STI 10-148

Safety Goals at NASA

or

"How Safe is Safe Enough and How to Get There"

TRISAMC, NSC
October 26, 2010

Dr. Michael Stamatelatos, Director
Safety and Assurance Requirements Division
Office of Safety and Mission Assurance
NASA Headquarters

Safety Improvement

- NASA is developing and implementing safety improvements in all its activities:
  - Mission design
  - Mission operation
  - Occupational safety
  - Etc.
- Decisions regarding where and how improvements are implemented to optimally enhance safety are discussed here

Rule- vs. Performance-based Decisions

- **Prescriptive (Rule based):** Decide based on rules dictated by experience or tradition
  - Example: Use double failure tolerance (triple redundancy) in design for all safety related systems to increase safety
- **Performance based:** Decide based on performance measures (metrics) that are related to risk
  - Example: Conduct a PRA and use levels of failure tolerance (or redundancy) in design that are consistent with the risk importance of the system (e.g., higher levels of redundancy for systems with higher risk contribution

Safety Thresholds and Safety Goals

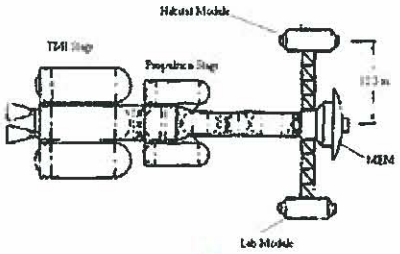
- **Safety Thresholds** are used for risk acceptability decisions; not meeting these values is not acceptable

- **Safety Goals** are directions to drive safety improvements to; it is desirable but not mandatory to meet these values

Safety Thresholds and Safety Goals (cont'd)

- Collectively, safety goal and threshold help
  - Designers with safety performance allocation
  - Decision makers to deal with safety-related decisions
    - Risk acceptance
    - Risk mitigation
    - Safety optimization

Integration of Safety Analysis Techniques



Vehicle

Systems

Sub-Systems

Components and supporting systems

Scenarios

Probabilistic Analysis

Phenomenological Analysis

Hazards Analysis

Insights and Controls, and Decision Making

Safety Regimes and Safety Decisions

Standard of "Optimally and Sufficiently Safe"
More than this May have diminishing return
GOAL

Standard of "Minimally Safe Level"
Less than this would be "unacceptable"
TRESHOLD

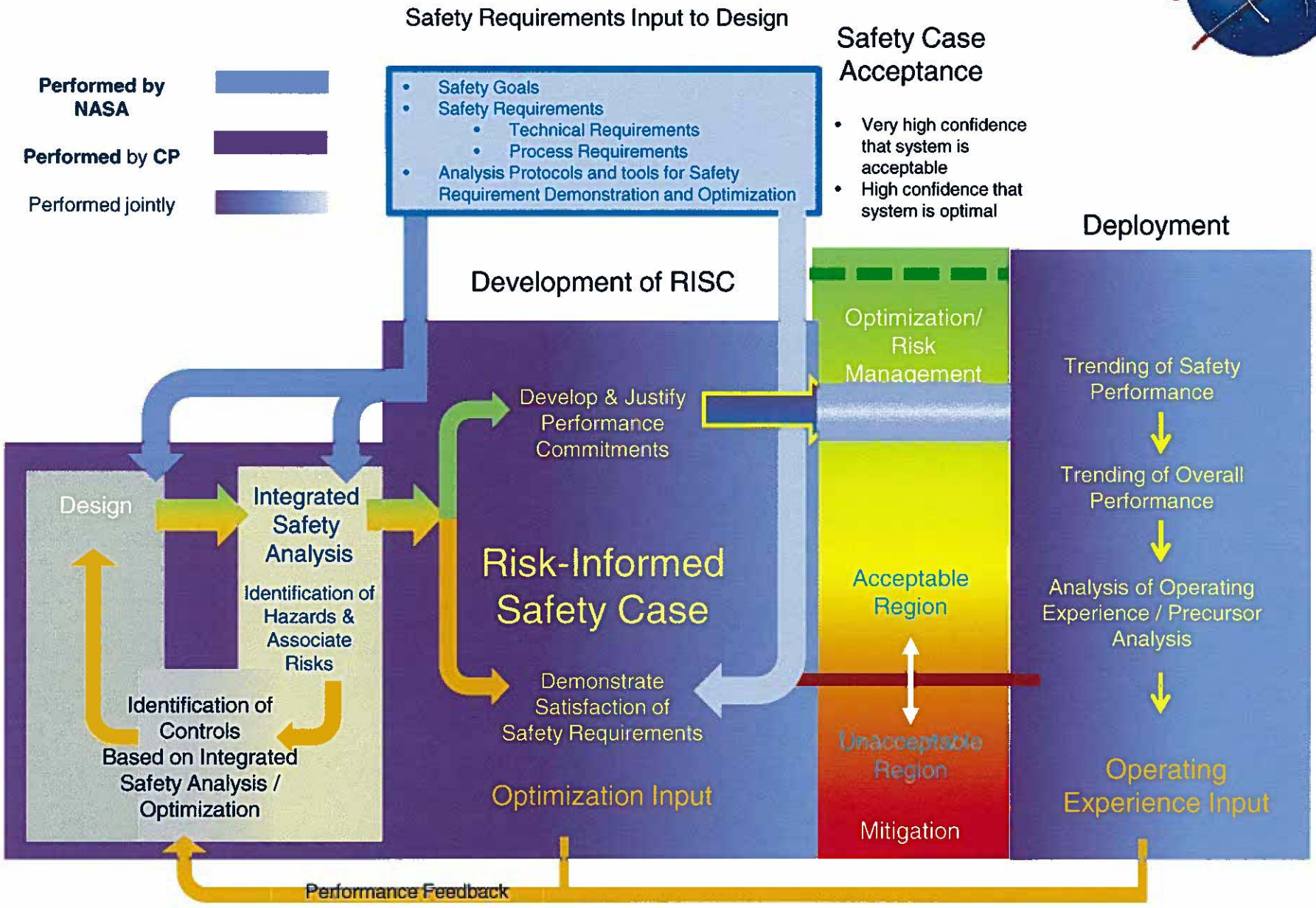
- Keep alert for enhancements, but focus more on maintaining the good safety level that has been been achieved

- Actively pursue safety improvements via risk tradeoff studies
- Actively identify unaccounted-for hazards via precursor analysis

- Don't proceed with the lunch or procurement
- Fix design or operation to meet the threshold.

Aggregate Frequency of Scenarios Leading to Loss of Crew

Role of Commercial Provider (CP) and Role of NASA



Risk-Informed Safety Case (RISC)

A documented body of evidence that provides a convincing and valid argument that…

1. **Applicable safety standards and requirements are met**
   - **The design is executed to the specifications indicated,**
   - **The system is operated in accordance with specified operational rules and practices (e.g., system / mission-specific flight rules),**
   - **Programmatic and Risk Management activities provide ongoing assurance of satisfaction of allocated safety performance**
   - **Operating experience is analyzed to assure, to the extent possible, that unaccounted-for hazards are identified and controlled if necessary through modifications to design or operating practice (precursor analysis)**

AND

2. **A given system is adequately and optimally safe for a given application in a given environment,**

AND

3. **A process of system optimization has been carried out to identify and implement net-beneficial improvements**

System designers are encouraged to continuously optimize (throughout the lifecycle), not just comply with requirements.
The goal is to be "optimally safe enough" – this is a safety philosophy.

Performance-Based Launch Decisions

- Decisions regarding launch safety should be based on safety performance measures, e.g. the probability of loss of crew, p(LOC)
- The total p(LOC) for the mission is:

  $p(LOC) = p(LOC)_{ascent} + p(LOC)_{orbit} + p(LOC)_{entry}$
- A good measure for a safety comparison among space vehicles is the $p(LOC)_{flight}$, the p(LOC) value for only the flight portion of the mission, i.e.

  $p(LOC)_{flight} = p(LOC)_{ascent} + p(LOC)_{entry}$

  The $p(LOC)_{orbit}$ varies depending on the length of the mission

Safety Goal and Threshold Evaluation Protocol

- Analysis protocol is:
  - Use model (e.g., success criteria) and show you are good enough
  - Analysis insensitive to credible modeling perturbations and realistically foreseeable new information (i.e., is robust).
- Evaluation protocol is:
  - Verify that RISC (or subset) meets our acceptance criteria, safety goal, and safety threshold
- Protocol will include reviews at key decision points:
  - Review is on the RISC, which provides the technical argument that the system will be operated at a level of safety consistent with deterministic and probabilistic safety criteria
  - As additional evidence is gathered, design may be judged to meet (or not) safety thresholds