The New Iron Triangle: Risk, Process, and Judgment

Dr. John Sommerer
Space Department Head
and
JHU Gilman Scholar

October 18, 2011

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

Apollo 13

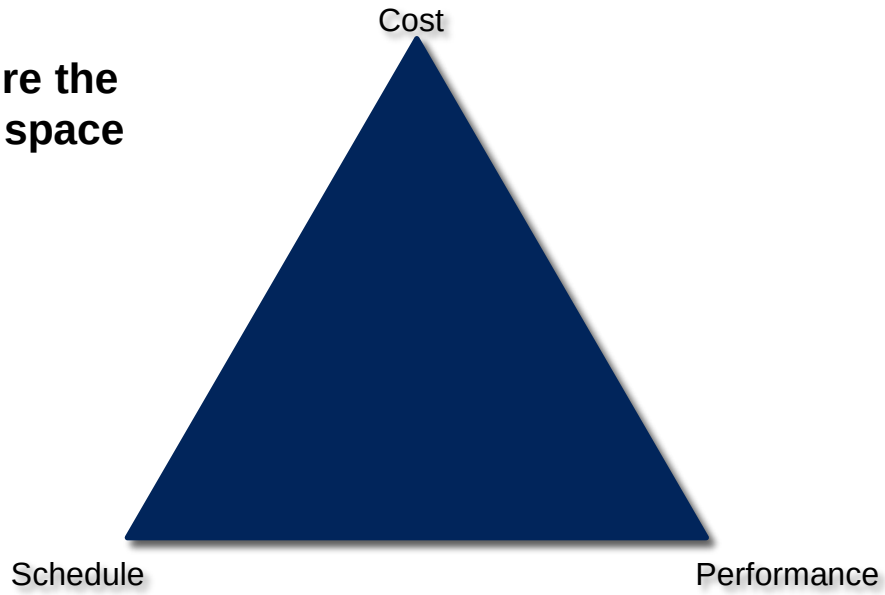
Traditional Project Management Modeling

- **The "Project Management Triangle" or "Iron Triangle" developed in the 1970s by Dr. Martin Barnes has been used throughout the last 45+ years to illustrate the interrelated constraints imposed on any project.**

- **The related theory is, of course, that emphasizing or focusing on any one inevitably affects the others.**

- **However, this triangle does not capture the dilemma in which we find today's US space program.**

- **We need a new "iron triangle"**
  - **Risk**
  - **Process**
  - **Judgment**



The New Iron Triangle - Risk

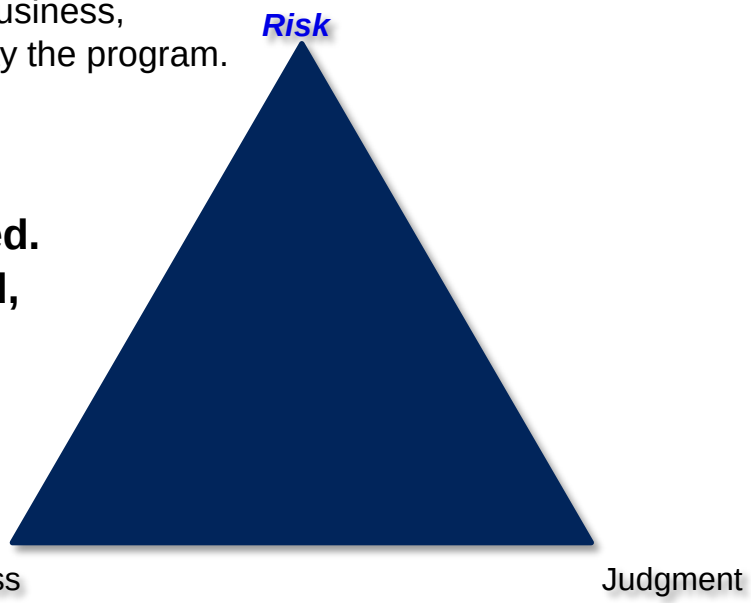
- **Early in the Space Program, it was understood that our work is inherently risky and that failures were going to occur.**

- **The continuation of the Apollo program even after devastating loss was evidence that risk was accepted as part of the path to exceptional achievement.**

If we die, we want people to accept it. We are in a risky business, and we hope that if anything happens to us it will not delay the program. The conquest of space is worth the risk of life.

- Astronaut Virgil 'Gus' Grissom, January 1967

- **Over time, however, this attitude has changed. The level of risk we accept has been lowered, and achievements are more incremental.**



The New Iron Triangle - Risk

- **Often, the method used to try and reduce risk in response to failures in the Space Program has been to add requirements, introduce additional process controls, and reduce independent decision making.**

- **After the tragic loss of Challenger, in 1986, six of the nine Rogers Commission recommendations related to adding oversight, processes, more stringent requirements, or increasing the number of required approvers to move forward on the path to mission completion.**

- **More than two thirds of the Columbia Accident Investigation Board's 29 recommendations were similarly focused on process controls, additional procedural requirements, and increased independent oversight.**

The New Iron Triangle - Risk

- **We have adopted the risk averse Hollywood version of how the Space Program should be run made famous in the 1995 movie Apollo-13:**

"FAILURE IS NOT AN OPTION"

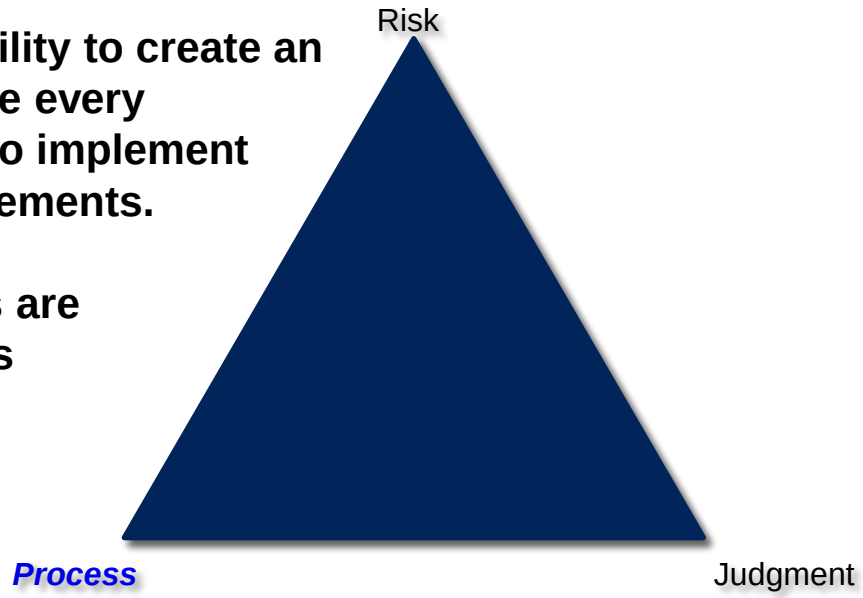
- **We should, instead, consider looking at the origin of that famous historical fiction made public 2009:**

In preparation for the movie, the script writers, Al Reinart and Bill Broyles, came down to Clear Lake to interview me on "What are the people in Mission Control really like?" One of their questions was "Weren't there times when everybody, or at least a few people, just panicked?" My answer was "No, when bad things happened, we just calmly laid out all the options, and ***failure was not one of them***. We never panicked, and we never gave up on finding a solution." - *Jerry C. Bostick*

- **Our desire to mitigate risk need not only to focus on additional process and requirements, it must also focus on improving decision making and judgment of the people working the program.**

The New Iron Triangle - Process

- **Addressing myriad processes, requirements, reviews, and additional oversight have become a large part of both planning and cost for today's space missions.**
- **Many are rational and direct responses to attempting to ensure that failures experienced do not recur. Individually, they may each address a possible condition that should be avoided.**
- **Collectively, however, they have the ability to create an environment where by trying to mitigate every possible risk, we may become unable to implement ground-breaking technological advancements.**
- **The well known quip that "All missions are Class A once they get to the range" has become painfully true in our work.**

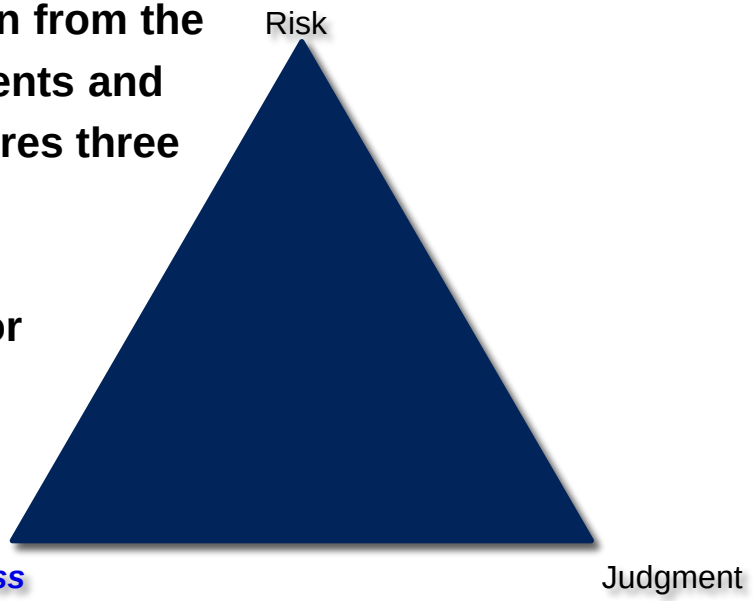


The New Iron Triangle - Process

- **A recent review of the standard Safety and Mission Assurance requirements from one government sponsor demonstrated that there were over 2400 "shall" statements in the body of the text, with 40 additional reference documents that each contained a similar number of additional requirements.**

- **Contractually imposed requirements between two NASA missions at APL demonstrated that a mission from the early 1990s came with 27 pages of requirements and process controls while a 2006 contract requires three two inch binders to hold all of the pages.**

- **A streamlining project currently underway for APL's AS9100 and CMMI Level 3 certified Quality Management System includes over 16000 requirements.**



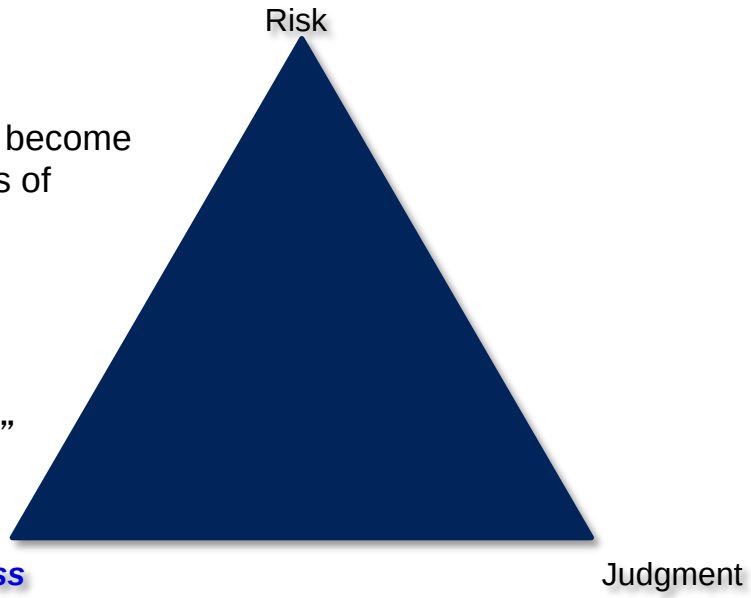
The New Iron Triangle - Process

- **The concern about overburdening programs with processes and requirements in not a new one, but it as relevant today as it was early on in the Space Program.**

- **As early as 1969, the recognition that risk mitigation based solely on adding process controls and more stringent requirements was expressed by top NASA management.**

I believe that the fundamental difficulty is that we have all become so entranced with technique that we think entirely in terms of procedures, systems…reliability systems, configuration management, and the other minor paper tools…
We have forgotten that someone must be in control and must exercise personal management, knowledge and understanding to create a system. As a result, we have developments that follow all of the rules, but fail."

- Robert Frosch, Former NASA Administrator

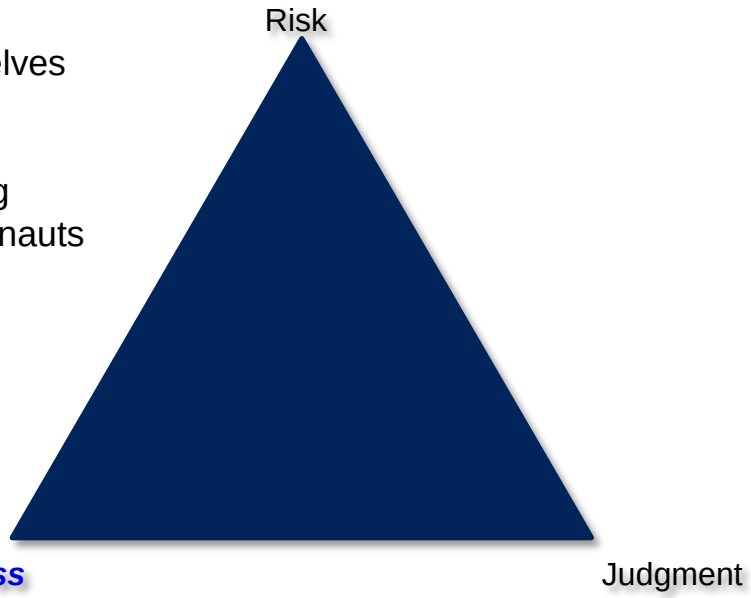


The New Iron Triangle - Process

- **Another critical aspect of increased dependence on process controls and the belief that the stringent requirements imposed on Space Missions to consider is that it can lead to a false sense of security – a belief that compliance with controls and requirements will ensure success and reduced mission risk.**

Challenger was lost because NASA came to believe its own propaganda… that technology—engineering—would always triumph over random disaster if certain rules were followed. The engineers-turned-technocrats could not bring themselves to accept the psychology of machines with abandoning the core principle of their own faith: equations, geometry, and repetition—physical law, precision design, and testing —must defy chaos. No matter that astronauts and cosmonauts had perished in precisely designed and carefully tested machines. Solid engineering could always provide a safety margin, because the engineers believed, there was complete safety in numbers.

- William E. Burrows, This New Ocean, 1998

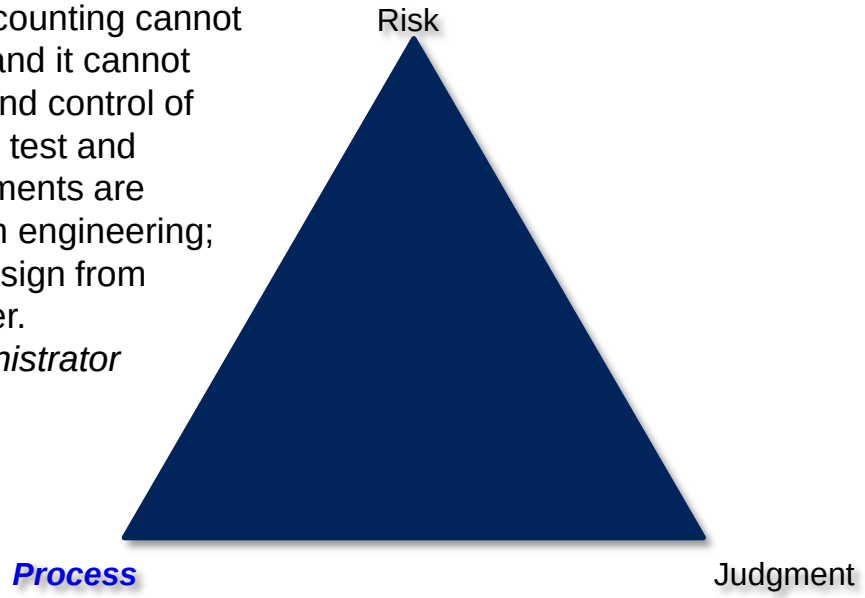


The New Iron Triangle - Judgment

- **Along with risk and process, we must understand the critical role of maintaining experienced-based judgment as part of the new Iron Triangle**

…the system engineering *process* bears the same relationship to system engineering that financial *accounting* does to financial management. Careful financial accounting is an essential element of a good financial management plan; however, accurate accounting cannot distinguish between a good plan and a poor one, and it cannot make a bad plan better. Similarly, understanding and control of system interfaces, development of comprehensive test and verification plans, and proper allocation of requirements are among the things which are crucial to good system engineering; however, they do not help to distinguish a good design from a poor one, nor can they make a poor design better.

- *Michael D. Griffin, Former NASA Administrator*
  September 27, 2010

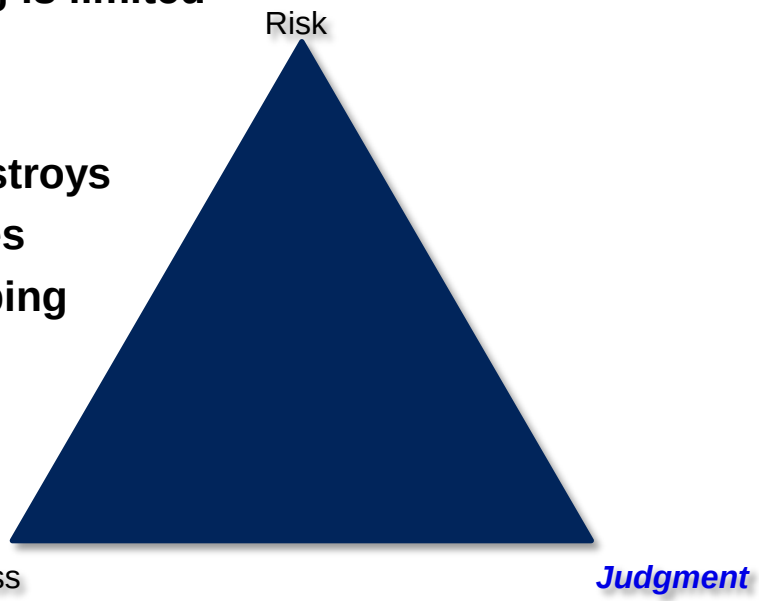


The New Iron Triangle - Judgment

- **There are critical reasons for ensuring that we focus on maintaining the ability for mission members to use their own judgment during program development.**

- **The best engineering teams shut down when they no longer feel authority or responsibility because their decision making is limited by imposed processes.**

- **Taking away engineering judgment often destroys natural mission cadence; standard processes typically run on predefined schedules, stopping to check on whether decisions being made meet requirements or require waivers can take hours or days.**



The New Iron Triangle - Judgment

I can best describe the spirit of what I have in mind by thinking of a music student who writes a concerto by consulting a checklist of the characteristics of the concerto form, being careful to see that all of the canons of the form are observed, but having no flair for the subject, as opposed to someone who just knows roughly what a concerto is like, but has a real feeling for music. The results become obvious upon hearing them. The prescription of technique cannot be a substitute for talent and capability, but that is precisely how we have tried to use technique.…

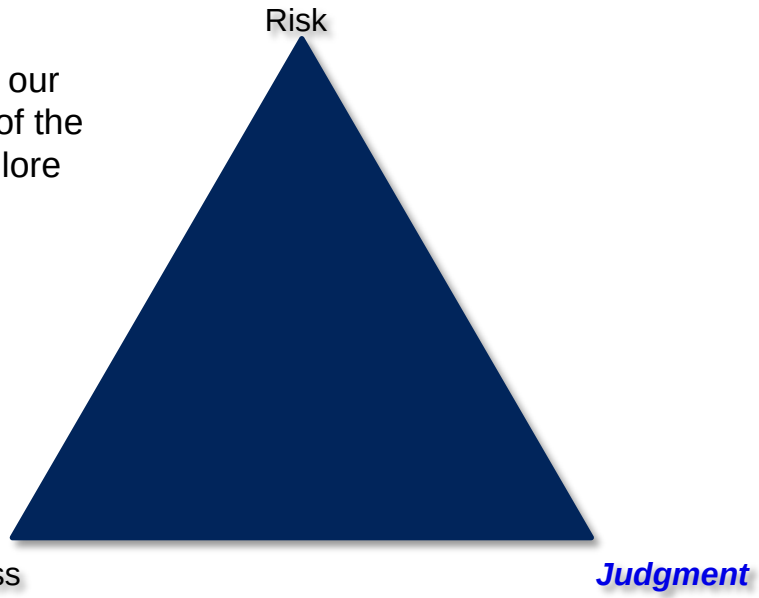
- Robert Frosch, Former NASA Administrator, 1969

You have to be willing to take chances and get it wrong every once in a while. If something's going to go wrong in our world at NASA I want it to be because we're on the edge of the envelope. We do dangerous stuff, we experiment, we explore and what that means is every once in a while we're going to screw up. We do not want to make a stupid mistake, but we're always trying to go a little bit farther than our arms can extend.

- Charles Bolden, NASA Administrator, 2011

If one took no chances, one would not fly at all.
Safety lies in the judgment of the chances one takes.

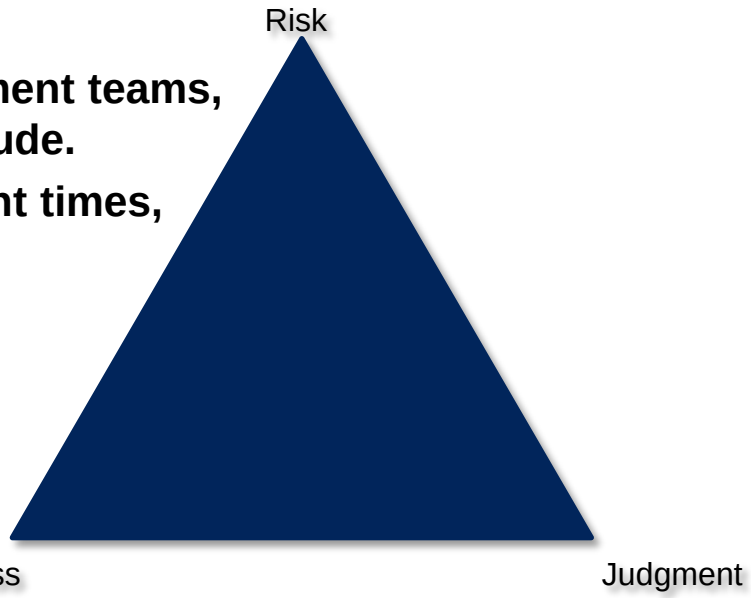
- Charles Lindbergh, 1938



The New Iron Triangle - Summary

- **Failure is *always* an option. One exercised by the Universe.**
  - **Space exploration carries risk.**
- **We need to learn from failure, and not repeat mistakes.**
- **We need to recognize that mistakes will happen in the development of complex systems.**
  - **The processes followed must encourage the the discovery of mistakes.**
- **Excessive process demotivates development teams, engendering a CYA, "check the box" attitude.**
- **Excessive process lengthens development times, and thus interferes with the development of experience-based judgment.**

Balance in all things



JOHNS HOPKINS
UNIVERSITY

Applied Physics Laboratory

Backup Materials

- **Remainder of the presentation**

Back-up Materials

Rogers Commission:

While the report of the Rogers Commission is several thousand pages long, the nine basic recommendations, and specific actions taken by NASA prior to the return of Space Shuttles to flight on September 29, 1988 may be summarized as follows:

1. The Space Shuttle Solid Rocket Boosters (SRB) were extensively redesigned. This involved recertifying the boosters through a series of static test firings at the Morton Thiokol test facility in Utah.
The redesign effort added an extra O-ring to the joints between the SRB segments and greatly strengthened the physical connections between these segments. Heaters were also added to the joints between the SRB segments to prevent cold weather from affecting the sealing capability of the O-rings.

2. Although landing system safety obviously was not a factor in the Challenger explosion, the Rogers Commission did uncover basic flaws in the safety of the Space Shuttle landing system.
The Space Shuttle tires, brakes and nose wheel steering mechanisms were upgraded. A drag chute system was added to the Space Shuttle to help reduce its speed upon landing.

3. Numerous hardware, software and safety improvements were incorporated into the Space Shuttle. These included the addition of a crew escape system which would allow astronauts to parachute from the Space Shuttle in certain conditions.
Astronauts, who had previously been boarding the Space Shuttle dressed in jumpsuits and helmets, were required to instead wear pressurized flight safety suits during launch and landing operations.

4. New and strict risk identification and reduction programs were applied to all Space Shuttle operations. NASA and contractor quality control work forces were strengthened.

Back-up Materials

Rogers Commission (continued)

5. The Space Shuttle program was reorganized and decentralized to make sure all pertinent information was made available to management personnel at all levels. Where possible, experienced astronauts were placed in key NASA management positions to assure that the unique astronaut perspective would be consulted in launch decisions.

6. Documentation from all previous Space Shuttle missions was reviewed, and all documented waivers to existing flight safety criteria were revoked and forbidden. These included, but were not restricted to, previous decisions that allowed Space Shuttles to be launched in overly windy, cloudy and/or rainy conditions.
Certain launch commit weather criteria, especially those concerning temperature, winds and cloud cover, were reviewed and made more strict. Requirements were enacted which forced NASA and the contractor community at all management levels to be in complete agreement regarding launch decisions.

7. Any technical issues arising during preparation for a particular Space Shuttle mission were opened up to review by independent government agencies, such as the National Research Council, who would in turn relay their analysis and opinions to NASA.

8. A series of open reviews were enacted to discuss all significant and outstanding issues prior to a particular Space Shuttle mission. These discussions were elevated to the level of the NASA Associate Administrator for Space Flight and the NASA Associate Administrator for Safety.
These open reviews would afford discussions of all occurring or potentially occurring issues surrounding a Space Shuttle mission, with participation encouraged from all levels of NASA and contractor management, engineering and safety personnel.

9. A mechanism was put into place that would allow NASA and contractor personnel to provide open and anonymous reporting of Space Shuttle safety concerns without fear of reprisal.

Back-up Materials

CAIB's Recommendations and Observations
Return to Flight (RTF) Recommendations. CAIB recommends that NASA:

- initiate an aggressive program to eliminate all External Tank foam shedding;
- initiate a program to increase the orbiter's ability to sustain minor debris damage;
- develop and implement a comprehensive inspection plan to assess the structural integrity of the RCC panels, supporting structure, and attaching hardware;
- develop a practical capability to inspect and effect emergency repairs to the orbiter's thermal protection system (TPS) both when near the International Space Station and when operating away from it, and accomplish an on-orbit TPS inspection;
- upgrade the ability to image the shuttle during its ascent to orbit;
- obtain and downlink high resolution images of the External Tank after it separates from the orbiter, and of certain orbiter thermal protection systems;
- ensure that on-orbit imaging of each shuttle flight by Department of Defense satellites is a standard requirement;
- test and qualify "bolt catchers" used on the shuttle;
- require that at least two employees attend final closeouts and intertank area handspraying procedures when applying foam to the External Tank;
- require NASA and its contractors to use the industry-standard definition of "foreign object debris";
- adopt and maintain a shuttle flight schedule that is consistent with available resources;
- implement an expanded training program for the Mission Management Team;
- prepare a detailed plan for creating an independent Technical Engineering Authority, independent safety program, and reorganized space shuttle integration office; and
- develop an interim program of closeout photographs for all critical sub-systems that differ from engineering drawings.

Back-up Materials

Continuing to Fly Recommendations. The Board recommends that NASA:

• increase the orbiter's ability to reenter the atmosphere with minor leading edge damage to the extent possible;
• develop a better database to understand the characteristics of Reinforced Carbon-Carbon (RCC) by destructive testing and evaluation;
• improve the maintenance of launch pad structures to minimize leaching of zinc primer onto RCC;
• obtain sufficient RCC panel spares so maintenance decisions are not subject to external pressures relating to schedules, costs, or other considerations;
• develop, validate, and maintain physics-based computer models to evaluate Thermal Protection System damage from debris impacts;
• maintain and update the Modular Auxiliary Data System (MADS) on each orbiter to include current sensor and data acquisition technologies, and redesign the MADS so they can be reconfigured during flight;
• develop a state-of-the-art means to inspect orbiter wiring;
• operate the shuttle with the same degree of safety for micrometeoroid and orbital debris as is used in the space station program, and change guidelines to requirements;
• establish an independent Technical Engineering Authority that is responsible for technical requirements and all waivers to them, which should be funded directly from NASA Headquarters and have no connection to or responsibility for schedule or program cost;
• give direct line authority over the entire shuttle safety organization to the Headquarters Office of Safety and Mission Assurance, which should be independently resourced;
• reorganize the Space Shuttle Integration Office to make it capable of integrating all elements of the Space Shuttle Program, including the Orbiter;
• develop and conduct a vehicle recertification prior to operating the shuttle beyond 2010 and include recertification requirements in the Shuttle Life Extension Program;
and
• provide adequate resources for a long-term program to upgrade shuttle engineering drawings.

Characterization	Class A	Class B	Class C	Class D
Priority (Criticality to Agency Strategic Plan) and Acceptable Risk Level	High priority, very low (minimized) risk	High priority, low risk	Medium priority, medium risk	Low priority, high risk
National significance	Very high	High	Medium	Low to medium
Complexity	Very high to high	High to medium	Medium to low	Medium to low
Mission Lifetime (Primary Baseline Mission	Long, >5years	Medium, 2-5 years	Short, <2 years	Short < 2 years
Cost	High	High to medium	Medium to low	Low
Launch Constraints	Critical	Medium	Few	Few to none
In-Flight Maintenance	N/A	Not feasible or difficult	Maybe feasible	May be feasible and planned
Alternative Research Opportunities or Re-flight Opportunities	No alternative or re-flight opportunities	Few or no alternative or re-flight opportunities	Some or few alternative or re-flight opportunities	Significant alternative or re-flight opportunities
Achievement of Mission Success Criteria	All practical measures are taken to achieve minimum risk to mission success. The highest assurance standards are used.	Stringent assurance standards with only minor compromises in application to maintain a low risk to mission success.	Medium risk of not achieving mission success may be acceptable. Reduced assurance standards are permitted.	Medium or significant risk of not achieving mission success is permitted. Minimal assurance standards are permitted.
Examples	HST, Cassini, JIMO, JWST	MER, MRO, Discovery payloads, ISS Facility Class Payloads, Attached ISS payloads	ESSP, Explorer Payloads, MIDEX, ISS complex subrack payloads	SPARTAN, GAS Can, technology demonstrators, simple ISS, express middeck and subrack payloads, SMEX

	Class A	Class B	Class C	Class D
Single Point Failures (SPFs)	Critical SPFs (for Level 1 requirements) are not permitted unless authorized by formal waiver. Waiver approval of critical SPFs requires justification based on risk analysis and implementation of measures to mitigate risk.	Critical SPFs (for Level 1 requirements) may be permitted but are minimized and mitigated by use of high reliability parts and additional testing. Essential spacecraft functions and key instruments are typically fully redundant. Other hardware has partial redundancy and/or provisions for graceful degradation.	Critical SPFs (for Level 1 requirements) may be permitted but are mitigated by use of high reliability parts, additional testing, or by other means. Single string and selectively redundant design approaches may be used.	Same as Class C.
Engineering Model, Prototype, Flight, and Spare Hardware	Engineering model hardware for new or modified designs. Separate prototype and flight model hardware. Full set of assembled and tested "flight spare" replacement units.	Engineering model hardware for new or significantly modified designs. Protoflight hardware (in lieu of separate prototype and flight models) except where extensive qualification testing is anticipated. Spare (or refurbishable prototype) hardware as needed to avoid major program impact.	Engineering model hardware for new designs. Protoflight hardware permitted (in lieu of separate prototype and flight models). Limited flight spare hardware (for long lead flight units).	Limited engineering model and flight spare hardware.
Qualification, Acceptance, and Protoflight Test Program	Full formal qualification and acceptance test programs and integrated end-to-end testing at all hardware and software levels.	Formal qualification and acceptance test programs and integrated end-to-end testing at all hardware levels. May use a combination of qualification and protoflight hardware. Qualified software simulators used to verify software and system.	Limited qualification testing for new aspects of the design plus full acceptance test program. Testing required for verification of safety compliance and interface compatibility.	Testing required only for verification of safety compliance and interface compatibility. Acceptance test program for critical performance parameters.
EEE Parts *http: // nepp .nasa .gov/ index_nasa .cfm/ 641	NASA Parts Selection List (NPSL)* Level 1, Level 1 equivalent Source Control Drawings (SCDs), and/or requirements per Center Parts Management Plan.	Class A requirements or NPSL Level 2, Level 2 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B or NPSL Level 3, Level 3 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B, or Class C requirements, and/or requirements per Center Parts Management Plan.
Reviews	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and code.	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Mission Directorate participation. Include formal inspections of software requirements, design, verification documents, and peer reviews of code.	Full formal review program. Independent reviews managed at Center level with Mission Directorate participation. Include formal inspections of software requirements, peer reviews of design and code.	Center level reviews with participation of all applicable directorates. May be delegated to Projects. Peer reviews of software requirements and code.
Safety	Per all applicable NASA safety directives and standards.	Same as Class A.	Same as Class A.	Same as Class A.

	Class A	Class B	Class C	Class D
Materials	Verify heritage of previously used materials and qualify all new or changed materials and applications/configurations. Use source controls on procured materials and acceptance test each lot/batch.	Use previously tested/flown materials or qualify new materials and applications/configurations. Acceptance test each lot of procured materials.	Use previously tested/flown materials or characterize new materials. Acceptance test sample lots of procured materials.	Requirements are based on applicable safety standards. Materials should be assessed for application and life limits.
Reliability NPD 8720.1	Failure mode and effects analysis/critical items list (FMEA/CIL), worst-case performance, and parts electrical stress analysis for all parts and circuits. Mechanical reliability, human, and other reliability analysis where appropriate.	FMEA/CIL at black box (or circuit block diagram) level as a minimum. Worst-case performance and parts electrical stress analysis for all parts and circuits.	FMEA/CIL scope determined at the project level. Analysis of interfaces. Parts electrical stress analysis for all parts and circuits.	Analysis requirements based on applicable safety requirements. Analysis of interface.
Fault Tree Analysis	System level qualitative fault tree analysis.	Same as Class A.	Same as Class A.	Fault tree analysis required for safety critical functions.
Probabilistic Risk Assessment NPR 8705.5	Full Scope, addressing all applicable end states per NPR 8705.5.	Limited Scope, focusing on mission-related end-states of specific decision making interest per NPR 8705.5.	Simplified, identifying major mission risk contributors.Other discretionary applications.	Safety only.Other discretionary applications.
Maintainability[1] NPD 8720.1	As required by NPD 8720.1	Application of NPD 8720.1 determined by program. (Typically ground elements only.)	Maintainability considered during design if applicable.	Requirements based on applicable safety standards.
Quality Assurance NPD 8730.5 NPR 8735.2 (NPR 8735.1)	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, and stringent surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, moderate surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, tailored surveillance. GIDEP failure experience data and NASA Advisory process.	Closed-loop problem reporting and corrective action, configuration management, GIDEP failure experience data and NASA Advisory process. Other requirements based on applicable safety standards.
Software	Formal project software assurance program. Independent Verification and Validation (IV&V) as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance insight. IV&V as determined by AA OSMA.
Risk Management NPR 8000.4	Risk Management Program. Risk reporting to GPMC.	Same as Class A.	Same as Class A.	Same as Class A.
Telemetry Coverage[2]	During all mission critical events to assure data is available for critical anomaly investigations to prevent future recurrence.	Same as Class A.	Same as Class A.	Same as Class A