Safety and Mission Assurance Overview

University Of Colorado at Bolder

George K. Gafka, 281-483-7732

September 2011

Safety and Mission Assurance (S&MA)
Agenda

- **What is S&MA?**
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- **How does S&MA fit into Programs/Projects?**
- **Program/Project S&MA in the "Real World"**

What is S&MA?

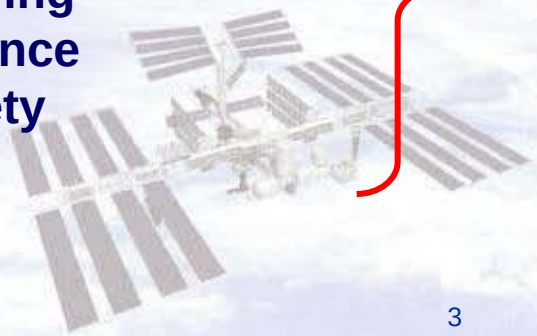
S&MA is… Program/Project Management!
S&MA is… Systems Engineering!
S&MA is… Real Engineering!
S&MA is… a framework of methodologies, analyzes, tools, and processes:

- **For the meaningful organization of complex data and information**
- **For the successful execution of critical tasks**
- **And ultimately for the proactive management of risks and margins to achieve desired results.**

S&MA:
Works when you want it to,
Doesn't work when you don't want it to,
Provides capability in a contingency

S&MA, Six Primary disciplines:

- **System Safety**
- **Reliability and Maintainability**
- **Quality Engineering**
- **Software Assurance**
- **Operational Safety**
- **Aviation Safety**



Safety and Mission Assurance (S&MA)
Agenda

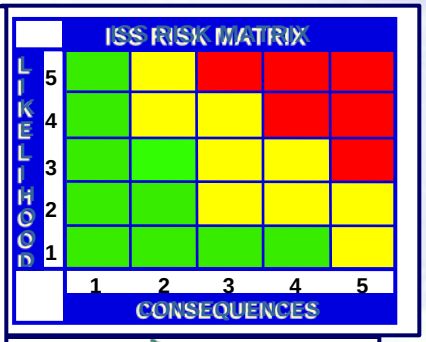
- What is S&MA?
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- How does S&MA fit into Programs/Projects?
- Program/Project S&MA in the “Real World”

What is System Safety?

System Safety engineering specifically addresses the identification, analysis, and control of system risks to humans, the environment, and mission assets.

The System Safety assessment includes numerous forms of high-level analyses performed to support safety decisions such as:

- **Hazard Analysis**
- **Probabilistic Risk Assessment**
- **System Safety Performance Analysis**
- **Phenomenological Analysis**



What is System Safety?

SMA Technical Excellence Program
STEP

Basics of System Safety

NASA

COURSE MAP

Key Concepts and Analysis Techniques > Risk Reduction Protocol

Risk Reduction Protocol

Follow NPR 8715.3 to eliminate the danger, reduce the probability of it happening, or reduce the impact.

Project managers shall ensure that hazards and dominant contributors to risk are controlled according to the following:

a) Eliminate accident scenarios (*e.g., eliminate hazards or initiating events by design*).

b) Reduce the likelihood of accident scenarios through design and operational changes (*hazard control*).

c) Reduce the severity of accident consequences (*hazard mitigation*).

d) Improve the state-of-knowledge regarding key uncertainties that drive the risk associated with a hazard (*uncertainty reduction to support implementation of the above strategies*).

Glossary Help PAUSE || « BACK NEXT » 2 of 9 REPLAY CC Exit

Safety and Mission Assurance (S&MA)
Agenda

- What is S&MA?
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- How does S&MA fit into Programs/Projects?
- Program/Project S&MA in the “Real World”

What is Reliability and Maintainability?

Through design evaluation, probabilistic modeling and analysis, and testing, the Reliability and Maintainability disciplines help establish the necessary confidence that the system and its components will function as required.

This discipline is split into two parts:

1. **Reliability Engineering: assessment and improvement of reliability performance of systems during their missions.**

Reliability: The system performs as intended when needed

2. **Maintainability Engineering: assessments and verification of the system design characteristics so that downtime and the need for maintenance are minimized.**

Maintainability: How fast, easy, and safe it is to repair the system when necessary

What is Reliability and Maintainability?

AVAILABILITY

When you want to use your car, is it available for your use?

RELIABILITY

How often does your car fail to start? How often do you have trouble with your car?

MAINTAINABILITY

How often does your car need repair? Can maintenance be done quickly and easily?

R&M performance metrics are based on future events; Never 100% accurate

R&M relies on past experiences, for example past mission performance or test data

R&M assesses ways in which the system fails, and methods by which it is restored

What is Reliability and Maintainability?

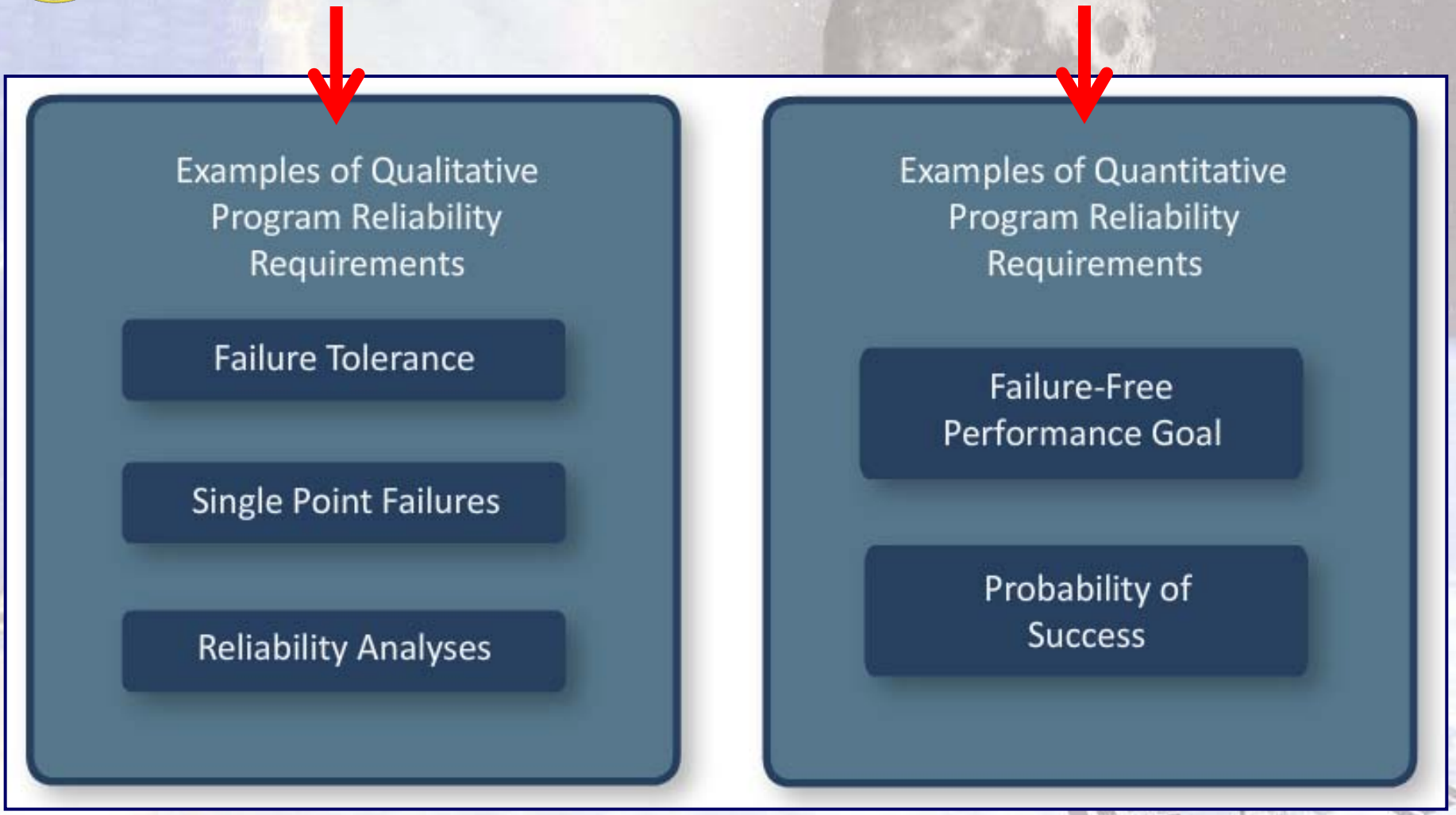
Design Engineer: Success Space

How will the system work?
What function will it perform?
What are the requirements?

Reliability Engineer: Failure Space/ Worst Case Failure Mode

How can the system fail?
How can the operating environment cause problems?
Is redundancy required?
Are there operational work-arounds?

What is Reliability and Maintainability?



What is Reliability and Maintainability?

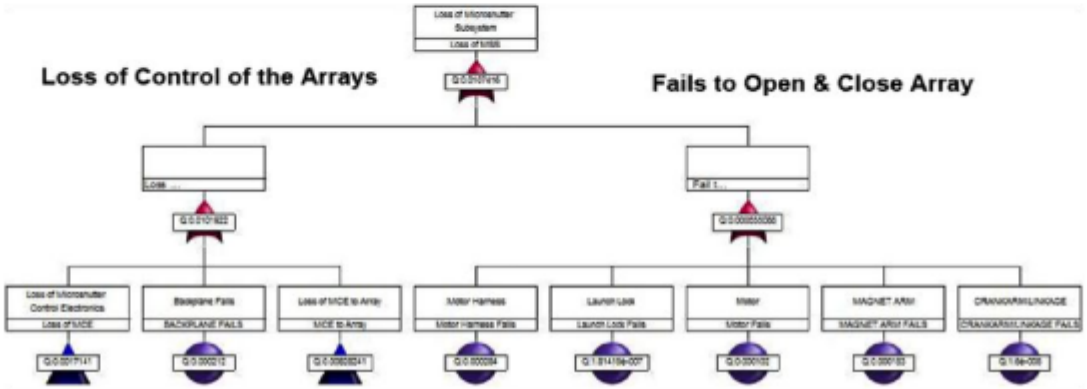
R&M Tools and Methodology

FMEA is a bottom-up analysis of failure modes whereas Fault tree logically decomposes system failures into contributing anomalous events and conditions. Example taken from James Webb Space Telescope (JWST).

FMEA Example

FAILURE MODE #	IDENTIFICATION OF ITEM/FUNCTION	FAILURE MODES	FAILURE EFFECTS			FAILURE DETECTION	MITIGATING PROVISIONS	SEV	Date Revised: 11/17/08
			ICE	MIRI					REMARKS
Harness 1.1	ICE Harness (WMC401)	short on ICE Side A	Loss of ICE A	None	None	Detect by ICE Over current Detection Circuit	ICE switch from side A to Side B	2R	Each line is electrically isolated; therefore, short can't be propagated.
Harness 1.2	ICE Harness (WMC401)	Open on ICE Side A	Loss of ICE A	None	None	Telemetry	ICE switch from side A to Side B	2R	

FTA Example



Safety and Mission Assurance (S&MA)
Agenda

- **What is S&MA?**
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- **How does S&MA fit into Programs/Projects?**
- **Program/Project S&MA in the "Real World"**

What is Quality Engineering?

Quality {qual·i·ty:} "the degree to which a set of inherent characteristics fulfills requirements."

Quality Engineering includes the design, compliance, and fitness for use of its products and services. As part of the overall Quality Assurance effort, it serves to provide confidence that product configurations meet safety and technical requirements. Quality Engineering forms an essential part of the overall plan to achieving safe and successful missions consistently and continuously.

Achieving Quality Engineering requires:

- **Establishing needs and expectations**
- **Developing an effective quality management process**
- **Establishing engineering and manufacturing practices that emphasize robust design, the state where the technology, product, or process performance is minimally sensitive to factors causing variability**
- **Identifying critical processes, processes that, if performed incorrectly or in violation of prescribed requirements, could result in loss of life, serious personal injury, loss of mission, or loss of a significant mission resource**
- **Identifying key characteristics, the features of a material, process, or part whose variation has a significant influence on product fit, performance, service life, or manufacturability**
- **Verifying that the product, as built, meets the design**
- **Developing process maturity through continuous process improvement efforts**

Example: Tile Repair, "Bubbles in the Goo"

What is Quality Engineering?

STEP — Basics of Quality Engineering

QE Overview > Why continuously strive for better quality?

If the shuttle has approximately 24,300 tiles adhered to its exterior surfaces. A tile installation process at:

- 99.38% (Four Sigma Level): approximately 150 tiles not being glued on properly.
- 99.99966% (Six Sigma Level): approximately 0.08 tiles not being glued on properly.

Good Enough?

Safety and Mission Assurance (S&MA)
Agenda

- What is S&MA?
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- How does S&MA fit into Programs/Projects?
- Program/Project S&MA in the “Real World”

What is Software Assurance?

The Software Assurance discipline operates under the scrutiny of a planned and systematic set of activities that ensure that the software and its related products:

- Conform to software life cycle processes
- Meet their specified requirements and standards
- Are consistent, complete, correct, and safe
- Are secure and reliable as warranted for the system and operating environment
- Satisfy customer needs
- Are implemented according to plan

In order to achieve these goals, the Software Assurance discipline consists of five distinct roles:

- Software Quality: assurance that quality is built into the software
- Software Safety: an approach to identifying, analyzing, and controlling software hazards
- Software Reliability: an approach to incorporating and measuring reliability throughout the product lifecycle by building in software error prevention, fault detection, isolation, recovery, and/or reduced functionality states
- Software Verification & Validation (V&V): activities which ensure that software satisfies functional requirements and that each phase of the development process yields acceptable products
- Independent Verification & Validation (V&V): additional V&V activities performed by an independent organization

Software has become an increasingly more significant, more complex, and more critical part of integrated space systems… and therefore software assurance has also grown significantly!

Safety and Mission Assurance (S&MA)
Agenda

- **What is S&MA?**
  - **System Safety**
  - **Reliability and Maintainability**
  - **Quality Engineering**
  - **Software Assurance**
  - **Operational Safety**
  - **Aviation Safety**
- **How does S&MA fit into Programs/Projects?**
- **Program/Project S&MA in the "Real World"**

What is Operational Safety?

Managing risks and preventing operational accidents is imperative for SMA's Operational Safety workforce. This NASA SMA function focuses on the prevention of operations-related safety hazards by:

- **Assuring mission success**
- **Protecting the public and flight, ground, laboratory, and underwater personnel**
- **Protecting the environment**
- **Protecting the aircraft, spacecraft, and payloads**
- **Protecting the facilities, property, and equipment**

The governing policy directive for this discipline is the NASA General Safety Program Requirements (NPD 8715.3) Chapter 3 which specifically focuses on the following key aspects: Motor Vehicle Safety; Personal Protective Equipment; Control of Hazardous Energy (Lockout/Tagout Program); Pressure System Safety; Electrical Safety; Hazardous Material Transportation, Storage, and Use; Hazardous Operations; Laboratory Hazards; Lifting Safety; Explosive, Propellant, and Pyrotechnic Safety; Underwater Operations Safety; Launch, Entry, and Experimental Aeronautical Vehicle Operations Safety; Test Operations Safety; Non-Ionizing Radiation; Ionizing Radiation; and, Confined Spaces.

Additionally, there are many Federal, State, and Local laws that also apply to Operational Safety at NASA.

Safety and Mission Assurance (S&MA)
Agenda

- **What is S&MA?**
  - **System Safety**
  - **Reliability and Maintainability**
  - **Quality Engineering**
  - **Software Assurance**
  - **Operational Safety**
  - **Aviation Safety**
- **How does S&MA fit into Programs/Projects?**
- **Program/Project S&MA in the "Real World"**

What is Aviation Safety?

…assure mission success and preserve human and material resources

Readiness Reviews

Airworthiness, flight safety, and mission readiness reviews are conducted for all aircraft modifications.

These reviews are to clear unique or nonstandard internal or external payloads or stores configurations for flight and to review nonstandard flight operations.

These reviews identify hazards so as to minimize risks to persons and property and to enhance the likelihood of mission and program success.

Formal review requirements are tailored according to the type of modification incorporated specific to the mission and the operational risks involved.

- **Indentify, Analyze, Eliminate, and Report Hazards**
- **Risk Assessment / Risk Management**
- **Fault Tree Analysis**
- **FMEA/CIL & FMECA**

Examples of Changes Requiring an Airworthiness Review

- Structural and material changes that alter the basic aircraft design
- Modifications of the exterior contour or mold line of the aircraft
- Modification to the flight control system, including software revisions
- New or modified propulsion system or its control system
- Modifications of any subsystem interfacing with and affecting flight or propulsion systems
- Modification of the aircrew life support systems
- Flight test instrumentation that interfaces with normal aircraft systems
- Intentional operation in a degraded mode for test purposes
- Dropping of uncertified stores or objects
- Any other modifications, payloads, or operations that are nonstandard according to established flight manuals

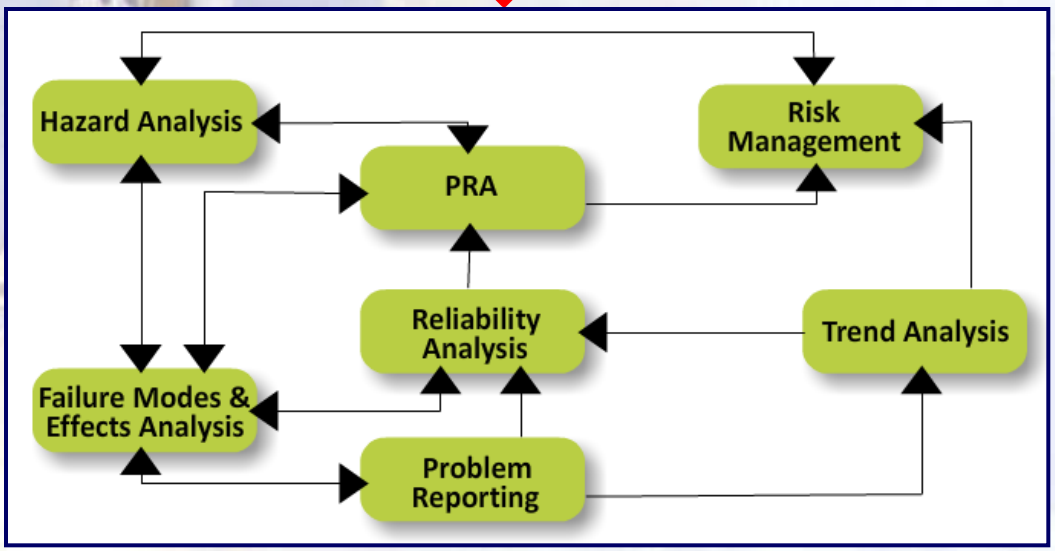
Safety and Mission Assurance (S&MA)
Agenda

- **What is S&MA?**
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- **How does S&MA fit into Programs/Projects?**
- **Program/Project S&MA in the "Real World"**

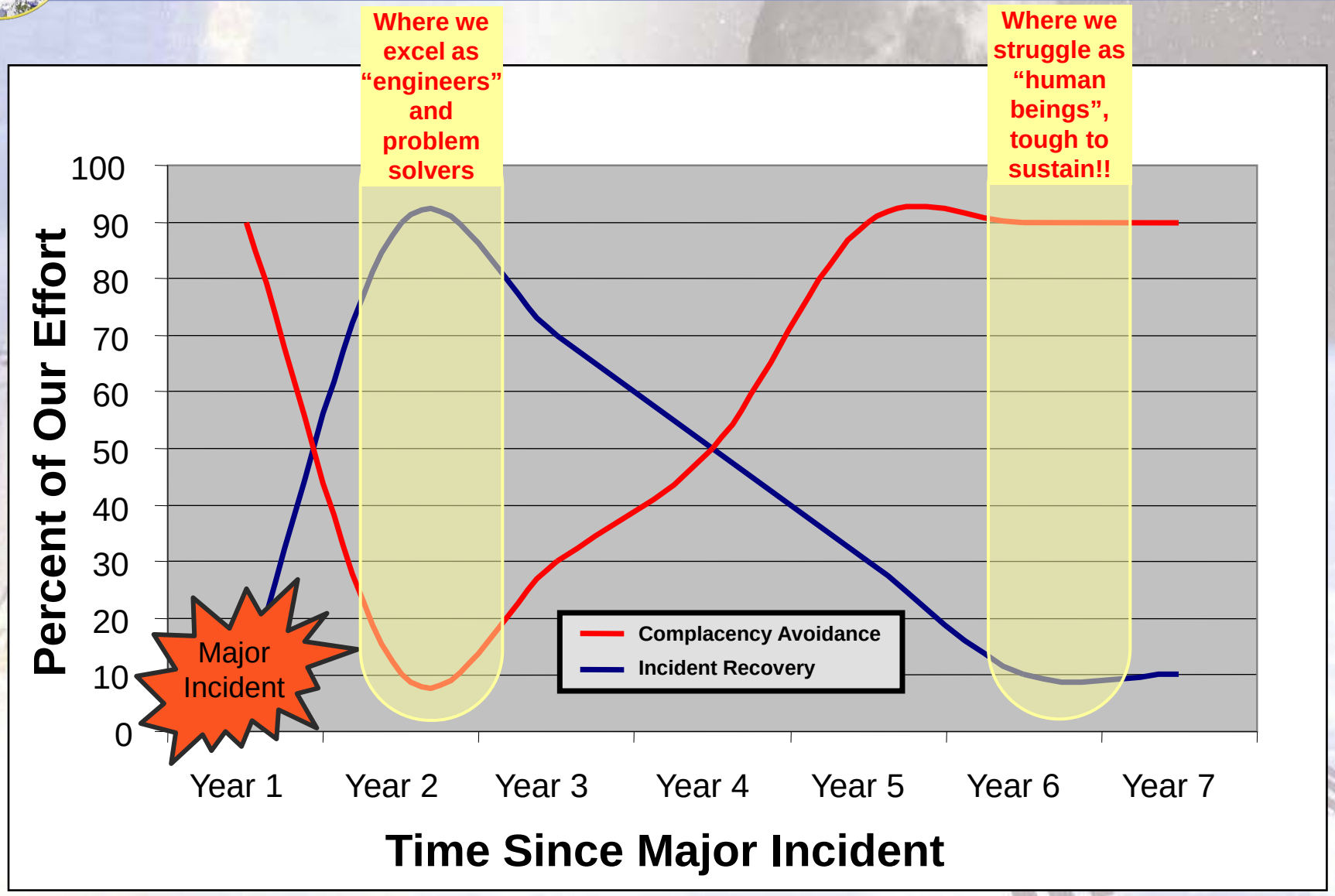
What is S&MA?
An Integrated Discipline!

Six primary S&MA disciplines:

- System Safety
- Reliability and Maintainability
- Quality Engineering
- Software Assurance
- Operational Safety
- Aviation Safety



What is S&MA?
The "Psychology" Side of S&MA



What is S&MA?
The "Softer/People" Side of S&MA

Bryan O'Connor
Agency Chief, S&MA

Bryan O'Connor's Characteristics of a Great S&MA Professional:

- Technically Credible
- Imbued with "Engineering Curiosity"
- Courageous ("truth to power")
- High Integrity
- Solid Knowledge of Requirements and Rationale
- Good Communication Skills (Verbal & Written)
- Experience in Applicable Field
- Humble Yet Engaged
- Persistent Yet Pragmatic
- Energetic and Creative (Yes, if….)
- Thick Skin and Sense of Humor (for Longevity)

"We're just flat not as smart as we think we are"

Tommy Holloway
Space Shuttle Program Manager

Safety and Mission Assurance (S&MA)
Agenda

- **What is S&MA?**
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- **How does S&MA fit into Programs/Projects?**
- **Program/Project S&MA in the "Real World"**

Birth and Sustainment
Of US “Assurance”?

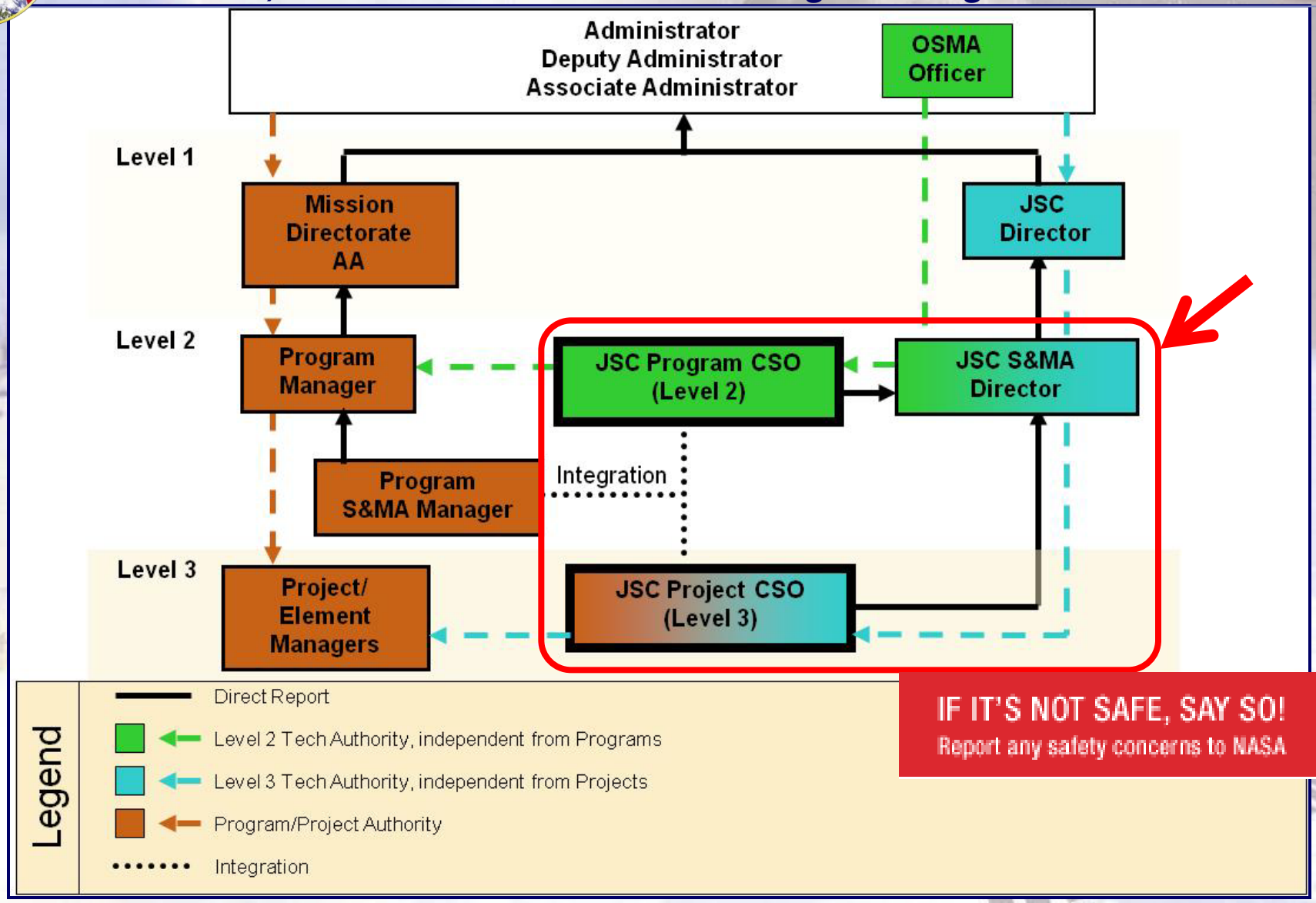
“No man is allowed to be a judge in his own cause, because his interest would certainly bias his judgment, and, not improbably, corrupt his integrity. With equal, nay with greater reason, a body of men are unfit to be both judges and parties at the same time;”

The Federalist No. 10
(a series arguing for the ratification of the United States Constitution)
James Madison
November 23, 1787

“Trust, but verify”

Adopted and made famous by U.S. president Ronald Reagan. Reagan frequently used it when discussing U.S. relations with the Soviet Union. Reagan rightly presented it as a translation of the Russian proverb *"doveryai, no proveryai"* (Russian: Доверяй, но проверяй). Soviet revolutionary Vladmir Lenin also frequently used the phrase. Reagan used the phrase at the signing of the INF Treaty, his counterpart Mikhail Gorbachev responded: "You repeat that at every meeting," to which Reagan answered "I like it.“

Program/Project S&MA Interfaces
Organizations and People, "Governance"
NPD 1000.0, NASA Governance and Strategic Management Handbook

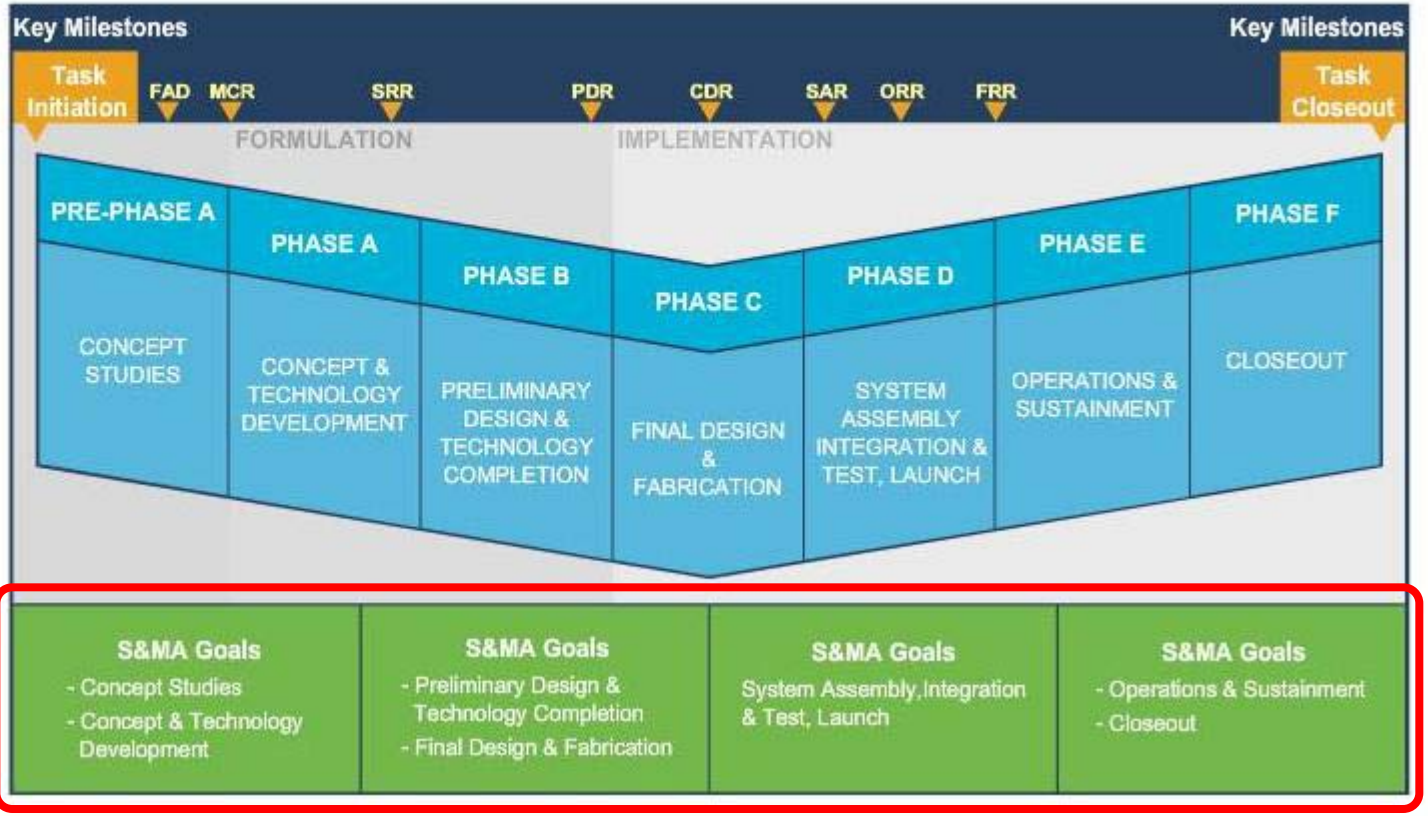


S&MA Throughout the Program Lifecycle Modeled after NPR7120.5

NPR 7120.5, NASA Space Flight Program and Project Management Requirements

NASA Life Cycle Highlighting System Safety Products and Services

A general overview of the activities, processes, and products associated with System Safety engineering within the NASA Project Life Cycle



Program/Project S&MA Interfaces
S&MA Content Example: NPR8705.2b
NPR 8705.2B Human-Rating Requirements for Space Systems

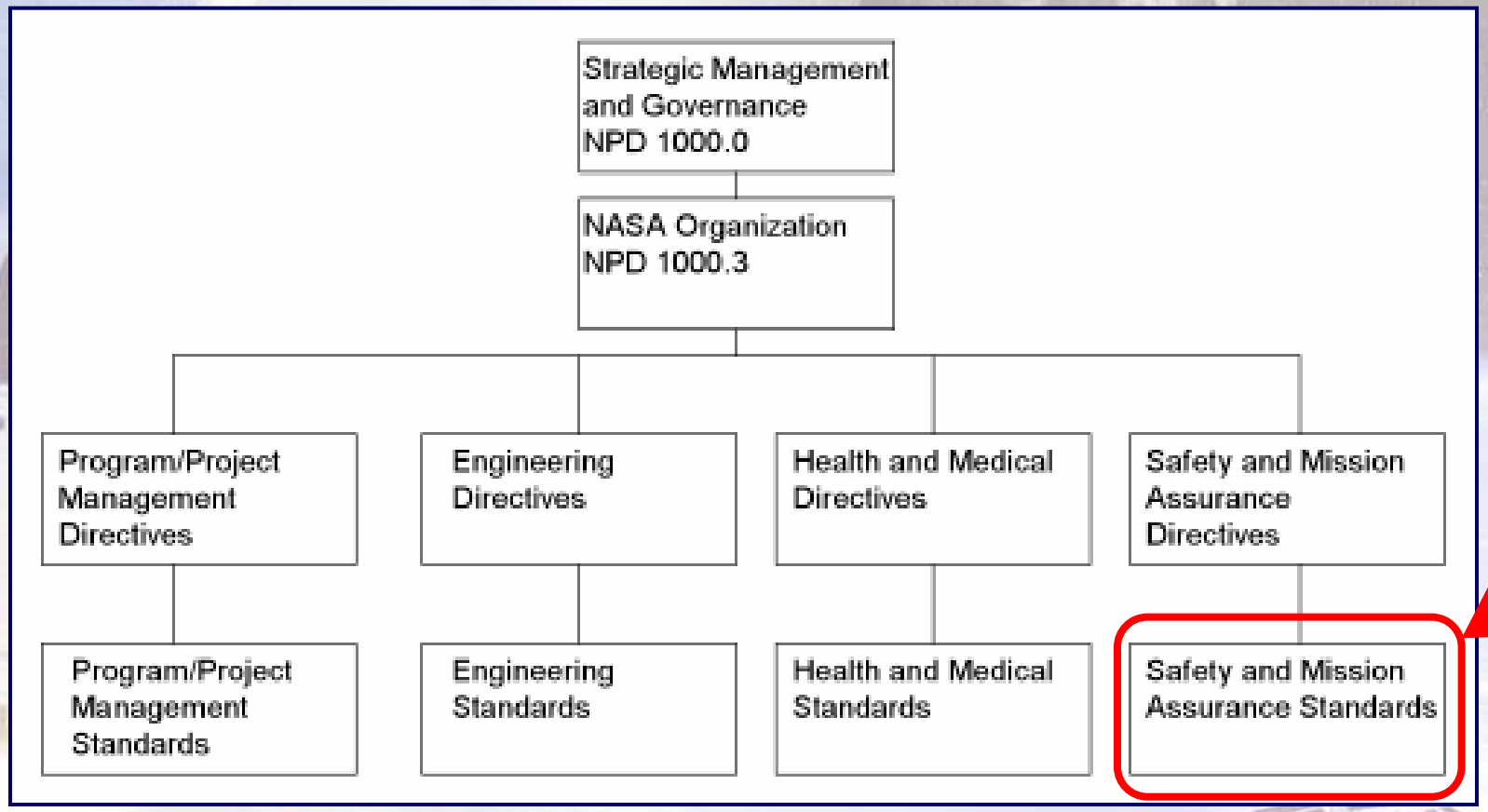


Figure 1 - Agency Requirements Framework Related to Human-Rating

Program/Project S&MA Interfaces
S&MA Content Example: NPR8705.2b
NPR 8705.2B Human-Rating Requirements for Space Systems

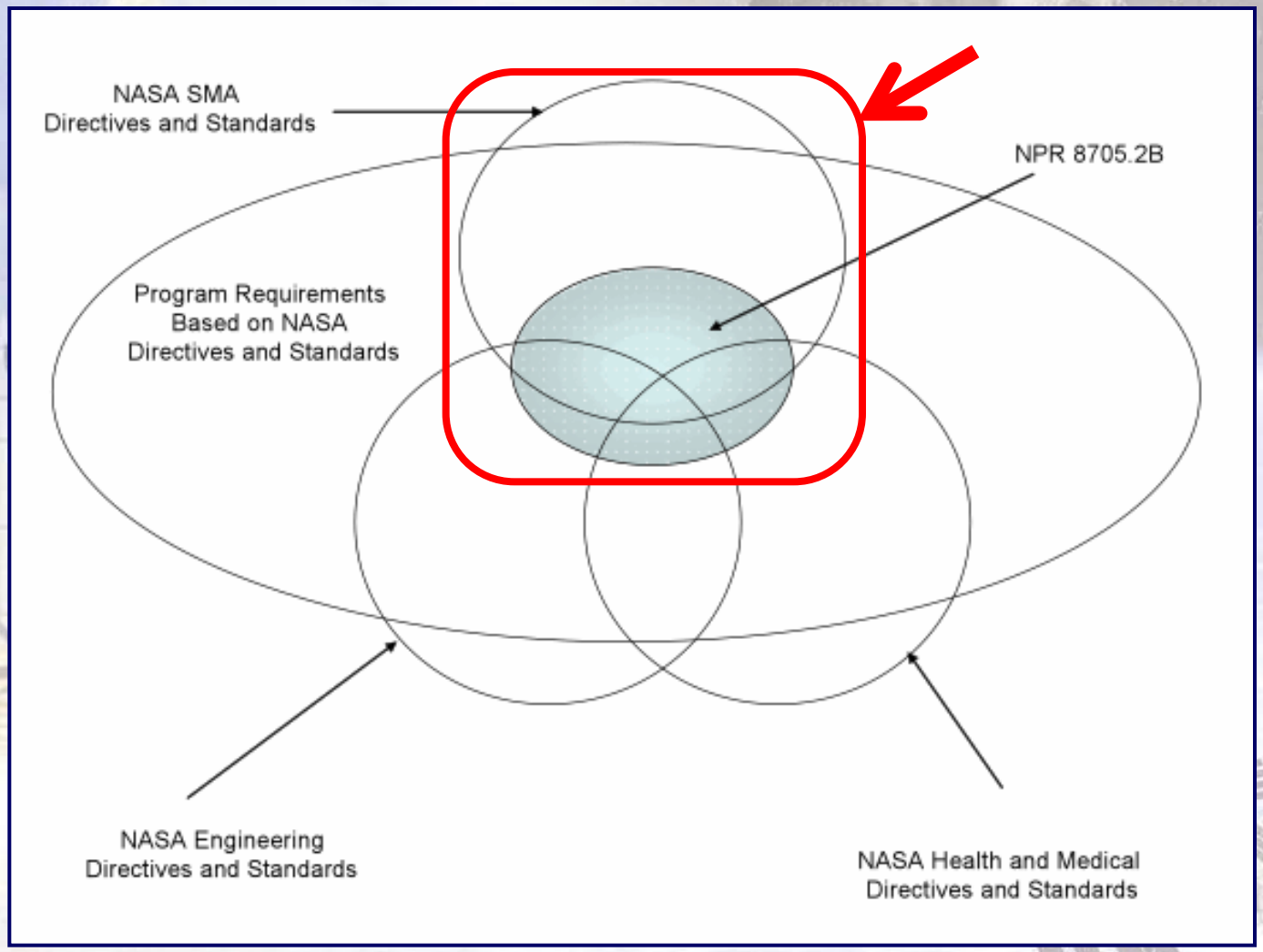
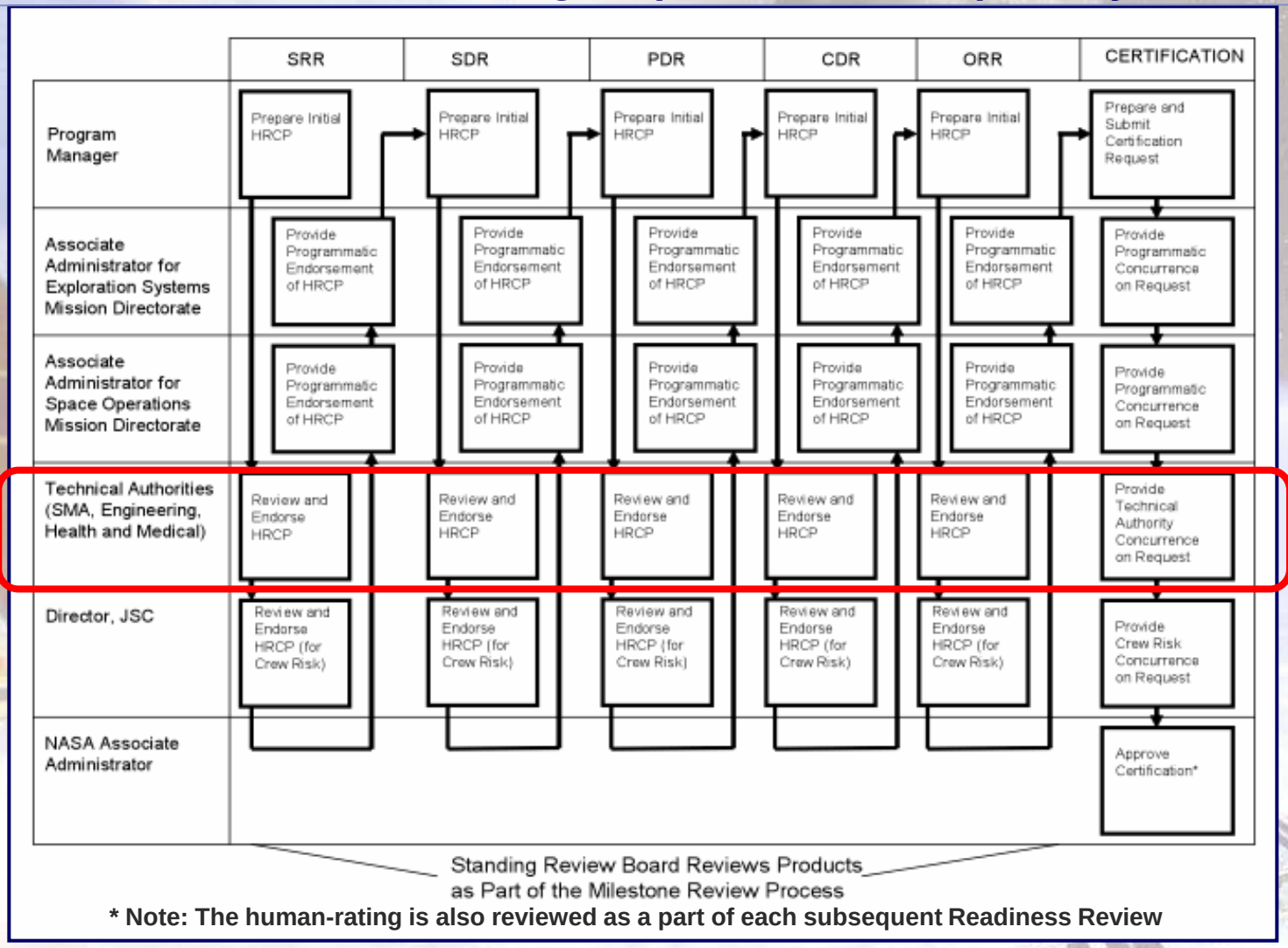


Figure 2 - Relationship Among Requirements

Program/Project S&MA Interfaces
S&MA Content Example: NPR8705.2b
NPR 8705.2B Human-Rating Requirements for Space Systems



*** Note: The human-rating is also reviewed as a part of each subsequent Readiness Review**

Figure 3 - Human-Rating Certification Process Flow

Interesting Relative Risks
Example: Agency Loss Of Crew (LOC)

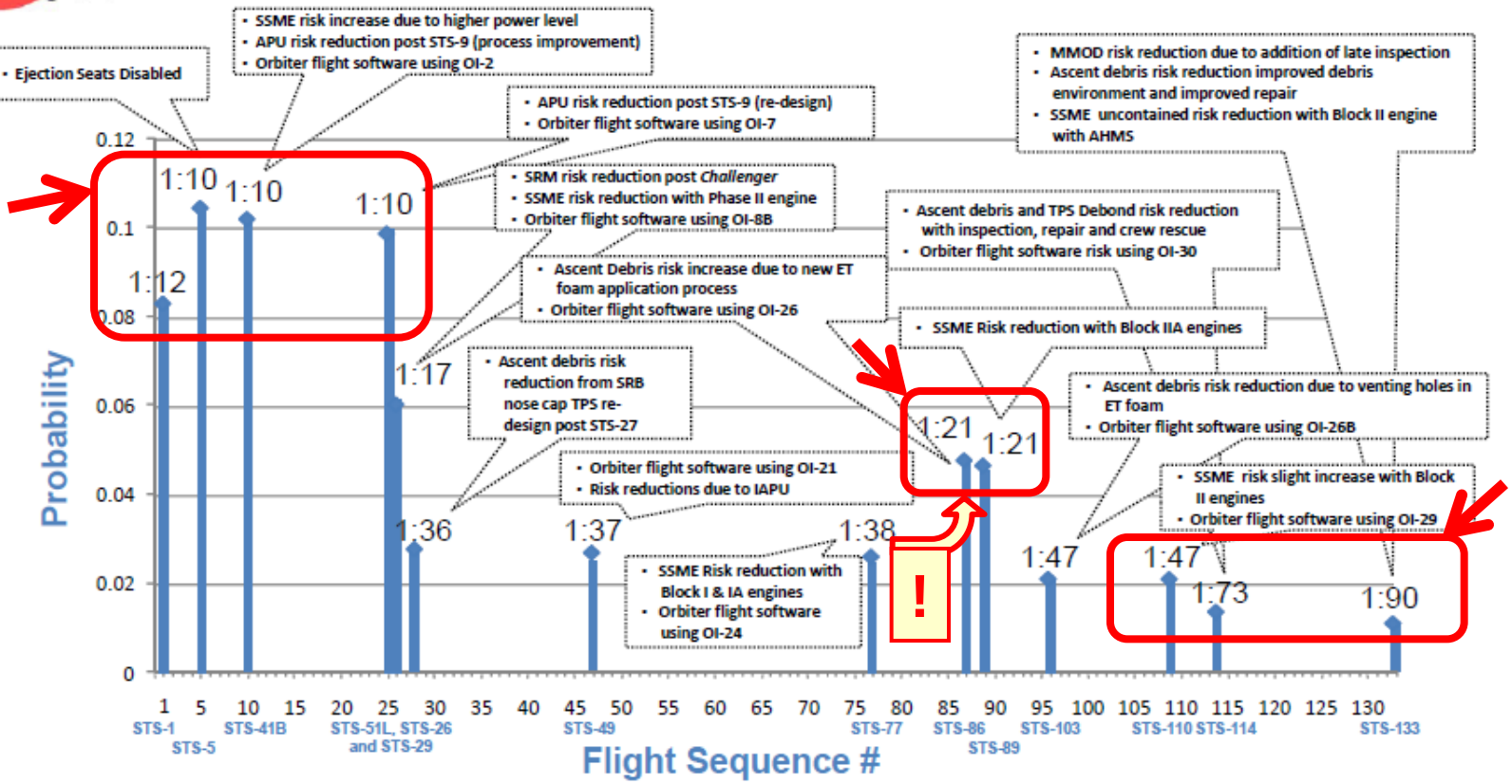
U.S. combatants in the battle of Iwo Jima 1945	1/10*
Doolittle raid1942, and Pickett's charge 1864	1/11*
U.S. combatants on D-Day	1/29*
New York City firefighter on 9/11	1/34*
B-17 single mission over Germany 1943	1/37**
Mt Everest climb (1922 – 2006)	1/49*
Soyuz missions (manned flight statistics 1967 – present)	1/52**
Space Shuttle mission (statistics 1981-present)	1/66**
Space shuttle mission to/fm ISS (2010 PRA)	1/89**
Cx and CCT agency threshold (single ISS mission)	1/150**
X-15 research flight	1/199**
Cx and CCT design requirement (single ISS mission)	1/270**
Alaskan crab fisherman (one year)	1/281*
U.S. crop duster pilot (one year)	1/510**
Cx and CCT recommended goal (single ISS mission)	1/750**
U.S. logging, timber cutting (one year)	1/775*
U.S. construction worker (one year)	1/2440*
U.S. coal miner (one year)	1/3450*

* deaths/total participants
** fatal mishaps/total missions

Safety Enhancements Throughout Lifecycle
Example: Shuttle Program, fixes & improvements

SPACE SHUTTLE PROGRAM
Space Shuttle Safety and Mission Assurance Office
NASA Johnson Space Center, Houston, Texas

RESULTS SUMMARY



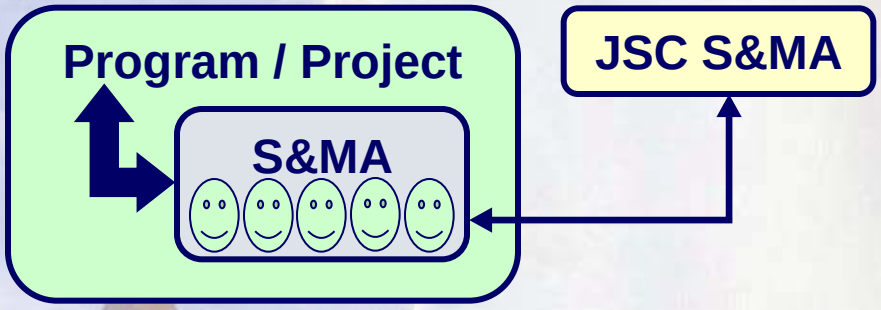
- There was an 8% likelihood of making it to flight 25 without LOCV and a 8% likelihood of making it from flight 26 to flight 113 without LOCV using the values on this chart
  - We were lucky, there were a number of close calls (e.g. STS-9 APU fire, STS-27 Ascent Debris, STS-95 drag chute door)

Safety and Mission Assurance (S&MA)
Agenda

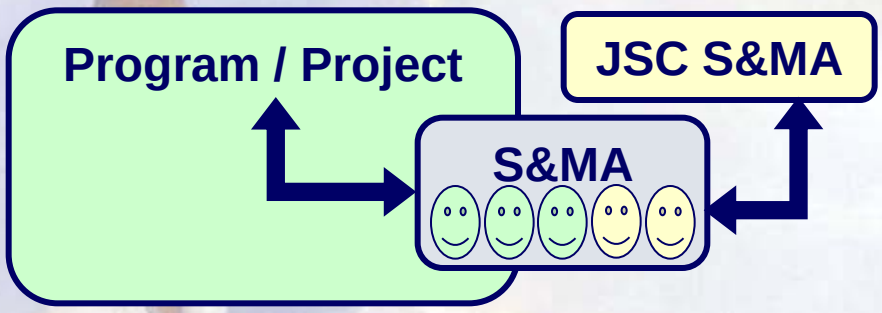
- **What is S&MA?**
  - System Safety
  - Reliability and Maintainability
  - Quality Engineering
  - Software Assurance
  - Operational Safety
  - Aviation Safety
- **How does S&MA fit into Programs/Projects?**
- **Program/Project S&MA in the "Real World"**

S&MA as a Function of Organization

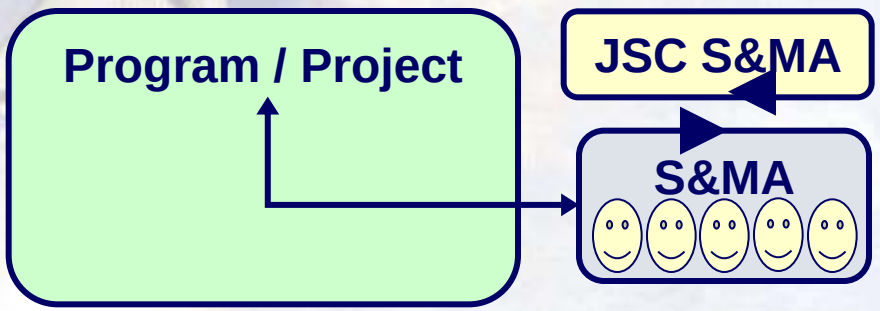
Program/Project S&MA Relationship ("tightly coupled")



- Not Independent
- Conscious of Program/Project?
- Value "as directed"
- Healthy tension? Checks & balances?



- Independent, yet engaged/informed
- Relevant conscious of Program/Project
- Value needed and proactive value added
- Healthy tension and checks & balances



- Independent, but informed?
- Conscious of Program/Project, relevant?
- Value needed? Value added?
- Checks & balances, but the right areas?

3 Jobs of S&MA: Doing… Checking… Technical Authority

S&MA as a Function of Engagement Timing
Engagement Example: NPR7123.1

NPR 7123.1, NASA Systems Engineering Processes and Requirements

S&MA Breadth of Initial/Significant Engagement

- Tailoring reqs and processes
- Informing risk trades
- Proper scoping

- Compliance to what's on the books
- Auditing "water under the bridge"
- Reactionary resourcing

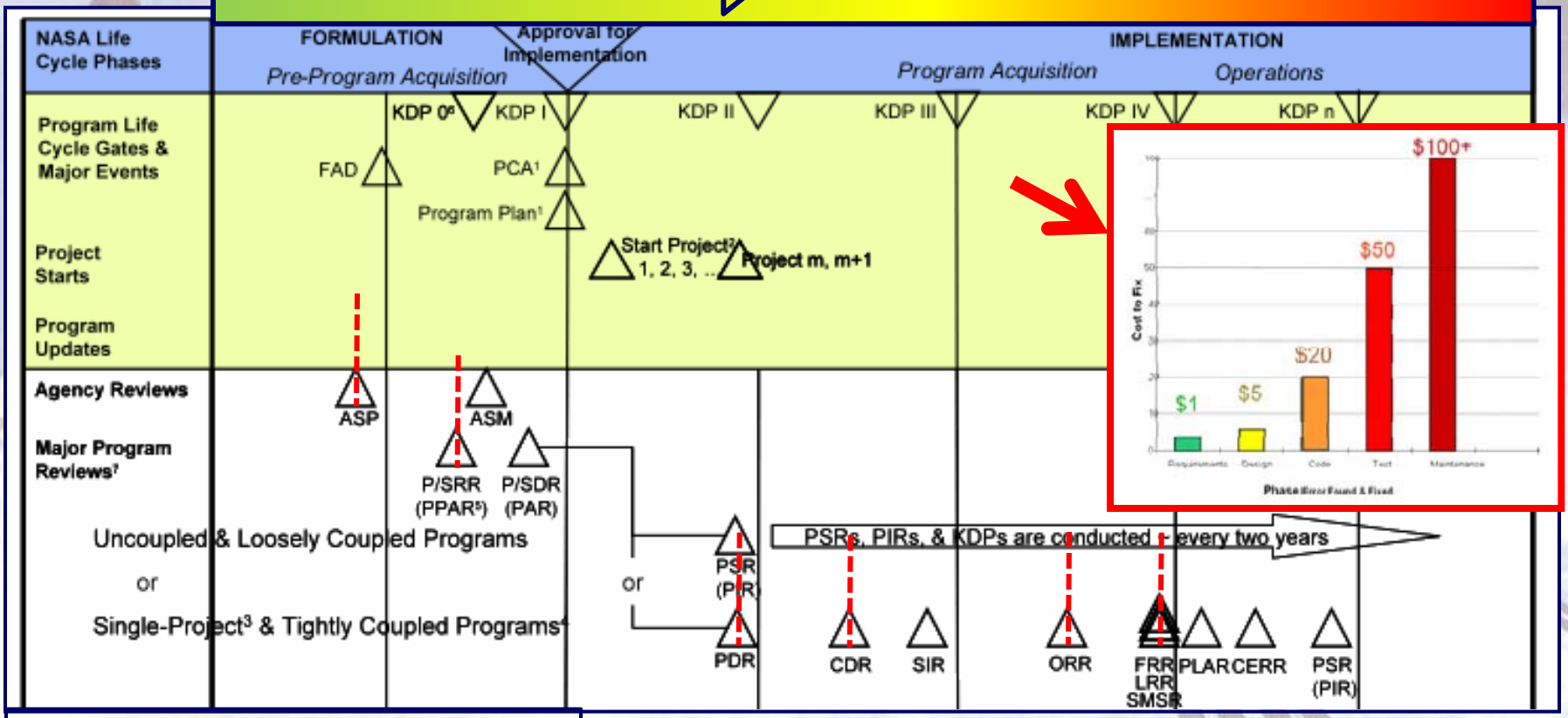
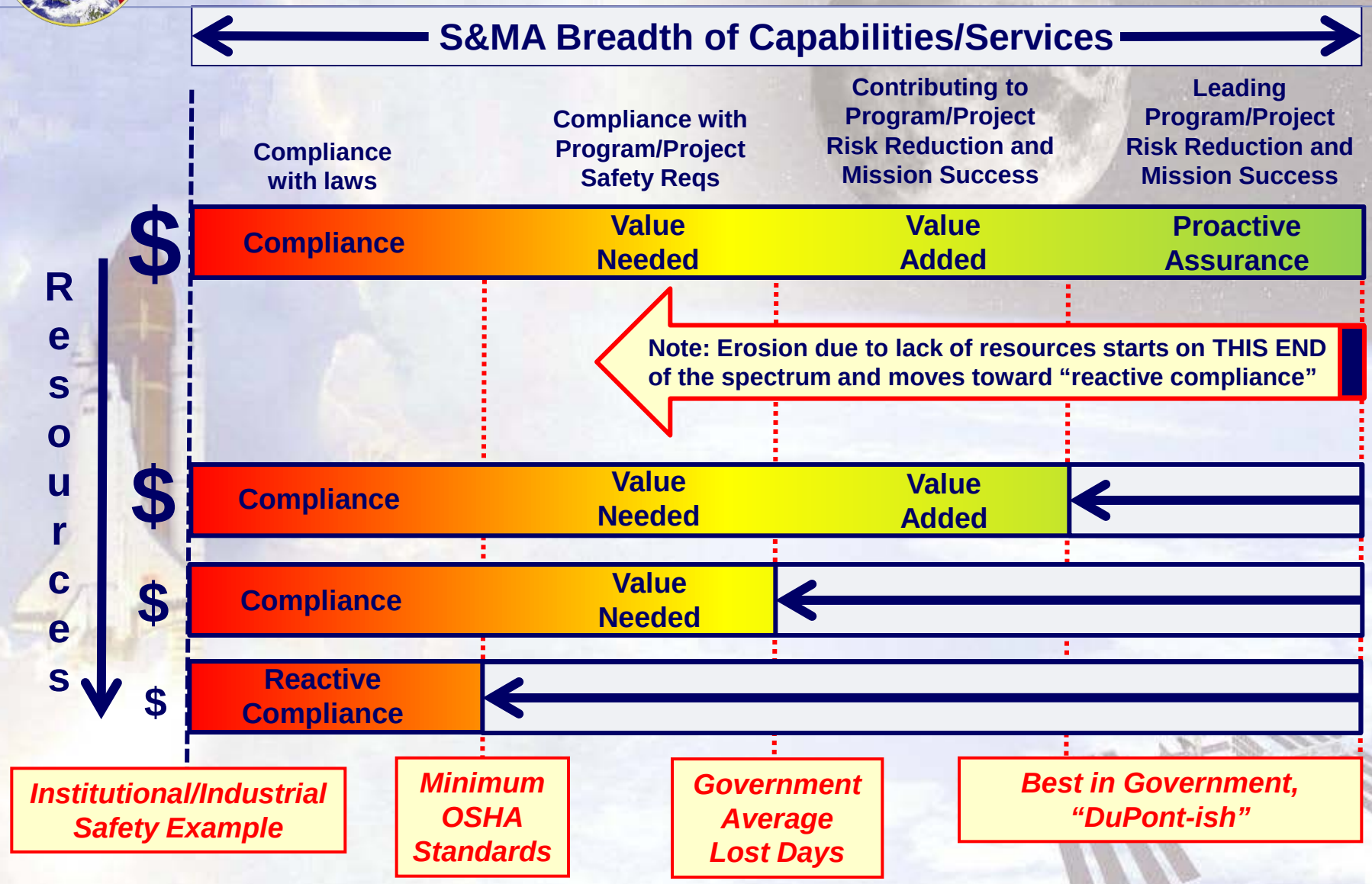


Figure 5.1 The NASA Program Life Cycle

S&MA as a Function of Resources



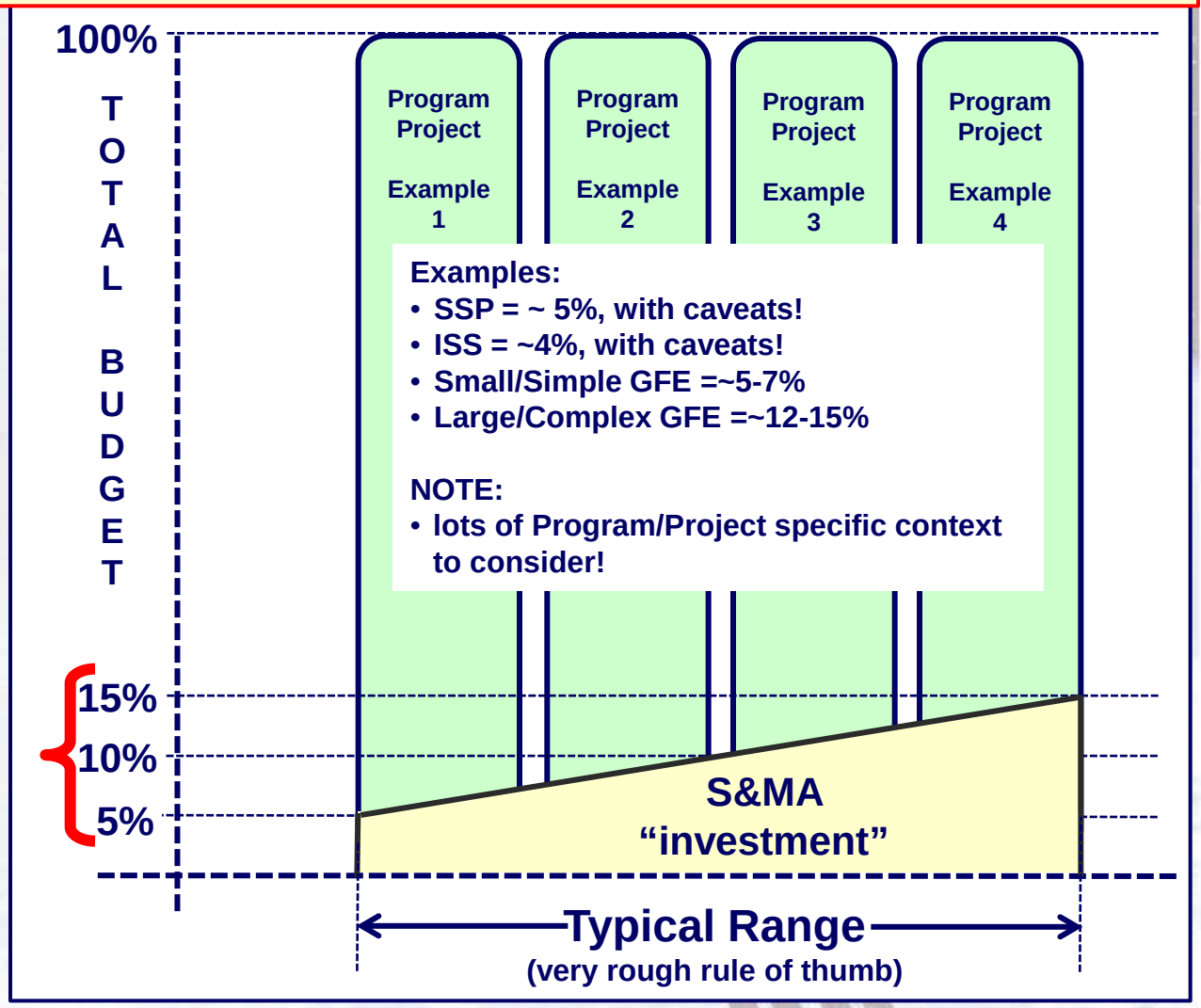
George K. Gafka 281-483-7732

~~So, how much should S&MA "cost"?~~
How much should be "invested" in S&MA?

Core tenets:
- S&MA is an "investment", not a "cost." S&MA enables safety and mission success… and actually saves money!
- S&MA is an Agency, Program, Project, or Center risk mitigation strategy against safety, mission success, schedule and cost (cost of quality) threats

Program/Project S&MA scope?
- Large? Small?
- Complex? Simple?
- Critical functions?
- Critical hazards?
- Make vs. buy? "in-line"?
- Insight/oversight model?
- "Human" spaceflight?
- Who is accountable?
- Multiple NASA centers?
- Multiple contractors?
- International Partners?
- TRL level? objectives?
- Acquisition phase/maturity? (SRR? PDR? CDR? Ops?)

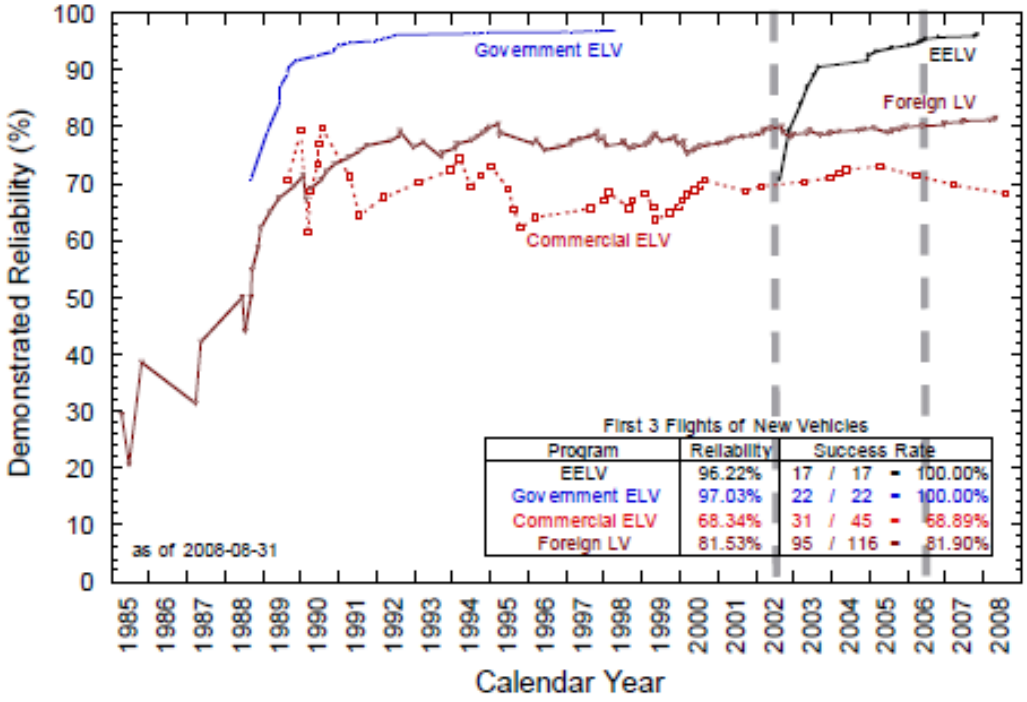
Notionally represents *one comparative snapshot in time*, changes over lifecycle!



Demonstrated Value of "Assurance"
Historical Example

Early Mission Reliability (First 3)

AEROSPACE
Assuring Space Mission Success



- Design certification effect on early mission reliability is significant
  - *97.0% vs 69.9% reliability – heritage vs. commercial*
  - *96.2% vs 69.9% reliability – EELV vs. commercial*
- Order of magnitude difference in failure rates
  - *3% vs 30% failure rates*

100% of failures were commercial launches

Historical Account of "Human Rating"
We've Gotten There Multiple Ways

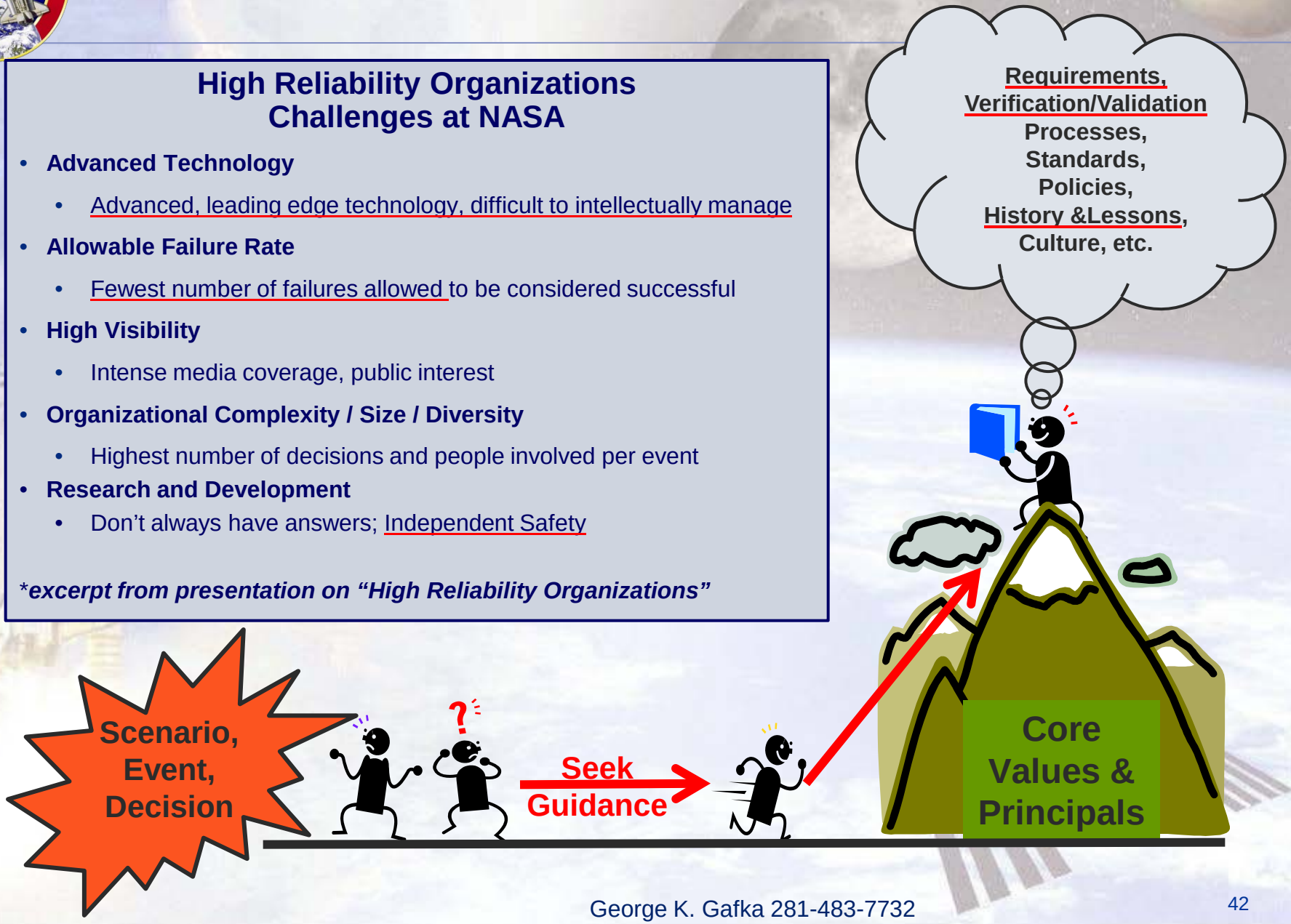
George K. Gafka 281-483-7732

S&MA's Challenges

High Reliability Organizations Challenges at NASA

- **Advanced Technology**
  - Advanced, leading edge technology, difficult to intellectually manage
- **Allowable Failure Rate**
  - Fewest number of failures allowed to be considered successful
- **High Visibility**
  - Intense media coverage, public interest
- **Organizational Complexity / Size / Diversity**
  - Highest number of decisions and people involved per event
- **Research and Development**
  - Don't always have answers; Independent Safety

****excerpt from presentation on "High Reliability Organizations"***



Modern-Day Guidance For "Transportation"
Do We Set Ourselves Up For "Failure"?

High Risk Endeavour!

Mission Directorate: Exploration Systems
Theme: Commercial Spaceflight
Program: Commercial Crew Program Overview

"Failure" meaning: performance ≠ expectations

The Commercial Crew Program will provide $6 billion over the next five years to support the development of commercial crew transportation providers to whom NASA could competitively award a crew transportation services contract analogous to the Cargo Resupply Services contract for ISS.

These funds will be competed through COTS-like, fixed-price, milestone-based Space Act Agreements that support the development, testing, and demonstration of multiple commercial crew systems. As with the COTS cargo program, some amount of private investment capital will be included as part of any Space Act Agreement and NASA will use this funding to support a range of higher- and lower-programmatic risk systems. Unlike the COTS program, which exclusively funded entirely new and integrated systems (launch vehicles plus capsules), this program will also be open to a broad range of commercial proposals including, but not limited to: human-rating existing launch vehicles, developing spacecraft for delivering crew to the ISS that can be launched on multiple launch vehicles, or developing new high-reliability rocket systems.

NASA will leverage existing COTS and Commercial Crew Development (CCDev) activities to engage a broad spectrum of private industry, from emerging to established companies, with a full and open competition for commercial development activities at the conclusion of the CCDev activities. The competition will result in a targeted portfolio of up to four companies with a mixed risk balance consisting of launch vehicles, crew capsules, and supporting technologies, similar to the Commercial Crew Development awards from Recovery Act funds announced on February 2, 2010. The number of awardees will be based on such factors as technical competency and available funds. Firm-fixed-price awards will be issued for production of crew services after a key progress review of the down-selected commercial companies as necessary, within the available budget.

?!?

At no point in the development and acquisition of commercial crew transportation services will NASA compromise crew safety. NASA has unique expertise and history in this area, and a clearly demonstrated record of success. NASA will bring that experience to bear in the appropriate way to make sure that commercial crew transportation services are a success both programmatically, and with respect to safety. In that regard, NASA agrees with the Aerospace Safety Advisory Panel, which stated, "it is crucial that NASA focus on establishing the certification requirements, a certification process for orbital transportation vehicles, and a process for validating compliance. The performance and safety requirements must be stated promptly and clearly to enable NASA and non-NASA entities to proceed in the most productive and effective manner possible." NASA will work to complete an agency and industry-coordinated human rating draft by the end of 2010.

http://www.nasa.gov/pdf/428356main_Exploration.pdf

George K. Gafka 281-483-7732

Historic Guidance For "High Risk Exploration"

Today: Are We Too Risk Averse To "Explore" More Cheaply? Are We Too Cheap To Buy The Risk Posture We Say We Want?

Or, is there some new (elusive) way to achieve better S&MA for less $?

"To your own discretion therefore must be left the degree of danger you risk, and the point at which you should decline, only saying we wish you to err on the side of your safety, and to bring back your party safe even if it be with less information."

Thomas Jefferson Letter to Meriwether Lewis: 1803

During the "Heroic Age of Exploration," the period in which Shackleton's 1914-1916 British Imperial Trans-Antarctic Expedition took place, Antarctic expeditions often became ordeals of suffering. At the time, polar explorers were revered for their sacrifices and held up as heroes, albeit often tragic ones. Shackleton handpicked some members, to recruit the rest, ***it is said*** that he posted the following notice:


MEN WANTED
for hazardous journey, small wages, bitter cold, long months of complete darkness, constant danger, safe return doubtful, honor and recognition in case of success.
Ernest Shackleton 4 Burlington st.
MEN—Near-appearing young men of pleasing personality.

Thank you,
Onward and Upward!