Acceptance of Safety and Mission Success Risks

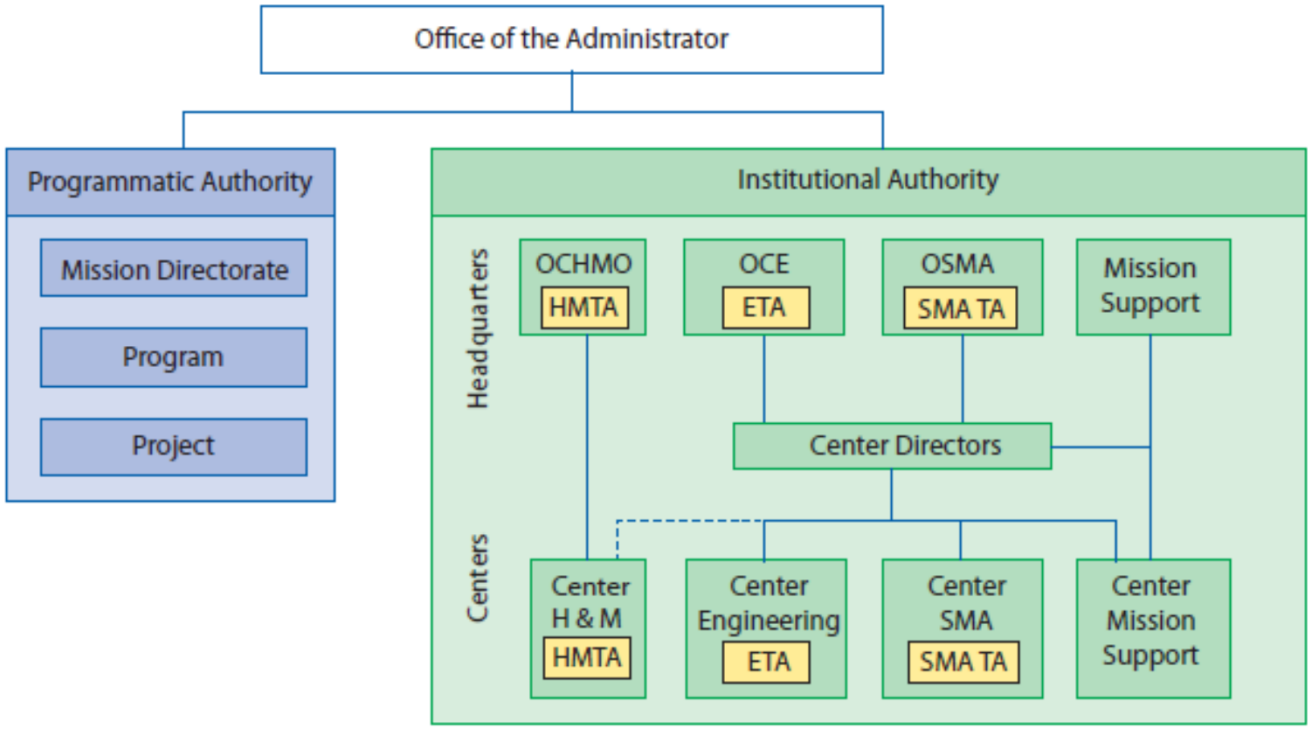
Frank Groen, NASA Office of Safety and Mission Assurance

Presented at Trilateral SMA Working Group meeting, ESRIN, Italy, May 2015

Risk Acceptance and Technical Authority

- Columbia Accident Investigation Board recommended:
  - Create a TA "responsible for technical requirements and all waivers to them"
  - "build a disciplined, systematic approach to identifying, analyzing, and controlling hazards"
- Technical Authority process important part of checks and balances
  - Three TAs: Engineering, SMA, Health and Medical
  - Delegated from Administrator to Chiefs, e.g., Chief SMA
  - Partially delegated to the Center and Program/Project Level
- Technical decisions resulting in residual safety and/or mission success risk require
  - formal acceptance of the risk by the applicable program, project, or operations and facilities manager
  - approval/concurrence of the cognizant Technical Authority (TA) that the risk is acceptable.

Technical Authority as part of NASA Governance Model



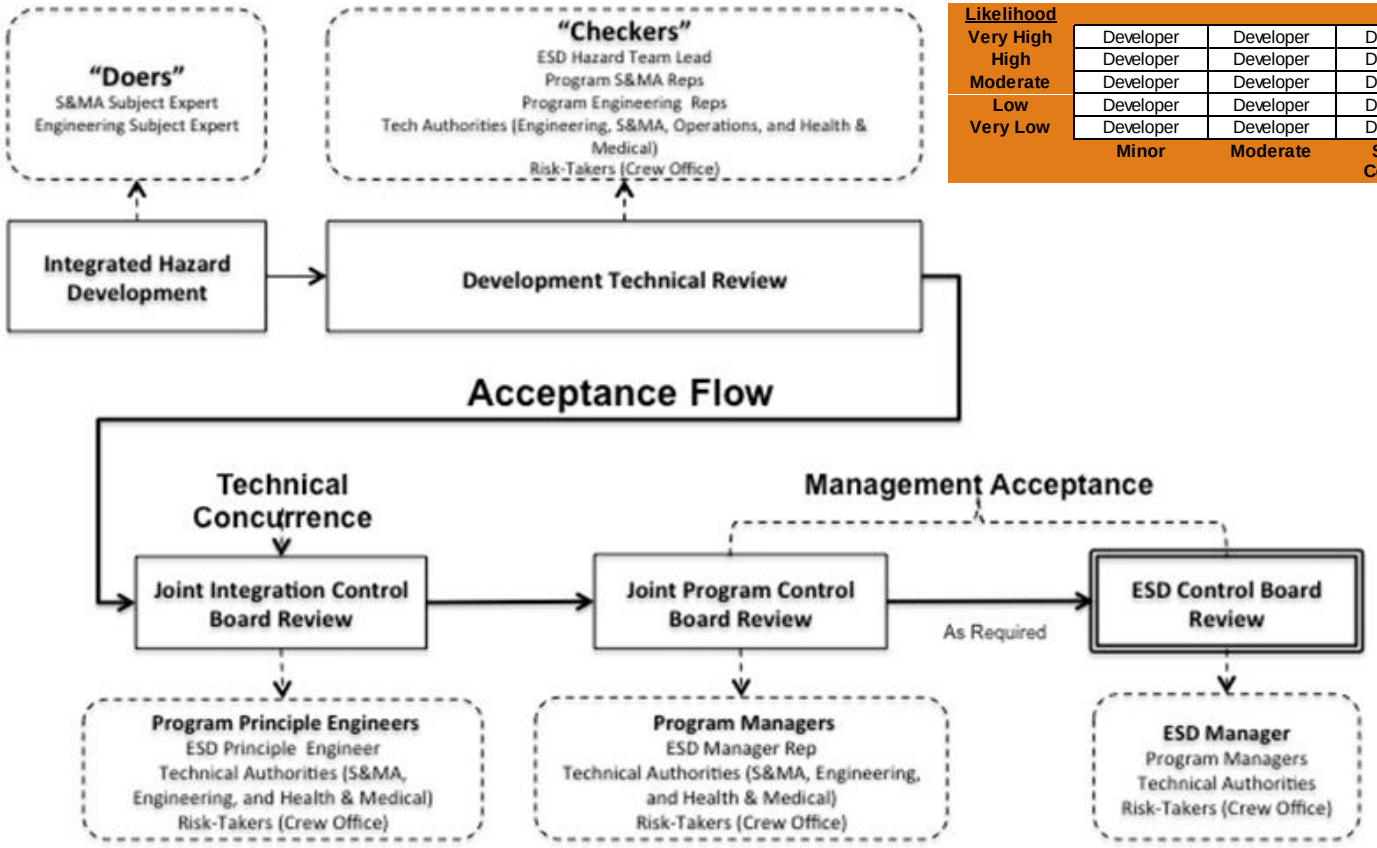
Legend: ---- indicates that not all Centers have HMTA. Sometimes that function is served by Engineering and SMA TAs.

Acronyms: OCE = Office of the Chief Engineer; OCHMO = Office of the Chief Health and Medical Officer; OSMA = Office of Safety and Mission Assurance; TA = Technical Authority.

Figure 2-3 Separation of Programmatic and Institutional Authorities

- http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20150000400.pdf

Example: Safety Risk Acceptance within Exploration Program



Likelihood	Minor	Moderate	Severe Consequence	Critical	Catastrophic
Very High	Developer	Developer	Developer	ESDCB	Administrator
High	Developer	Developer	Developer	ESDCB	ESDCB
Moderate	Developer	Developer	Developer	JPCB/PCB	ESDCB
Low	Developer	Developer	Developer	JPCB/PCB	JPCB/PCB
Very Low	Developer	Developer	Developer	JPCB/PCB	JPCB/PCB

* At any time in the process ESD reps, the Risk-Takers, or TA reps can elevate issues to Program, ESD or TA management

Evolution of Policies regarding Risk Acceptance

- "NASA should consistently provide formal versus ad hoc processes for managing risk with clear accountability. […] NASA often relies on the quality and integrity of its personnel to 'do the right thing,' which makes risk management personality-dependent rather than part of formal processes." – Aerospace Safety Advisory Panel 2013 Annual Report

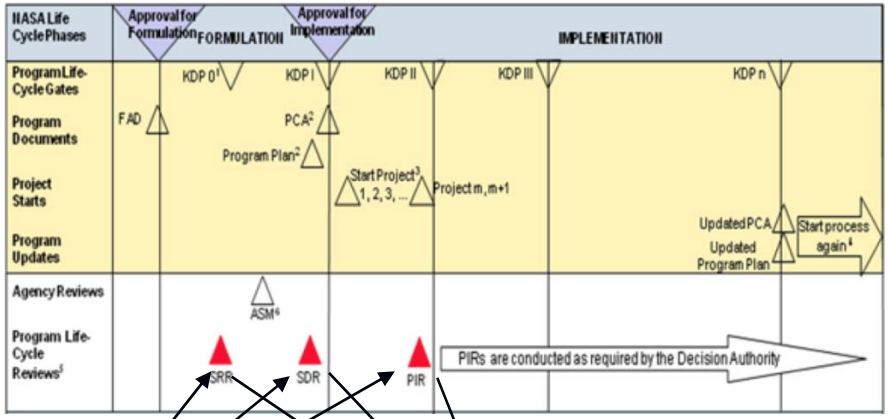
- Policy focus areas:
  - Formal, transparent, single-signature accountability risk acceptance decisions
  - Key Decision Points function as integrated, system-level roll-ups of many decisions through which risk is implicitly or explicitly accepted
  - Clear description of the purpose of any associated concurrences
  - Clear expectation that systems are made as safe as reasonably practicable
- In risk-informed decisions, dissent must be invited, not be a matter of courage

Risk Acceptance Accountability (Notional)

Technical Basis

Documented case that the system is, or will be, safe and reliable for its intended use in its intended environment

Program/Project Life Cycle



Decision Memorandum

Decision Authority signs off on his/her S&MS requirements risk acceptance for each top-level S&MS requirement

TA Non-Concurrence Elevates Risk Acceptance Decision Authority