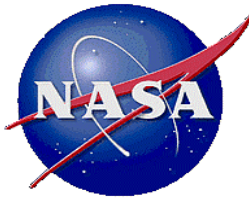
- **Safety goals and thresholds represent expectations about actual risk, including both known and unknown/underappreciated (UU) sources of risk**
  - ***Known sources of risk*** are amenable to explicit quantification via synthetic, scenario-based methods of analysis (e.g., PRA), and actuarial methods (when sufficient data are available)
  - ***UU sources of risk*** are not amenable to synthetic analysis or direct actuarial characterization, yet are historically recognized as significant contributors to risk
    - They tend to remain latent in the system until revealed by operational failures, precursor analysis, etc.
    - They tend to be most significant early in the system life cycle
    - They disproportionally reflect organizational issues and/or complex intra-system interactions

Accounting for Unknown/Underappreciated Risks

- ASAP and others have raised the need to consider the gap between *known* risk and *actual* risk when applying NASA safety thresholds and goals
- We use the concept of safety performance margin to account for UU risks
- Based on historical discrepancies between initially-calculated and eventually-demonstrated safety performance
- This provides a rational basis for deriving verifiable requirements on known risk

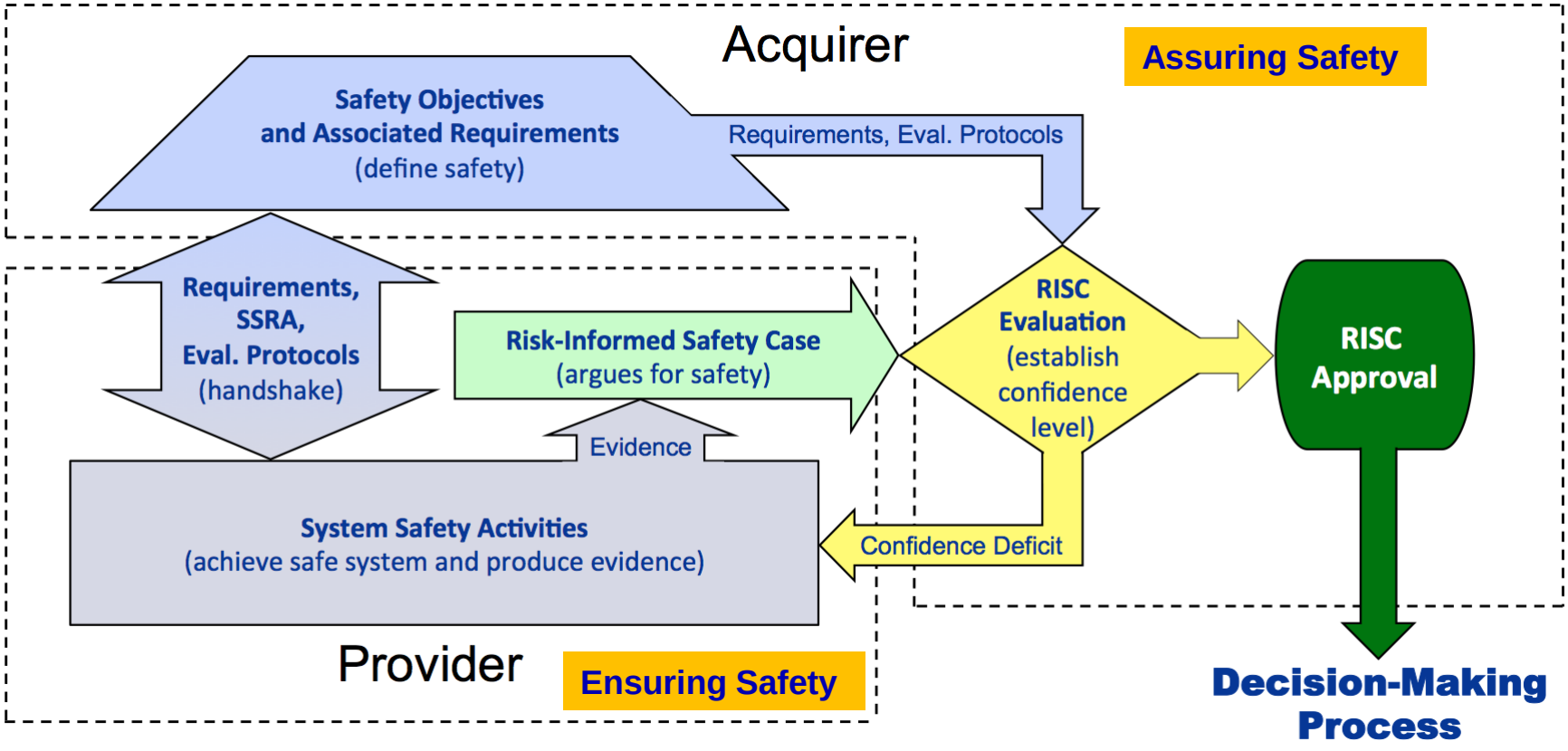


System Safety Framework

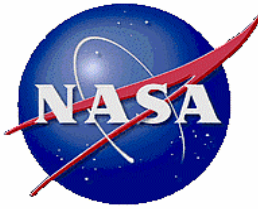


- The system safety framework of NASA/SP-210-580 is reflection of the evolution of the system safety approach as discussed earlier.
- The key four elements (functional areas) of this framework consists of the following:
  - Each program/project articulates operationalizable system safety objectives and associated verifiable safety-related requirements that derive from fundamental principles of safety
  - Program/project system safety activities are focused on the accomplishment of safety objectives, not just on the production of deliverables
  - The accomplishment of objectives is argued in a Risk-Informed Safety Case (RISC) that is evidentiary in nature and is presented and defended at major milestone reviews
  - The RISC (including supporting evidence) is evaluated to assess the veracity of the safety claims made therein in order to support risk acceptance decisions

NASA System Safety Framework (cont.)



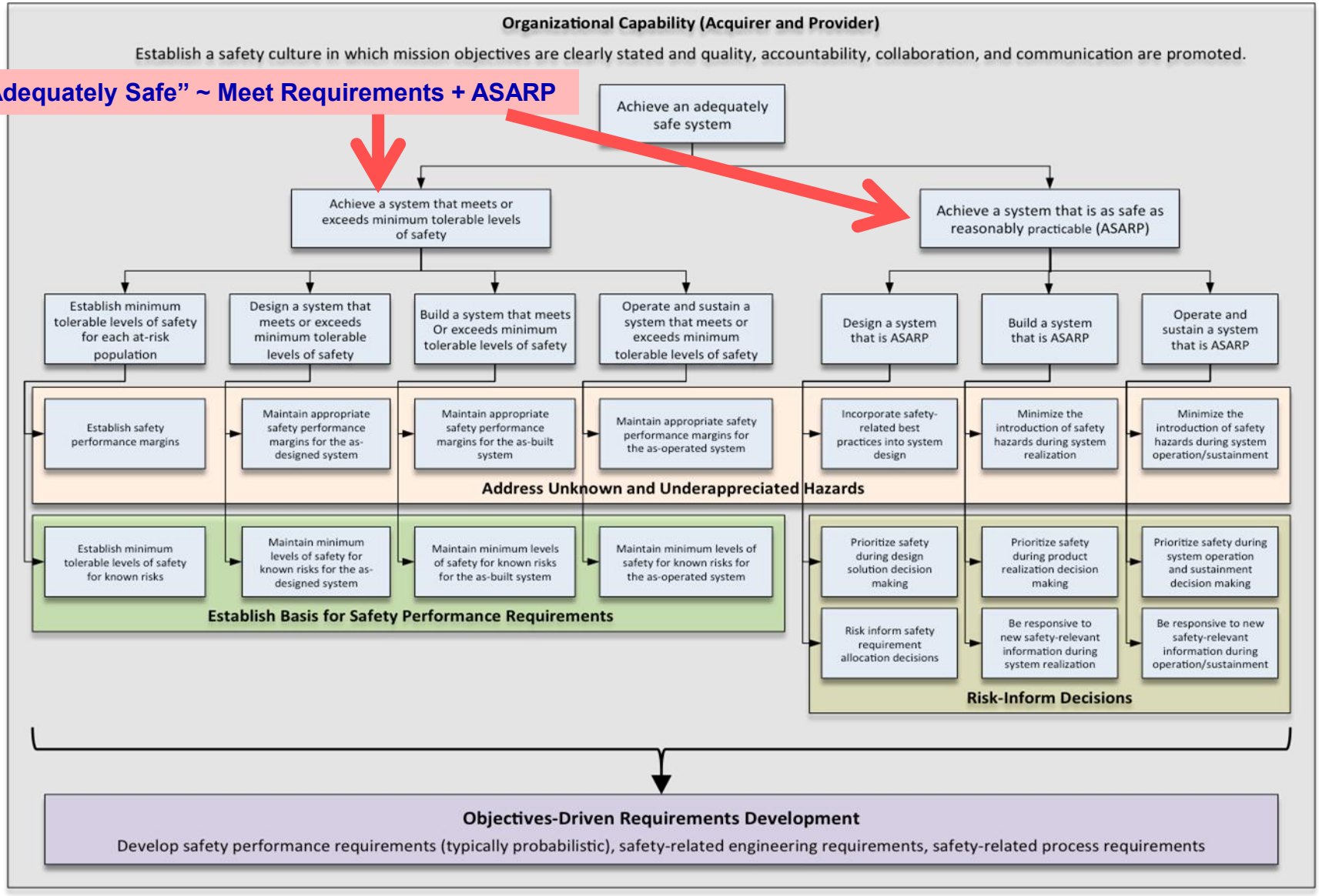
The Risk-Informed Safety Case is a Coherent and Evidentiary Statement of "How Adequately Safe" We are (or Will be) at a Given Stage of the Life Cycle



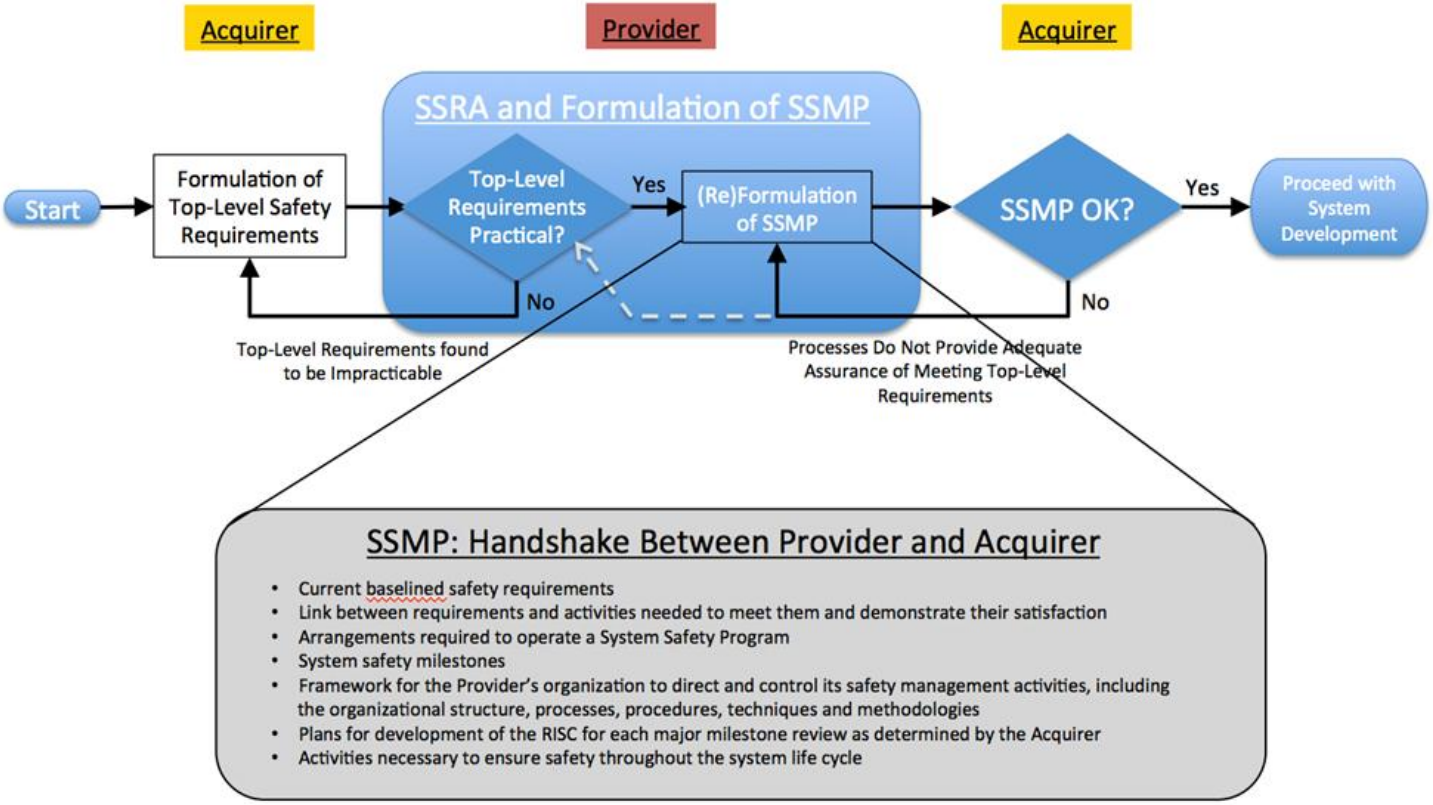
- The Risk-informed Safety Case (RISC) is a specialization of the "safety case" construct. The term 'risk-informed' is used to emphasize that adequate safety is the result of a deliberative decision making process that involves an assessment of risks, and strives for a proper balance between safety performance and performance in other mission execution domains
- The RISC gives the decision maker appropriate confidence and bases for safety claims regarding "adequate safety"
  - Assessing the veracity of claims
- Show what's being presumed
- Tie to Risk Management and assurance activities
- Show what needs to be accomplished
  - Performance allocations
  - Implied commitments (e.g., implementation of hazard controls)

Additionally, the RISC can serve as an organizing principle for system safety activities

Objectives-Driven Requirements Development *(Notional)*

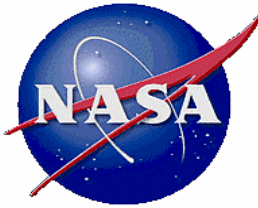


System Safety Requirements Analysis (SSRA) and System Safety Management Plan (SSMP)



- **SSRA is inspired by (and closely related to) MIL-STD-882's "SRHA", Task 203**
- **Handshake:**
  - **The Provider agrees to provide certain things that are deemed *necessary***
  - **The Acquirer agrees that these things are *sufficient***

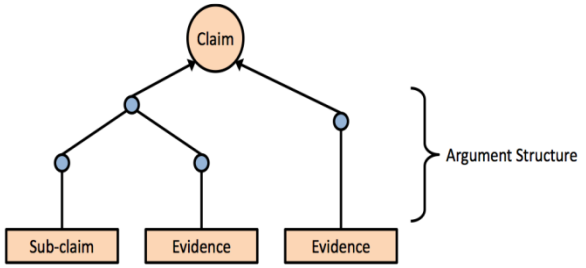
System Safety Activities

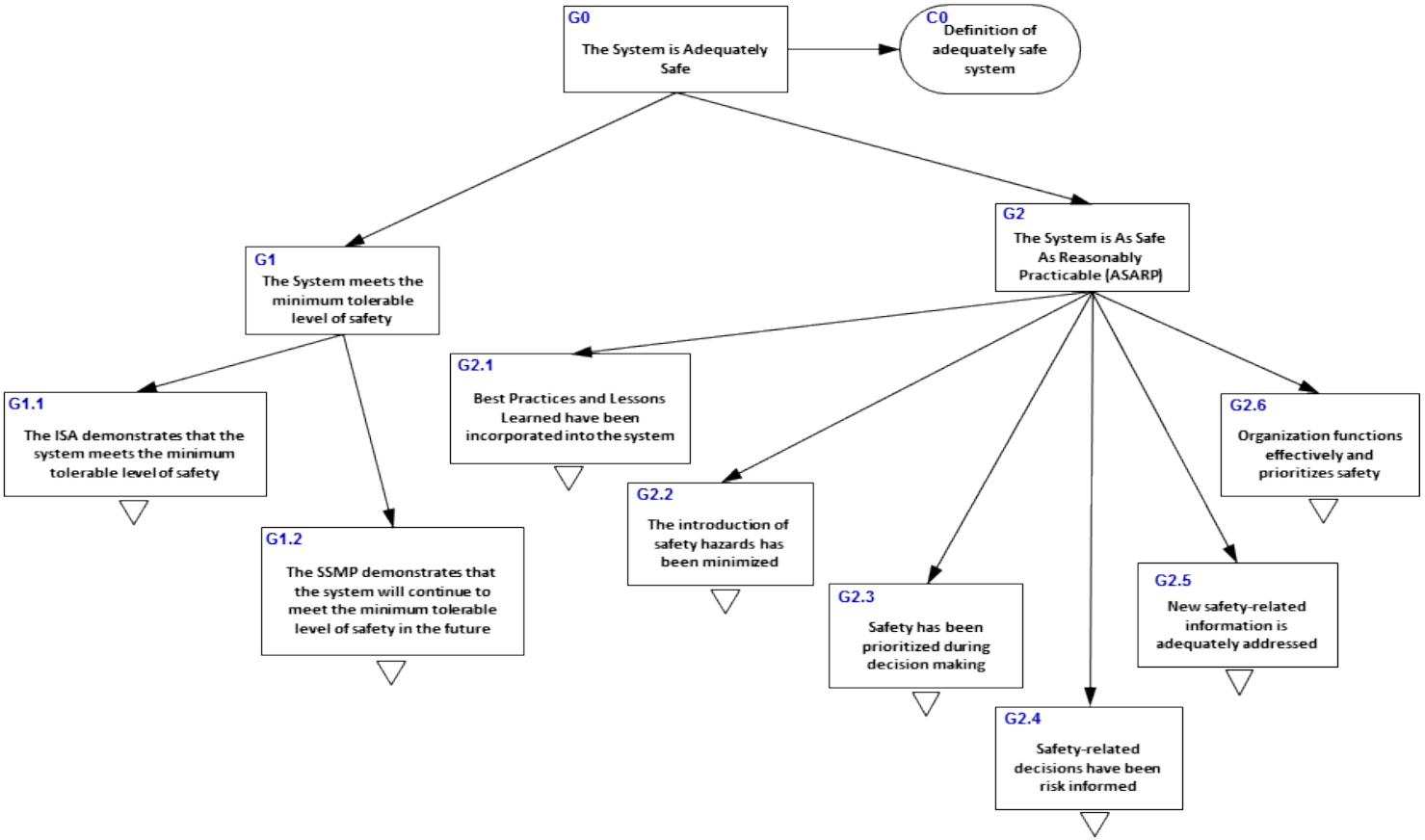


- **System safety activities include everything the Provider does to satisfy the levied safety requirements**
- **The initial activity is the development of a System Safety Plan (SSMP) that lays out the roadmap for the program/project with respect to system safety**
- **The central analysis activity is the conduct of an Integrated Safety Analysis (ISA)**
  - The ISA is a system-level, scenario-based analysis of potential accidents from all credible causes
  - It is scoped via a negotiated process between the Acquirer and Provider, allowing rigor to be tailored to areas of high utility (e.g., EDL vs. coast)
  - ISA provides a basis for identifying Safety-Critical Items (SCIs) and assuring their capability, reliability, and availability
- **Other system safety activities fall into the areas of requirements development support, system design support, program control and commitments support, and performance monitoring support**

RISC Development

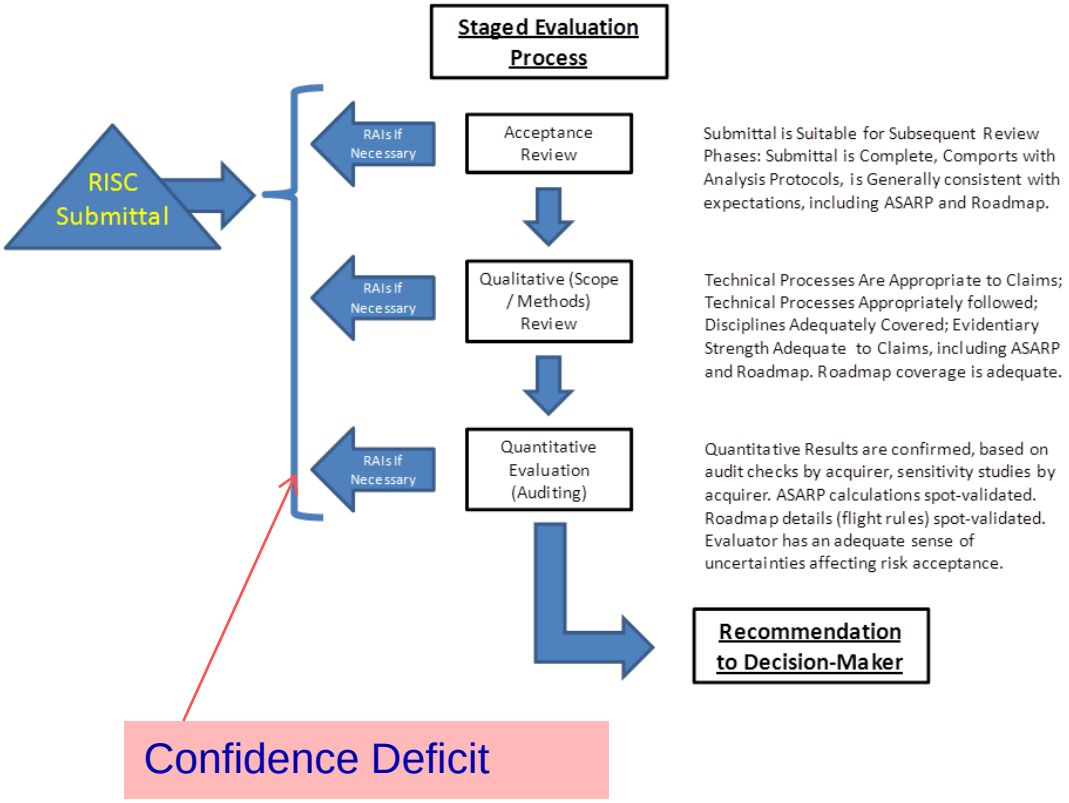
- **Elements of the RISC**
  - **An Explicit set of safety claims**
  - **Supporting evidence for the claim**
  - **Structured safety argument that links claims to evidence**

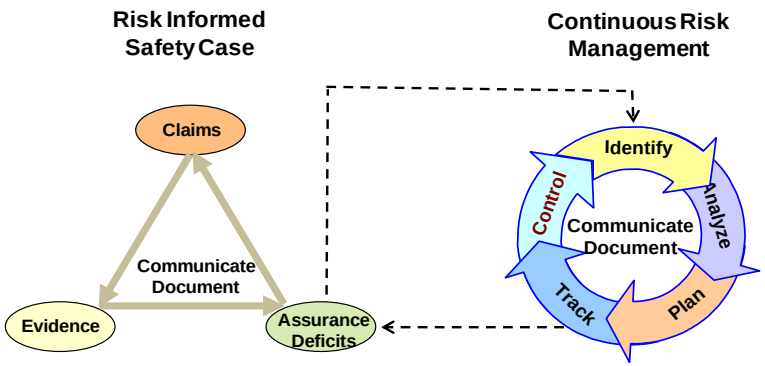




Evaluation of the RISC and Management of Assurance Deficits

RISC evaluation is carried out based on defined evaluation protocols for the system at its particular point in its life cycle.

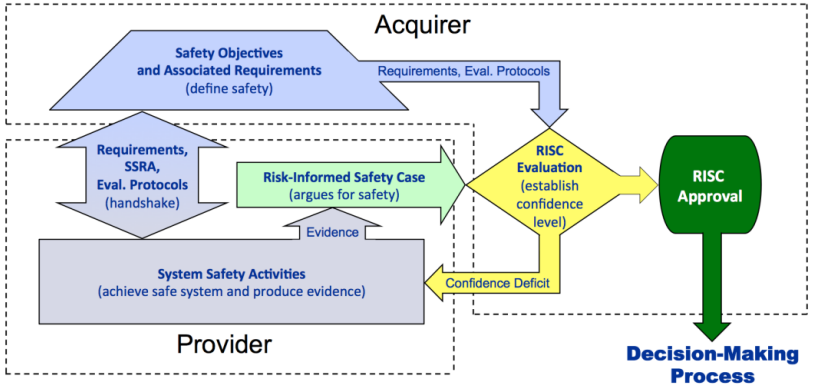




Relationship between Development of the Risk Informed Safety Case and Continuous Risk Management

Summary (1 of 4)

- **Our evolving System Safety framework makes essential use of the Risk-Informed Safety Case**
  - **What: The RISC presents the argument that the system's safety objectives are satisfied (and therefore that the system is adequately safe).**
  - **Who: The RISC is formulated by the provider and communicated to the acquirer.**
  - **Why:**
    - In the course of formulating the RISC, the provider considers how safety will be achieved and demonstrated.
    - Allows the acquirer to assess whether they are reasonably assured of the Adequate Safety of the system.
  - **When: For major decisions, including Key Decision Points (KDPs), throughout the lifecycle.**



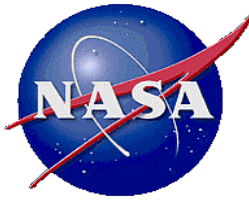
Summary (2 of 4)

- It is our intent to build upon, rather than replace, standards such as MIL-STD-882 by addressing NASA-specific needs that go beyond those addressed by existing documents. For example:
  - In its 2012 Annual Report, the Aerospace Safety Advisory Panel (ASAP) reiterated its belief that target levels of safety performance must be specified for NASA systems on a mission-specific basis, and that it is necessary to understand the tradeoffs between safety performance and performance in other domains (technical, cost, schedule) when programmatic decisions are made.
  - The “System Safety Requirements Analysis” has been inspired by the System Requirements Hazard Analysis (SRHA) concept in MIL-STD-882

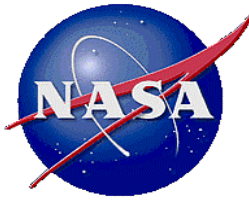
Summary (3 of 4)

- The present concept of the RISC is a specialization of the well-known general idea.
  - The term “risk-informed” is used here to emphasize that in NASA applications such as human rating, a determination of adequate safety is the result of a deliberative decision making process that necessarily entails an assessment of risks and tries to achieve a balance between the system’s safety performance and its performance in other areas.
  - The RISC, which evolves over the course of the system life cycle, supports decision making at system life cycle reviews and other major decision points.
- The RISC provides a complete set of information on safety at a point in the lifecycle
  - This set of information provides a safety baseline
  - Changes, controls, and operational events may be judged by looking at deviations from the baseline (prevent Normalization of Deviance)

Summary (4 of 4)

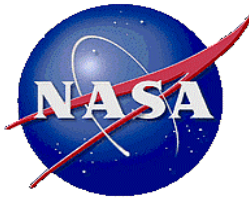


- We view the RISC as a key part of Risk Management
  - The current SS developments are specializations of NASA's Agency Risk Management Procedural Requirements (NPR 8000.4A)
  - Risk acceptance decision-making has always been central to the "safety case" topic, but in NASA's current development, receives more explicit emphasis: the Provider's RISC is the basis for the Acquirer's risk acceptance decision
  - In early life cycle stages, the conduct of the SSRA and the formulation of the RISC are part of general project Risk Management processes by both Acquirer and Provider
- The RISC is the ideal vehicle for making and evaluating an argument that a new space system, whether government or commercially developed, will meet safety performance thresholds and is As Safe as Reasonably Practicable (ASARP), as the basis for certification.



SUPPLEMENTARY SLIDES

Relationship to Existing SS Practice



- The SS framework of NASA/SP-2010-580, is not inconsistent with the traditional SS methods and tools (such as MIL-STD-882) based on identification of hazards and formulation of controls
- But the framework call for increased attention to aggregate risk and treatment of uncertainty
  - Situates classical SS practice within a Risk Management paradigm
  - Places increased emphasis on understanding the risks from a technical point of view:
    - Better integrating SS practice with the rest of Systems Engineering
    - Understanding and properly characterizing the limits of our state of knowledge
    - Making risk acceptance decisions in light of aggregate risk
  - Promotes the process of simplifying and rationalizing existing process requirements

MIL-STD-882E SS Management Tasks vs. NASA Draft SS Standard

882E Task No.	882E Task Title	Difference Compared to NASA SS Standard	882E Sub-Task Description	Difference Compared to NASA SS STD
101	Hazard identification and mitigation effort using the system safety methodology	Interpretation of "hazard" as any combination of conditions, departures, and consequences that have the potential to adversely affect system safety	Integrate hazard identification and mitigation into the DoD acquisition Systems Engineering (SE) process using the system safety methodology	Apply to risk management in general, not just acquisition. Perform analysis before mitigating. DoD's emphasis is different from ours. Theirs is on design for performance first, then budget and schedule, then mitigate. Ours is on safety first.
			The goal should always be to eliminate the hazard if possible	The goal is to reduce the risk to a level that is tolerable (e.g., meets safety thresholds and goals). On a hazard-by-hazard basis, however, elimination is still the ideal.
			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	In addition to meeting safety thresholds, goals, and cost/schedule constraints, the system should be made as safe as reasonably practicable (ASARP). The design order of precedence potentially fruitful approaches, but strategy selection should be risk-informed rather than a matter of precedence.
102	System Safety Program Plan (SSPP)	Equivalent to System Safety Management Plan (SSMP)	Develop a SSPP that documents the system safety methodology for the identification, classification, and mitigation of safety hazards as part of the overall SE process	The SSMP addresses those aspects of the systems engineering approach that affect safety, and those aspects of the risk management approach related to safety.
			The SSPP should be an integral part of the Systems Engineering Management Plan (SEMP)	OK
			The SSPP shall detail the tasks and activities that are required to implement a systematic approach of hazard analysis, risk assessment, and risk management	The SSMP is informed by System Safety Requirements Analysis (SSRA). The SSRA serves as the safety requirements "handshake" between Acquirer and Provider, and the SSMP serves as the process "handshake."

MIL-STD-882E SS Management Tasks vs. NASA Draft SS Standard (Cont.)

882E Task No.	882E Task Title	882E Sub-Task Description	Difference Compared to NASA SS STD
103	Hazard Management Plan (HMP)	Develop a HMP that documents a standard, generic system safety methodology for the identification, classification, and mitigation of hazards as part of the overall SE process	No separate document analogous to HMP. Superfluous, any differences with Task 102 can be covered in SSMP
104	Support Govt. reviews & audits	Support Government reviews, audits, and boards such as, but not limited to, program and technical reviews.	The Risk-Informed Safety Case (RISC) construct has been developed specifically to support the safety assurance function that such reviews and audits provide.
105	Integrated Product Team / Working Group Support	Participate as a member of designated IPTs or WGs.	Not covered in present SS Standard
106	Hazard Tracking System (HTS)	Establish and maintain a closed-loop Hazard Tracking System (HTS)	To underscore the impact that hazards have across mission execution domains (safety, technical, cost, schedule) the SS Standard specifies integration of safety management with risk management generally. It does not recommend a separate database for “safety risks.” It does specify that anomalies be assessed and addressed using a closed-loop process.
107	Hazard Management Progress Report	Submit periodic progress reports summarizing the pertinent hazard management and engineering activities that occurred during the reporting period	Risk reporting protocols, including safety risks, are negotiated between organizational units per the RM Handbook and documented in relevant plans (i.e., RMP, SSMP).
108	Hazard Material Management Plan (HMMP)	Implement a HMMP which shall be made available to the Govt. on request. HAZMAT management is an integral part of the RM effort within the program’s SE process	No separate document analogous to HMMP

MIL-STD-882E SS Management Tasks vs. NASA Draft SS Standard (Cont.)

882E Task No.	882E Task Title	882E Sub-Task Description	Difference Compared to NASA SS STD
201	Preliminary Hazard List	Compile a list of potential hazards early in development	The SS Standard specifies the development of a SSRA to inform the development of derived engineering and process requirements, and a system-level Integrated Safety Analysis that is methodologically non-prescriptive, integrates subsystem analyses, and evolves over the system life cycle. The ISA is a technical basis for identifying Safety Critical Items (SCIs) and determining the levels of capability, reliability, and availability to which they will be managed. The SS Standard does not explicitly address systems-of-systems except insofar as they are considered systems in their own right at a higher level of definition. Environmental safety is within the purview of the SS Standard.
202	Preliminary Hazard Analysis	Identify hazards, assess the initial risks, and identify potential mitigation measures	
203	System requirements hazard analysis (SRHA)	Determine the design requirements to eliminate hazards or reduce the associated risks for a system	
204	Subsystem hazard analysis (SSHA)	Verify subsystem compliance with requirements to eliminate hazards or reduce the associated risks	
205	System Hazard Analysis (SHA)	Verify system compliance with requirements to eliminate hazards or reduce the associated risks, including software and subsystem interfaces;	
206	Operating and Support Hazard Analysis (O&SHA)	Identify and assess hazards introduced by operational and support activities and procedures	
207	Health Hazard Analysis (HHA)	Identify human health hazards and evaluate proposed hazardous materials and processes using such materials	
208	Functional Hazard Analysis (FHA)	Identify and classify the system functions and the safety consequences of functional failure or malfunction. Identifying the safety-critical functions (SCFs), safety-critical item (SCIs), safety-related functions (SRFs), and safety-related items (SRIs)	
209	System-of-Systems Hazard Analysis	Perform and document an analysis of the System-of-Systems (SoS) to identify and eliminate or mitigate unique SoS hazards.	
210	Environmental Hazard Analysis (EHA)	Identify hazards to the environment throughout all life-cycle phases and modes	

MIL-STD-882E SS Management Tasks vs. NASA Draft SS Standard (Cont.)

882E Task No.	882E Task Title	882E Sub-Task Description	Difference Compared to NASA SS STD
301	Safety Assessment Report (SAR)	Provide a comprehensive evaluation of the status of safety hazards and their associated risks prior to test or operation of a system, before the next contract phase, or at contract completion	The RISC Report documents the RISC, and argues for the safety of the system.
302	Hazard Management Assessment Report (HMAR)	Same from the management perspective	Not a separate report. It's function is subsumed by the RISC Report
303	Test and Evaluation (T&E) Participation	Participate in the T&E process to evaluate the system, verify and validate risk mitigation measures, and to manage risks for test events	The SS Standard specifies that test plans and protocols shall be risk-informed to focus on priority system or subsystem designs, functions, and issues most affecting safety.
304	Review of engineering change proposals, change notices, deficiency reports, mishaps, and requests for deviation/waiver	Perform and document the application of the system safety process to Engineering Change Proposals (ECPs); change notices; deficiency reports; mishaps; and requests for deviations, waivers and related change documentation.	The ISA is used as a technical basis for deviations and waivers and it is kept current to reflect system changes, analysis deficiencies, operational experience including anomalies, and other safety concerns accepted into the RM process. The RISC is similarly updated, and re-evaluated.
401	Safety Verification	Define and perform tests and demonstrations or use other verification methods on safety-significant hardware, software, and procedures to verify compliance with safety requirements	The levels of SCI performance credited in the ISA shall be verified through testing, analysis, and application of engineering practices such as are in consensus standards.
402	Explosive Hazard Classification Data	Provide hazard classification data to support program compliance with the Department of Defense (DoD) Ammunition and Explosives Hazard Classification Procedures (DAEHCP)	Not needed as a separate topic in the SS Standard.
403	Explosive ordnance disposal data	Provide Explosive Ordnance Disposal (EOD) source data, recommended render-safe procedures, and disposal considerations.	Not covered in present SS Standard

RISC Evaluation Tool

- The RISC Evaluation Tool is a software tool designed to assist in the evaluation of RISCs
- The tool is developed in Microsoft Access, and is currently a pilot project with a beta-test version available
- Users follow a high-level, generic safety argument down to evidence nodes via a graphical representation of the safety argument
- Fields are provided for the evaluator to record findings, confidence scores, and assurance deficits
- Confidence scores may be automatically or manually aggregated through the tree
- Measures of percent complete, minimum confidence scores, number of outstanding RAIs, and aggregate confidence scores at each node throughout the safety argument are provided
- The tool also includes various reporting capabilities such as exporting an Excel file containing confidence scores and findings for each node in the tree

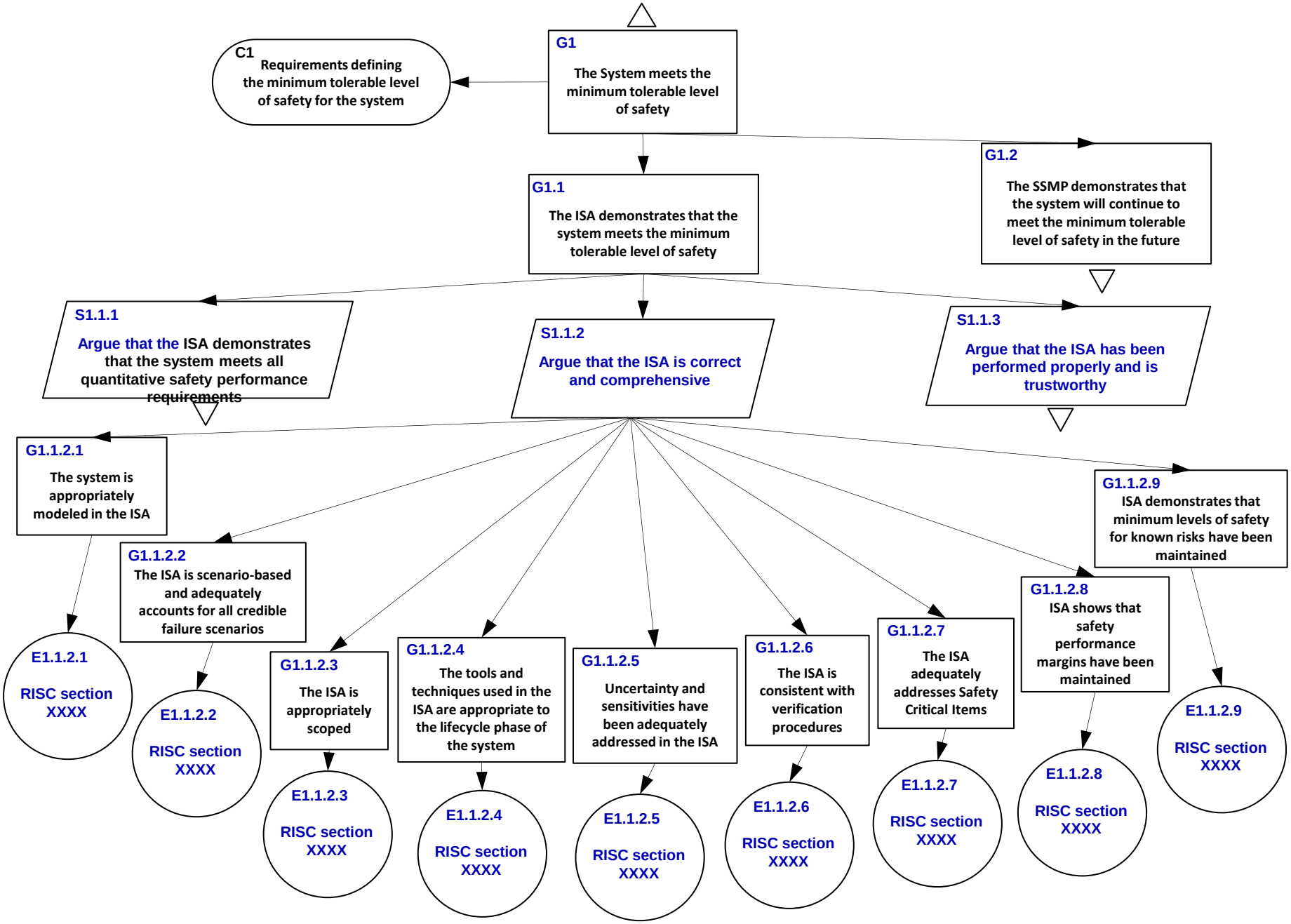
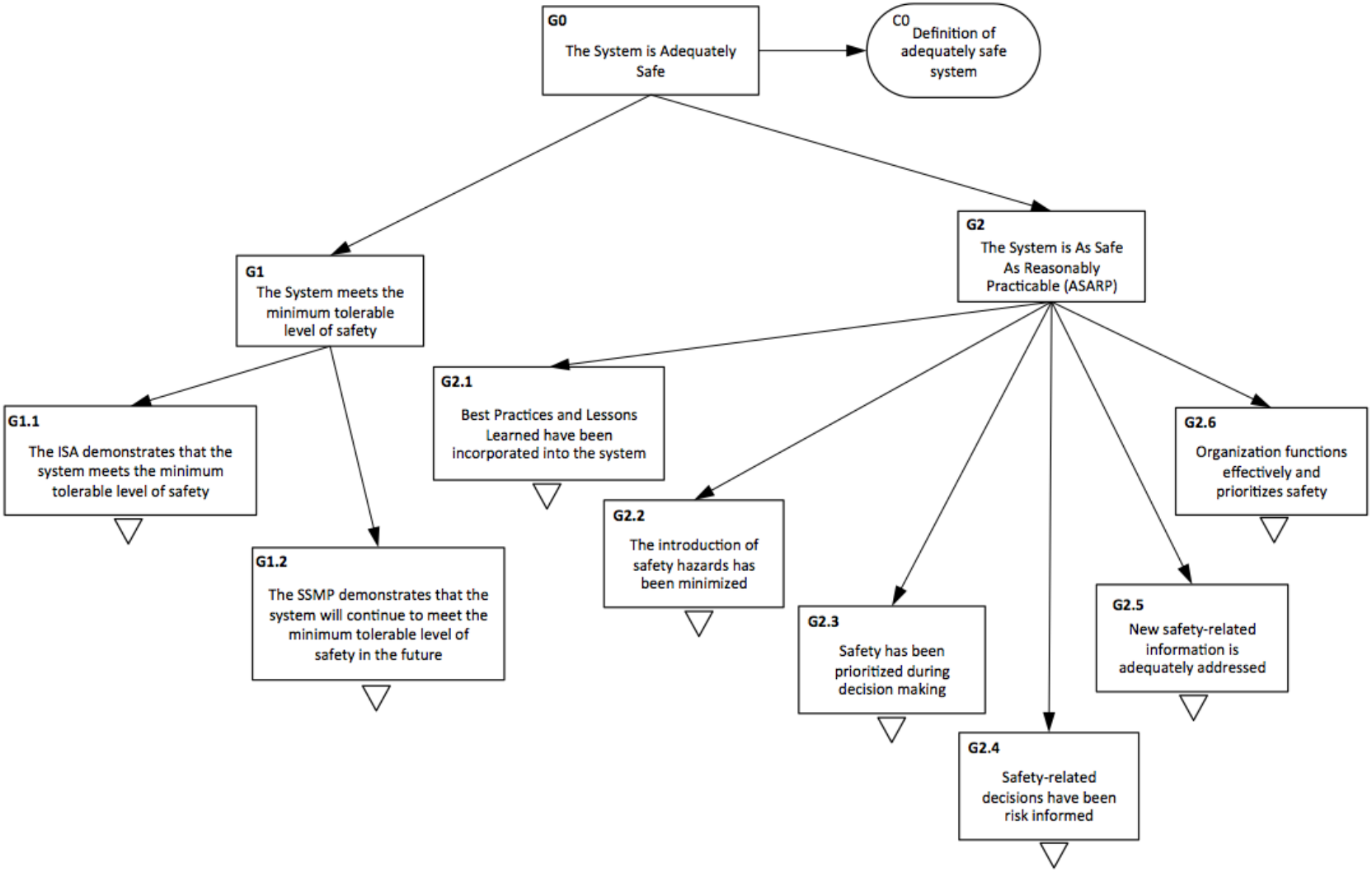
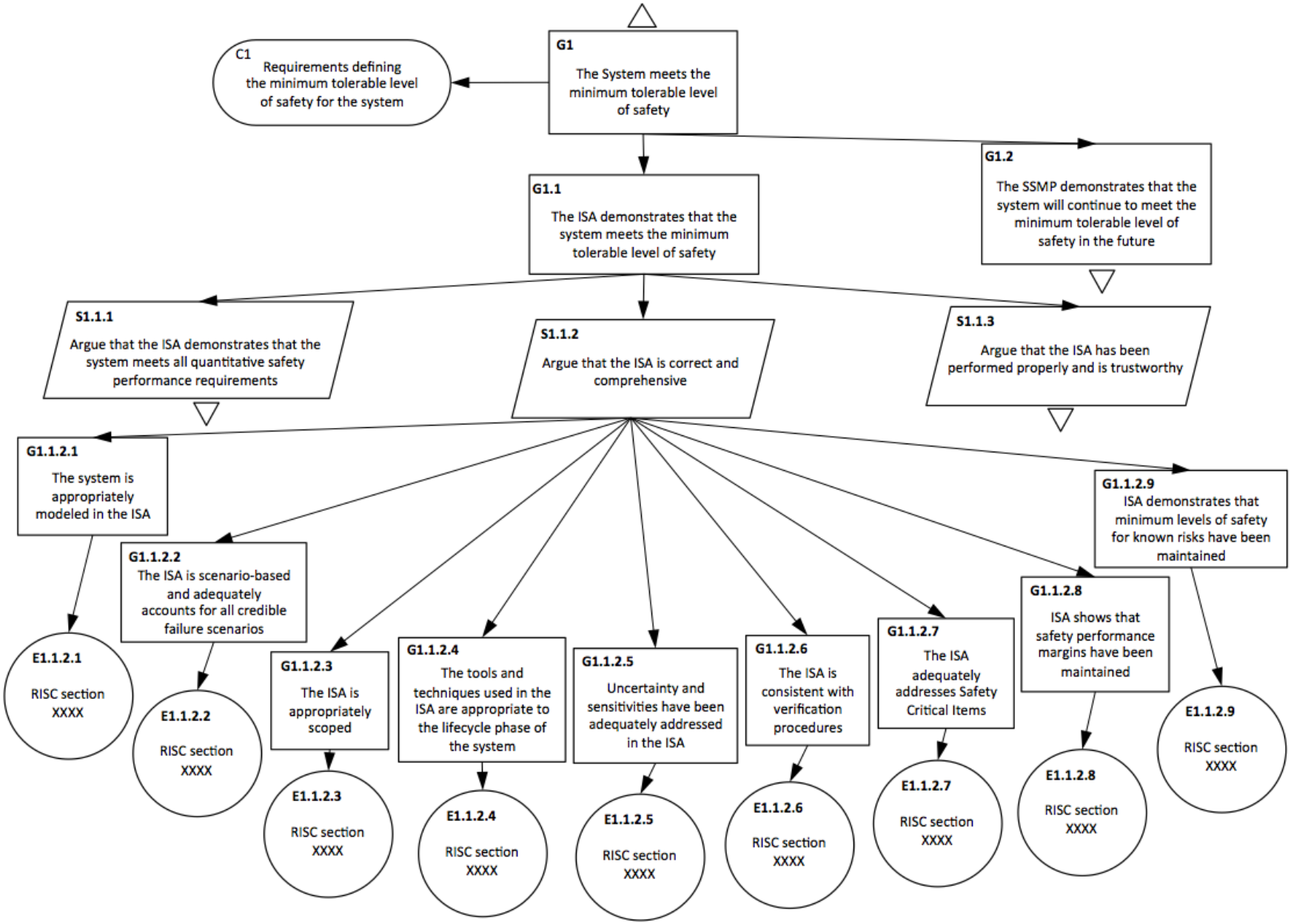
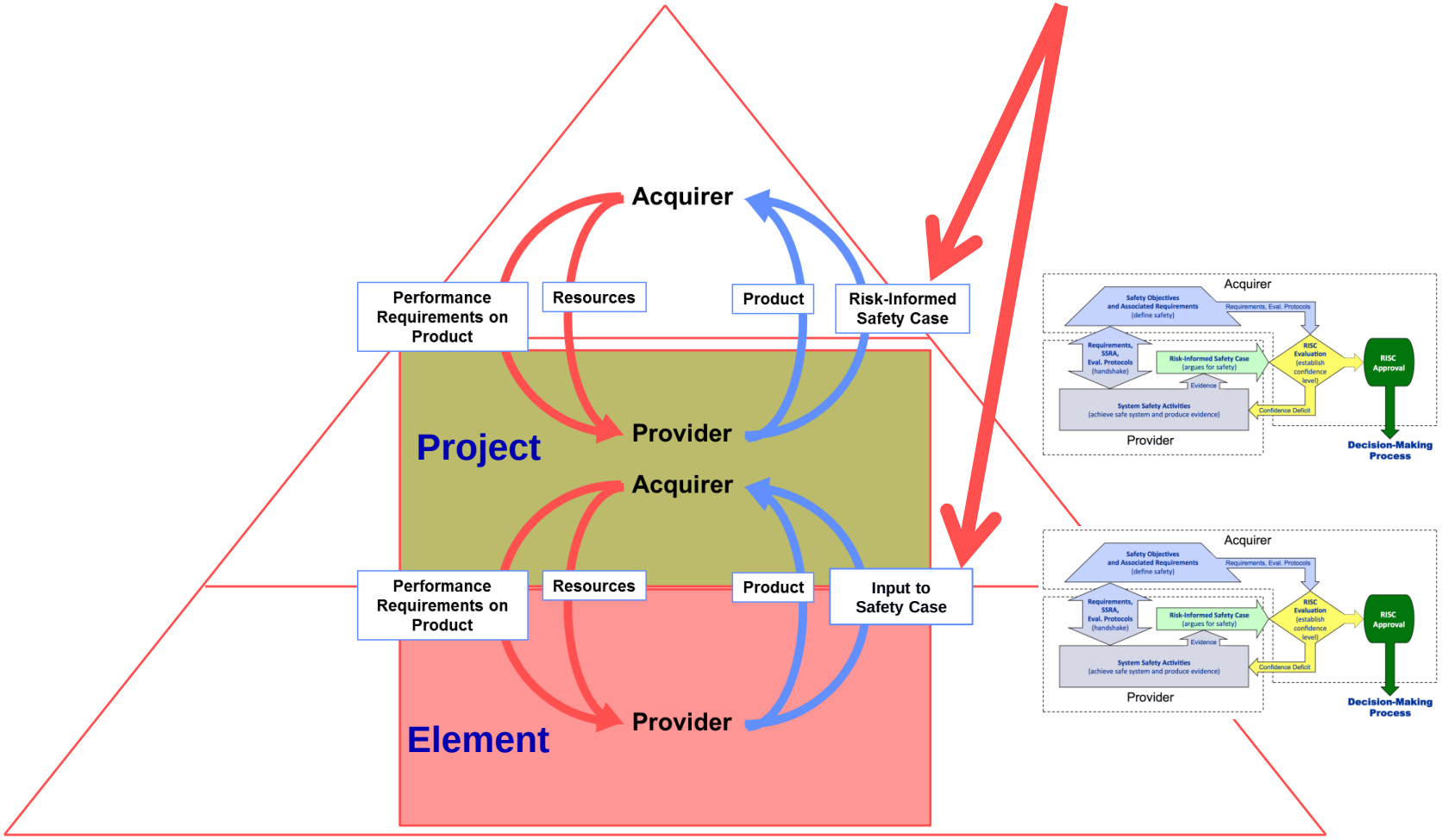


FIGURE 2: The System meets the minimum tolerable level of safety

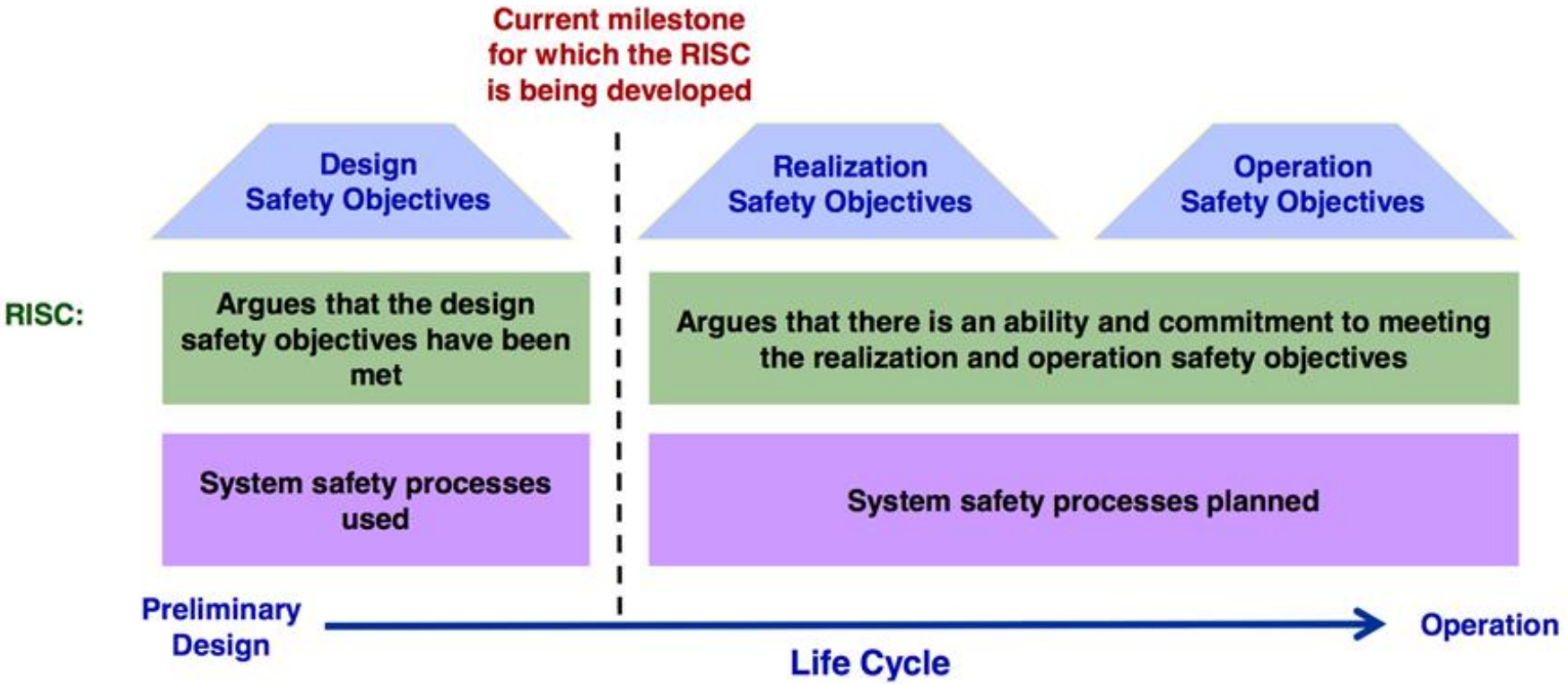

G0
The System is Adequately Safe
C0
Definition of adequately safe system
G1
The System meets the minimum tolerable level of safety
G2
The System is As Safe As Reasonably Practicable (ASARP)
G1.1
The ISA demonstrates that the system meets the minimum tolerable level of safety
G1.2
The SSMP demonstrates that the system will continue to meet the minimum tolerable level of safety in the future
G2.1
Best Practices and Lessons Learned have been incorporated into the system
G2.2
The introduction of safety hazards has been minimized
G2.3
Safety has been prioritized during decision making
G2.4
Safety-related decisions have been risk informed
G2.5
New safety-related information is adequately addressed
G2.6
Organization functions effectively and prioritizes safety


C1
Requirements defining the minimum tolerable level of safety for the system
G1
The System meets the minimum tolerable level of safety
G1.1
The ISA demonstrates that the system meets the minimum tolerable level of safety
G1.2
The SSMP demonstrates that the system will continue to meet the minimum tolerable level of safety in the future
S1.1.1
Argue that the ISA demonstrates that the system meets all quantitative safety performance requirements
S1.1.2
Argue that the ISA is correct and comprehensive
S1.1.3
Argue that the ISA has been performed properly and is trustworthy
G1.1.2.1
The system is appropriately modeled in the ISA
G1.1.2.2
The ISA is scenario-based and adequately accounts for all credible failure scenarios
G1.1.2.3
The ISA is appropriately scoped
G1.1.2.4
The tools and techniques used in the ISA are appropriate to the lifecycle phase of the system
G1.1.2.5
Uncertainty and sensitivities have been adequately addressed in the ISA
G1.1.2.6
The ISA is consistent with verification procedures
G1.1.2.7
The ISA adequately addresses Safety Critical Items
G1.1.2.8
ISA shows that safety performance margins have been maintained
G1.1.2.9
ISA demonstrates that minimum levels of safety for known risks have been maintained
E1.1.2.1
RISC section XXXX
E1.1.2.2
RISC section XXXX
E1.1.2.3
RISC section XXXX
E1.1.2.4
RISC section XXXX
E1.1.2.5
RISC section XXXX
E1.1.2.6
RISC section XXXX
E1.1.2.7
RISC section XXXX
E1.1.2.8
RISC section XXXX
E1.1.2.9
RISC section XXXX

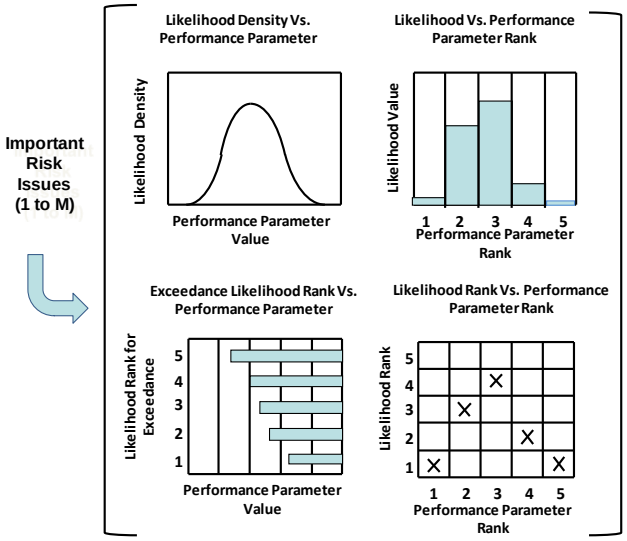
“Acquirers” and “Providers” in the Organizational Hierarchy



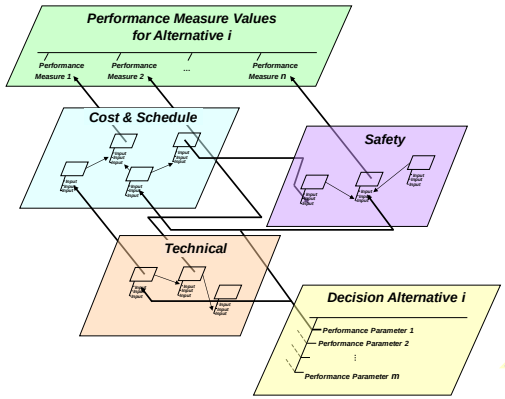
Coverage of the System Life Cycle in the RISC



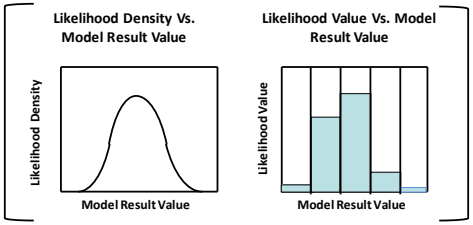
Risk as the Effect of Propagating Uncertainties in the Quantification of Performance Measures

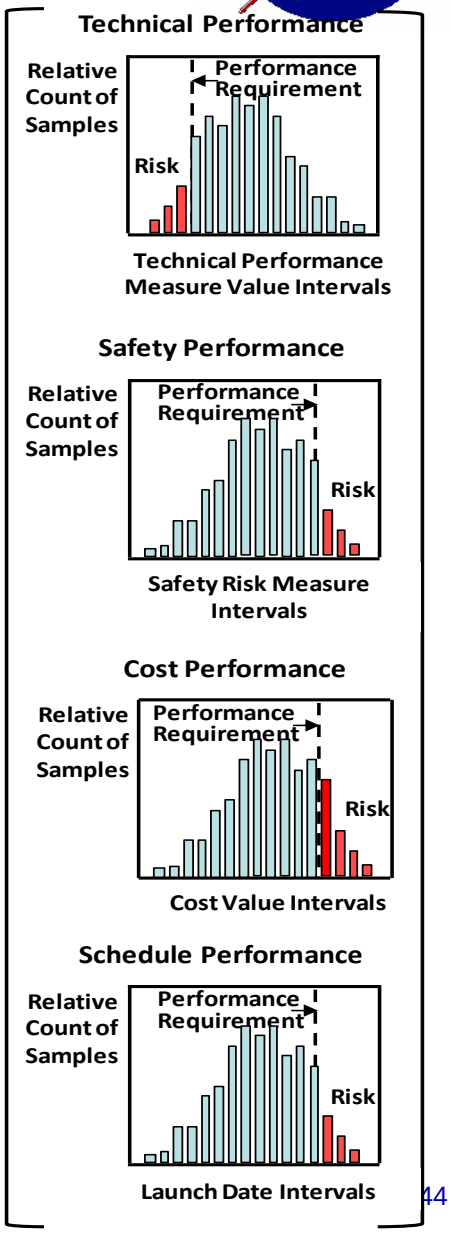


Monte Carlo Sampling



Monte Carlo Sampling

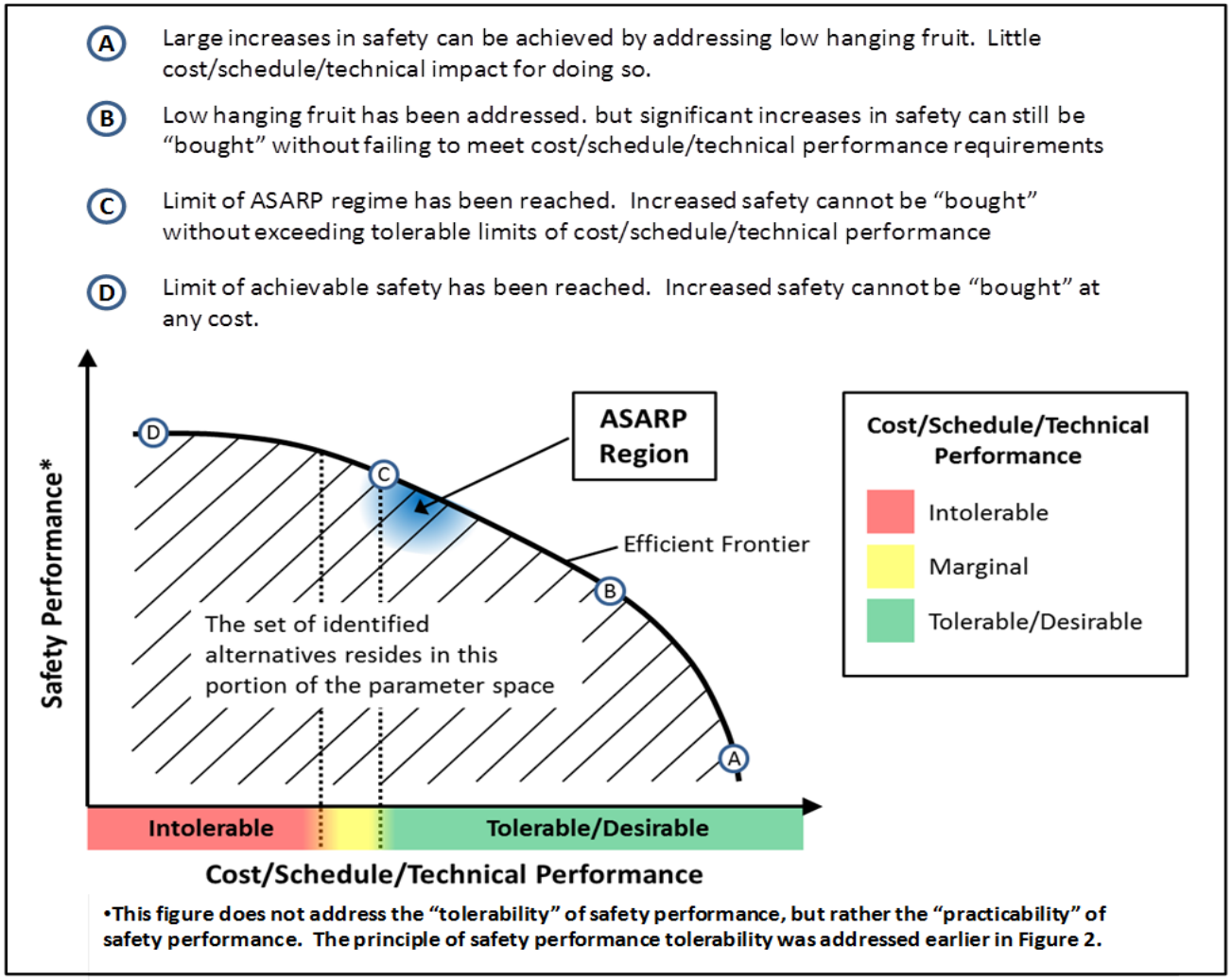




- Uncertainty distributions are obtained for quantities such as input parameters and model results
- Integrated models for technical performance, safety, cost, and schedule are run using a Monte Carlo process to obtain output uncertainty distributions for key PMs
- The output distributions provide the basis for determining the risk of not meeting each performance requirement
- The effect on risk of scenarios that are unknown or underappreciated have to be considered in decision-making, as well, since they are not included in the models (by definition)

Being As Safe As Reasonably Practicable (ASARP)

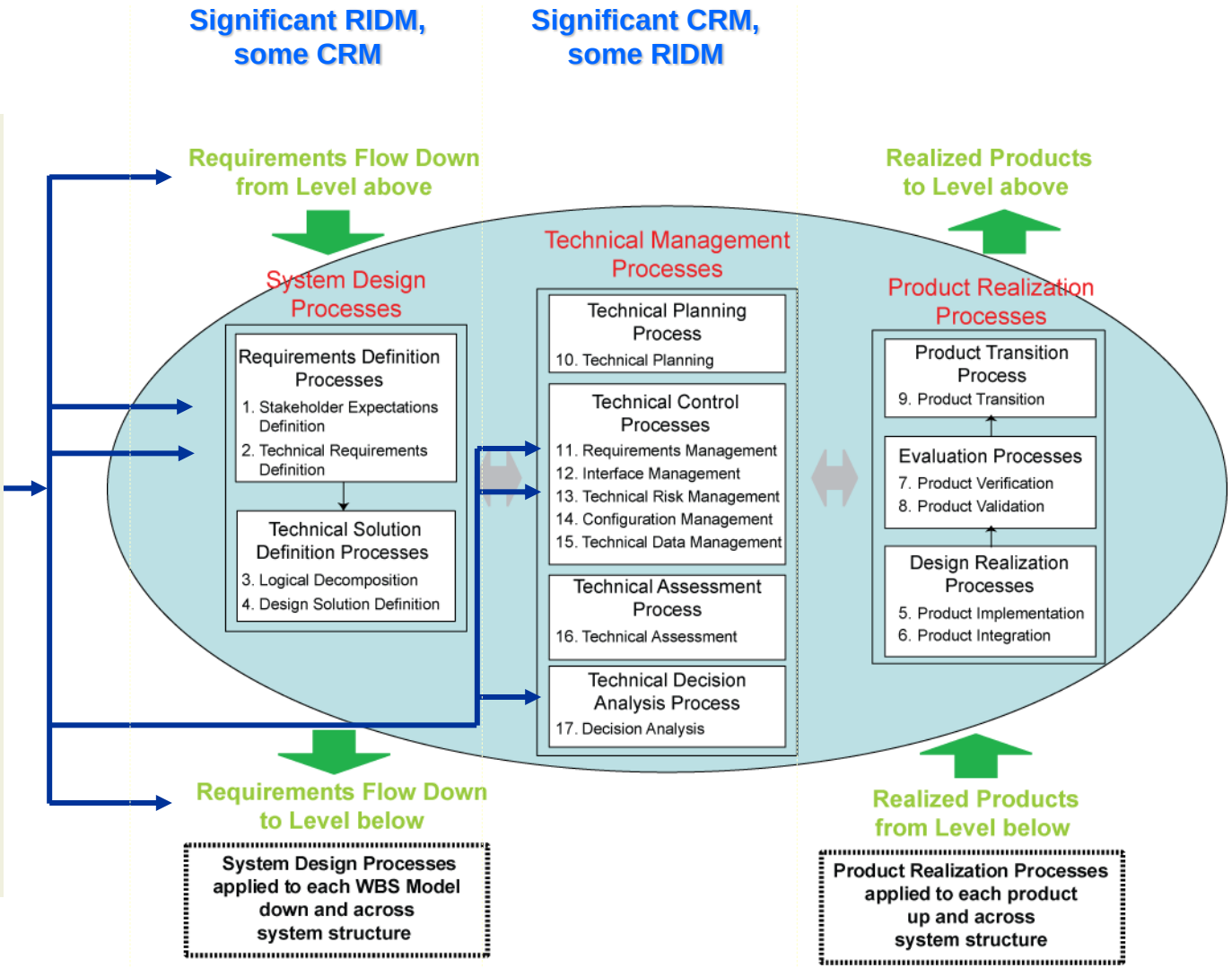
- **ASARP reflects a mindset of continuous safety improvement regardless of the current level of safety**



Issuance of NASA/SP-2007-6105

(Implementation Handbook for NPR 7123)

Modern SMA and risk concepts and techniques were introduced into the SE Handbook. For examples:

- **Model-based safety-related risk metrics (e.g., P(LOC)) are defined as performance measures to support allocation of safety performance and trade-off studies**
- **The process of decision-making (RIDM) was coupled with management of the risks during implementation (CRM)**

Above represents foundational work performed for the development of NPR 8000.4A