Risk Management
“Risk As A Resource”

Langley Research Center
May 14, 1998

Dr. Michael A. Greenfield
Deputy Associate Administrator
Office of Safety and Mission Assurance

Topics

- → New Requirements in NPG 7120.5A
- → Our New Environment - “Better, Faster, Cheaper”
- → A New Way: Risk as a Resource (Knowledge-Based, Not Rule-Based)
- → The Role of Safety and Mission Assurance in Understanding Risk

Past Risk Management Approach

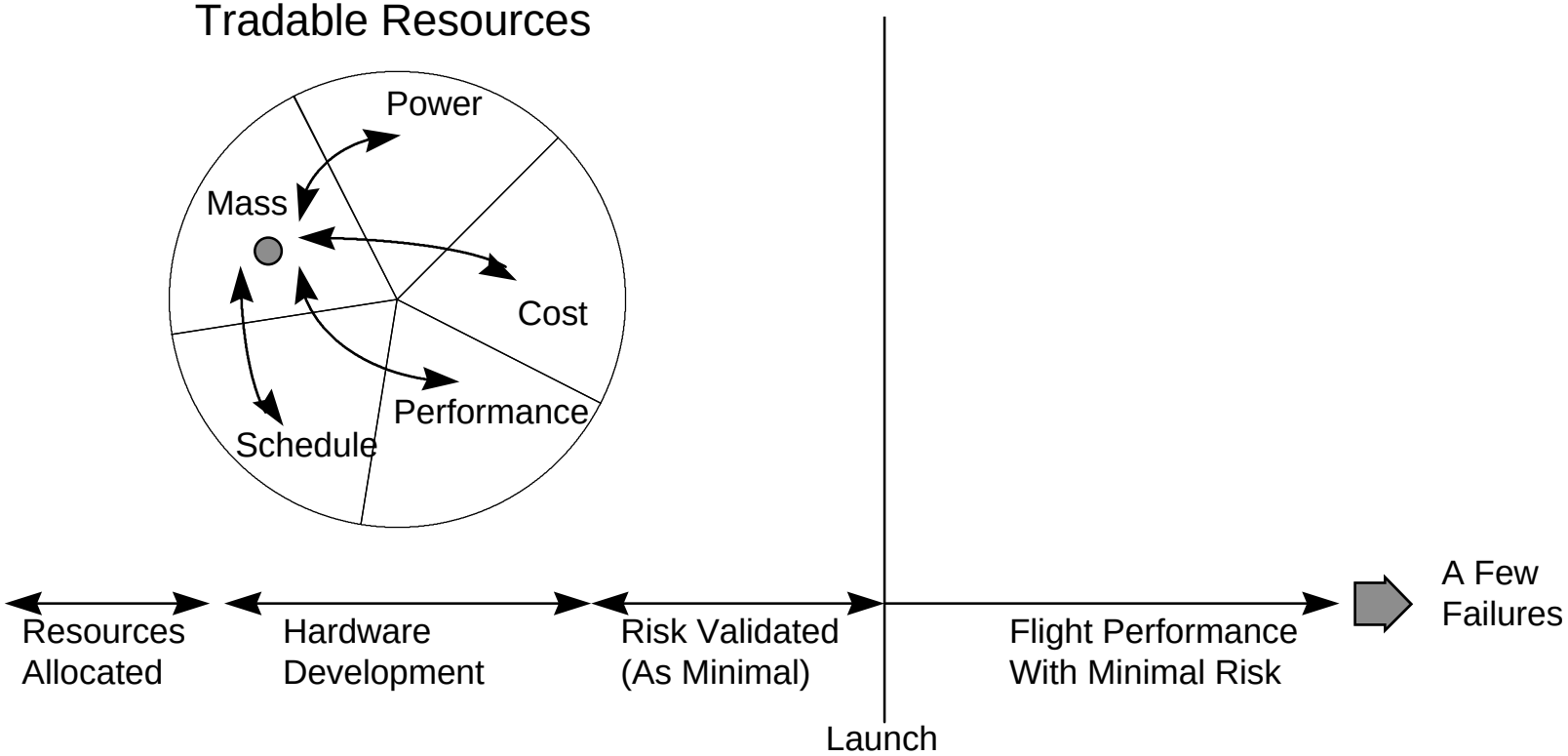
- → Weakly Structured
- → Decoupled from Program Planning
- → Driven by Squeaky Wheel
- → Suboptimized; Limited Data Base; Poor Communication of Overall Impacts
- → Risk as a Consequence
- → Rule-Based, NMI 8010.1A

Risk as a Consequence

Historically

→ Risk to Be Minimized (Avoided)
→ Extensive Analysis and Test
→ Residual Risk Is A Consequence of Deficiency in Tradable Resources

Tradable Resources



Characterization, Mission Success and SRM&QA Cost Guidelines for Class A-D Payloads

Classification	Class A	Class B	Class C	Class D
Characterization	High Priority, Minimum Risk	High Priority, Medium Risk	Medium Priority, Medium/High Risk	High Risk, Minimum Cost
Typical Factors Used to Determine Payload Classifications:	High National Prestige; Long Hardware Life Required; High Complexity; Highest Cost; Long Program Duration; Critical Launch Constraints; Retrieval/Reflight or in-Flight Maintenance to Recover From Problems Is Not Feasible.	High National Prestige; Medium Hardware Life Required; High to Medium Complexity; High Cost; Medium Program Duration; Some Launch Constraints; Retrieval/Reflight or in-Flight Maintenance to Recover From Problems Is Difficult or Not Feasible.	Moderate National Prestige; Short Hardware Life Required; Medium to Low Complexity; Medium Cost; Short Program Duration; Few Launch Constraints; Retrieval/Reflight or in-Flight Maintenance to Recover From Problems May Be Feasible.	Little National Prestige; Short Hardware Life Required; Low Complexity; Low Cost; Short Program Duration; Non-Critical Launch Time/Orbit; Reflyable or Economically Replaceable; In-Flight Maintenance May Be Feasible.
Achievement of Mission Success Criteria:	All Affordable Programmatic and Other Measures Are Taken to Achieve Minimum Risk. The Highest Practical Product Assurance Standards Are Utilized.	Compromises Are Used to Permit Somewhat Reduced Costs While Maintaining a Low Risk to the Overall Mission Success and Medium Risk of Achieving Only Partial Success. Stringent Product Assurance Standards Are Utilized.	Moderate Risks of Not Achieving Mission Success Are Accepted to Permit Significant Cost Savings. Reduced Product Assurance Requirements Are Allowed.	Significant Risk of Not Achieving Mission Success Is Accepted to Permit Minimum Costs. Minimal Product Assurance Requirements Are Allowed.
Estimated Relative SRM&QA Cost Factors:	1.0	0.7 X Class A	0.4 X Class A	0.1 X Class A

Notes: 1. There Are Wide Variations in the Methods for Specifying and Accounting for “SRM&QA Costs”. For Class A Programs, These Costs Are Typically in the Range of 10-15% of the Total Program Cost. The Relative SRM&QA Cost Factors Specified Here Are Intended to Require Substantive Differences in the SRM&QA Programs (and the Associated Costs) for the Various Program Classifications in Order to Establish a Meaningful Ladder of Cost/Risk Levels.

Rule-Based

Guidelines for SRM&QA Program Requirements for Class A-D Payloads

Classification	Class A	Class B	Class C	Class D
SRM&QA Element:				
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 Space" 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. Space (or Refurbishable Prototype) Hardware As Needed to Avoid Major Program Impact If Flight Units Must Be Replaced.	Engineering Model Hardware for New Designs. "Protoflight" Hardware (in Lieu of Separate Prototype and Flight Models). Limited Flight Spare Hardware (for Long Lead or Difficult to Replace Flight Units).	Limited Engineering Model and Flight Spare Hardware.
Failure Investigation Board Requirements	Formal Board Required - Initiated and Conducted by Headquarters.	Formal Board Required - Initiated by Headquarters; May Be Conducted by Cognizant Field Center (See Par. 7A(5)).	Formal Board Required - Initiated and Conducted by Cognizant Field Center.	Failure Investigation Initiated and Conducted by Cognizant Field Center. Formal Board Not Required.
Treatment of Single Failure Points (SFP's)	Success Critical SFP's Are Not Permitted Except by Formal Project Waiver. Retention of Unavoidable SFP's Requires Justification Based on Risk Analysis and Implementation of Measures to Mitigate Risk.	Success Critical SFP's Are Allowed W/O Formal Waiver 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.	Success Critical SFP's Are Allowed W/O Formal Waiver. Single String and Partially Single String Design Approaches Are Commonplace.	Same As Class C.

Rule-Based

Definition: Risk Management (7120.5A)

"An Organized, Systematic Decision-Making Process That Efficiently Identifies Risks, Assesses or Analyzes Risks, and Effectively Reduces Or Eliminates Risks to Achieving the Program Goals."

Effective Project Management Depends on a Thorough Understanding of the Concept of Risk, the Principles of Risk Management, and the Establishment of a Disciplined Risk Management Process.

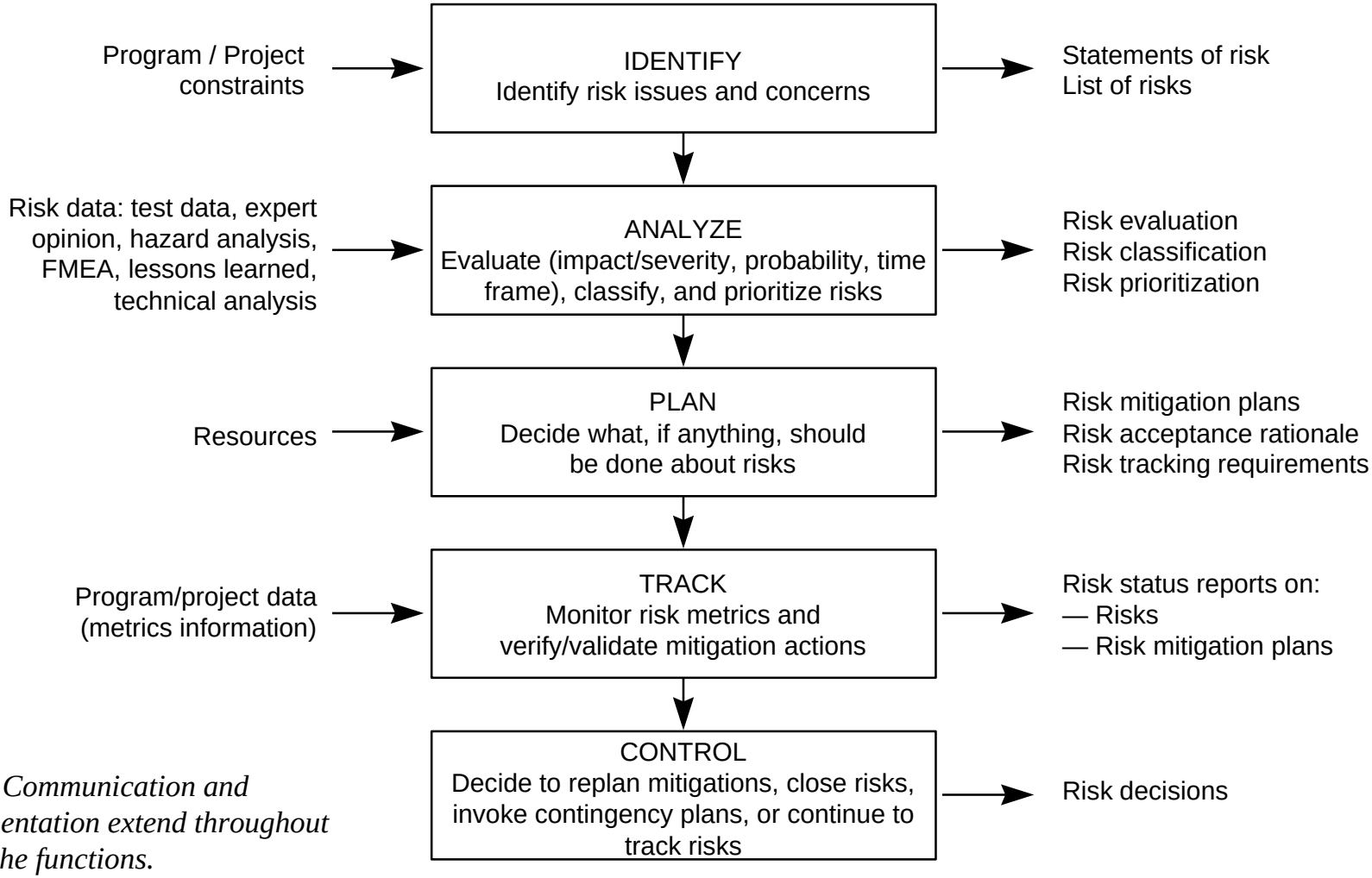
Risk Management in the Revised NASA NPG 7120.5A

- → New Handbook Is Divided Into Four Program Life Cycle Parts
  - → Formulation
  - → Approval
  - → Implementation
  - → Evaluation
- → Stresses Risk Management As an Integral Part of Project Management
- → Formulation Section Requires a Risk Management Plan to Be Developed before Approval
- → Implementation Section Defines a Risk Management/Risk Assessment Process
- → All Risks Must Be Dispositioned Before Flight

Risk Management Plan Requirements

- A Completed Risk Management Plan Is Required at the End of Formulation. It Must Include:
  - Risk Management Responsibilities, Resources, Schedules, and Milestones
  - Methodologies, Processes, and Tools to Be Used for Risk Identification, Risk Analysis, Assessment, and Mitigation
  - Criteria for Categorizing or Ranking Risks According to Probability and Consequences
  - Role of Decision-Making, Formal Reviews, and Status Reporting With Respect to Risk Management
  - Documentation Requirements for Risk Management Products and Actions

Risk Management Process



Note: Communication and documentation extend throughout all of the functions.

Brave New World - The Challenge

- Environment:
  - Shrinking NASA Budget
  - Many Fast Track and Fixed Price Projects - Better, Faster Cheaper
  - Small Budgets for S/C, Short Development Cycle
  - Limited Test Dollars

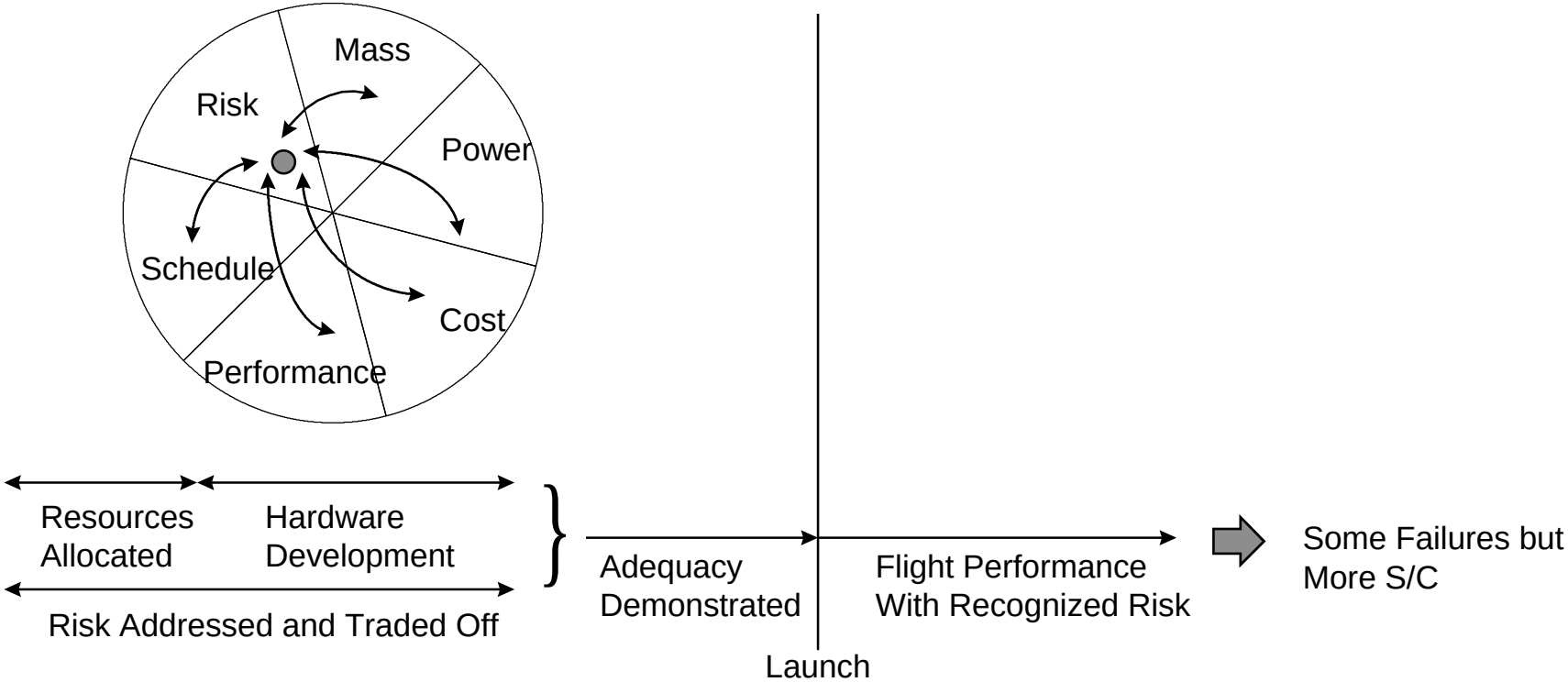
- Solution:
  - Robust Risk Management Processes are Essential
  - A Change from Rule-Based to Knowledge-Based Decision Processes is Needed

Risk As A Resource

Risk as a Resource

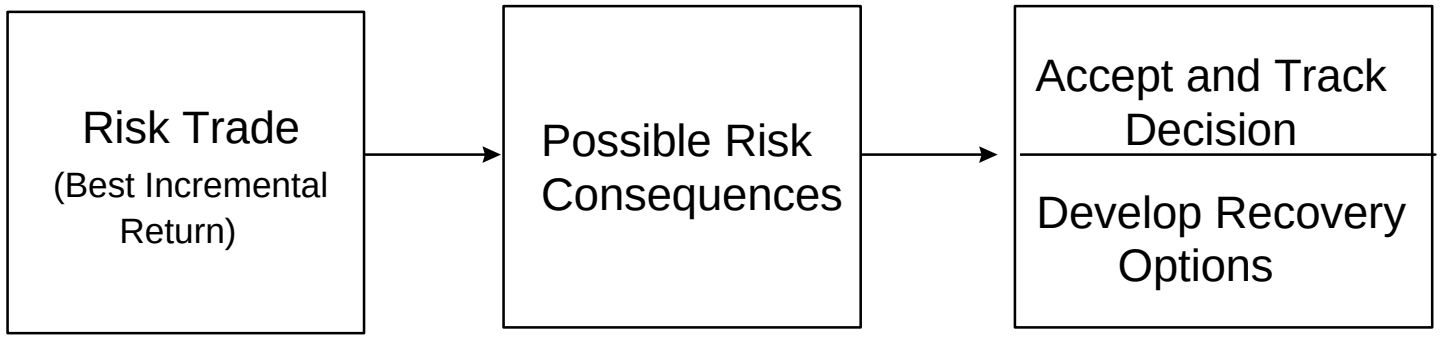
A New Paradigm → Risk to Be Identified and Thoughtfully Traded as a Resource with an Appropriate Level of Mitigation

Tradable Resources



Risk as a Resource Process

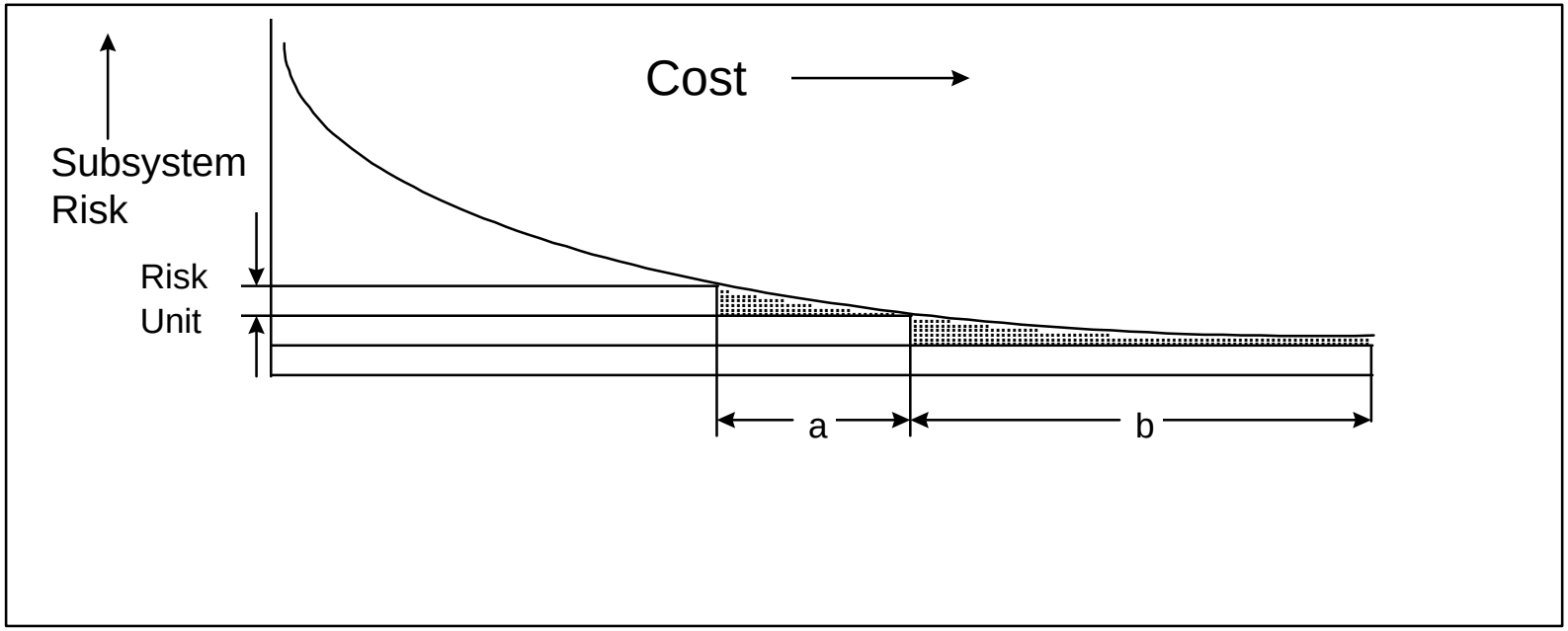
The Goal is to Optimize Overall Risk Posture through Accepting Risk in One Area to Benefit Another. A Strategy to Recover From the Occurrence of the Risk Must Also Be Considered.



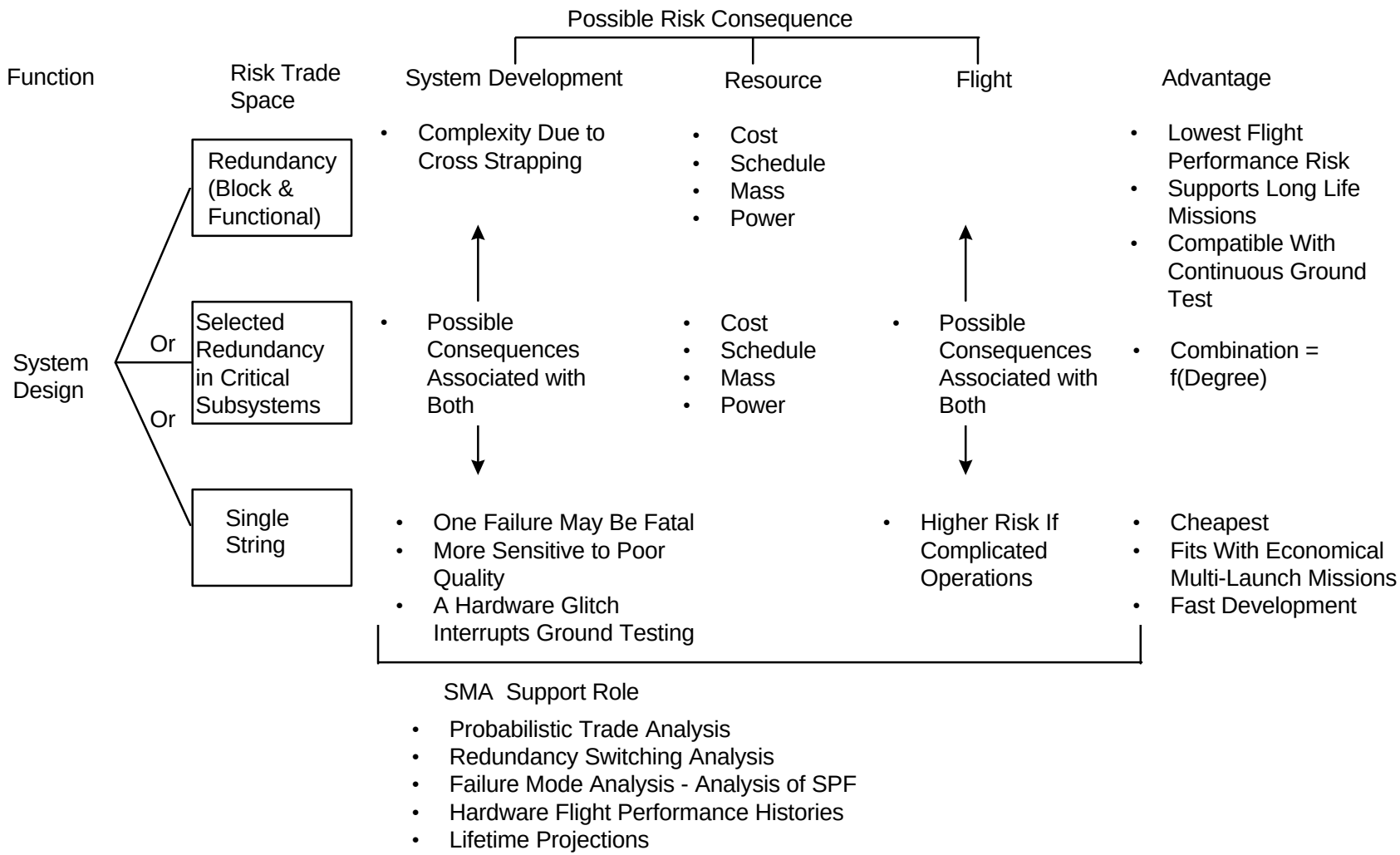
Reducing the Cost of Risk

<u>Marginal Cost of Risk</u>

→ When the Cost Per "Unit of Risk Reduction" in a Given Component or Subsystem Increases Significantly -- STOP. Buy Down Risk Somewhere Else.



Risk as a Resource
Redundancy or Single String



Risk as a Resource
Class of EEE Parts

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Advantage
EEE Parts Quality	Class "S"/ Grade 1	• Availability Poor • Higher Mass and Volume	• Cost • Schedule		• Lowest Risk • Fits Long Life Missions • More Resistant to SEE
Or					
	Class B	• No Heritage • Lot Variations Means Variable Radiation Tolerance	Many of same issues as Class "S" But with Less Flight Risk than "COTS"		• Moderate Cost • Higher Performance Expectation than "COTS"
Or					
	Commercial Off-the-Shelf (COTS)	• Quality Control at Parts Vendors • Post Procurement Screening & Burn in May Find Inadequacies	• Schedule (Test Operations)	• Performance Degradation • Incidence of "Maverick" Part	• Readily Available • Cheap • Fits Short Duration Missions with Multiple Launches

SMA Support Role

- Procurement Specifications
- Vendor Qualification
- Upgrading Process Definition
- Parts Testing Program
- Residual Parts Risk Assessment

Risk as a Resource
Design Validation

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Advantage
Dynamic Response	Analysis & Test	• Conflict Resolution Between Analysis & Test Results	• Cost • Schedule		• Most Reliable Design
Or	Analysis Only	• Adequacy Not Demonstrated	• Mass	• Considerable Performance Risk	• No Prelaunch Hardware Degradation
Or	Test Only	• Later Problem Discovery • Rework	• Mass • Cost/Schedule if Design Poor		• Simple (Design to Pass Test) • Cheap & Fast

SMA Support Role

- Test Requirement Definition
- Analysis Verification
- Test Oversight
- Residual Risk Assessment

Risk as a Resource - Component Level Validation (e.g., EMI)

Function	Risk Trade Space	Possible Risk Consequence: System Development	Possible Risk Consequence: Resource	Possible Risk Consequence: Flight	Advantage
EMI Validation Testing	Unit & Systems Testing		• Cost • Schedule		• Early and Thorough Problem Resolution • Lowest Flight Risk
Or	System Testing Only	• Rework Late in Schedule • Constrained Solutions - Mostly Shielding	• Mass		• Lowest Cost • Most Efficient Schedule

SMA Support Role

- Requirement Establishment
- Mitigation Strategy Development
- Problem/Corrective Action Assessment
- Definition of Residual Risk

Risk as a Resource
Software Verification & Validation

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Advantage
Software Verification and Validation	Test Only	• Unsure of proper corrective action • Requirements and design rework		• Considerable performance risk • Maintenance difficulties	• Cheap and fast
Or	Embedded V&V	• Same erroneous assumptions possible • Identified risks may be ignored	• Cost		• Added confidence • Early identification of issues
Or	Independent V&V	• Conflict resolution between developers and reviewers • Learning curve impact	· Longer time for requirements and design		• Most accurate identification of issues • Highest confidence • Best understanding of software response

SMA Support Role

- Test Requirement Definition
- Level and Scope
- Test Oversight of IV&V

Risk as a Resource
Technology Utilization

Possible Risk Consequence

Function	Risk Trade Space	System Development	Resource	Flight	Advantage
Technology Utilization	Advanced Technology*	• Technology Readiness Uncertainty • Greater (Imbedded) Functional Complexity • Interface Uncertainty	• Development Costs • Possible Redesigns Late in Lifecycle • Backup Design Cost • Technology Readiness Schedule • Qualification Cost	• Unknown Failures • Untried Recovery	• Quantum Performance to Resource Improvement • Less Hardware and Less Integration Complexity
	Or				
	Existing Technology**	• Constraints on Other Subsystems • Resource Compromise May Induce Failures • Heritage Traps	• Mass • Power	• Work Around Complexity	• Qualified and Flight Proven; Heritage • Availability • Confidence in Established Reliability

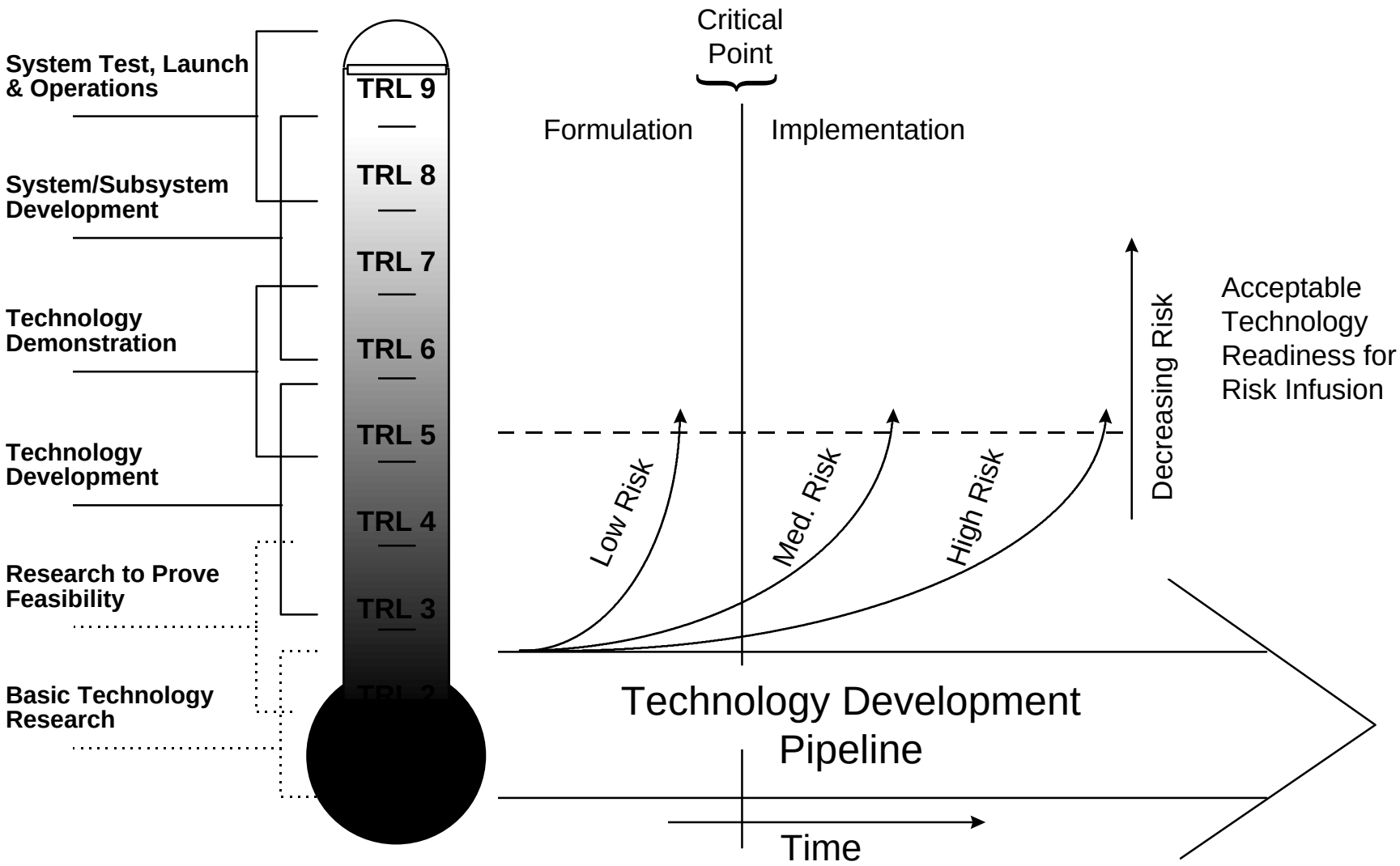
* Greater Success Risk for Significant Resource Advantage

** Greater Resource Demand for More Confidence in Reliability

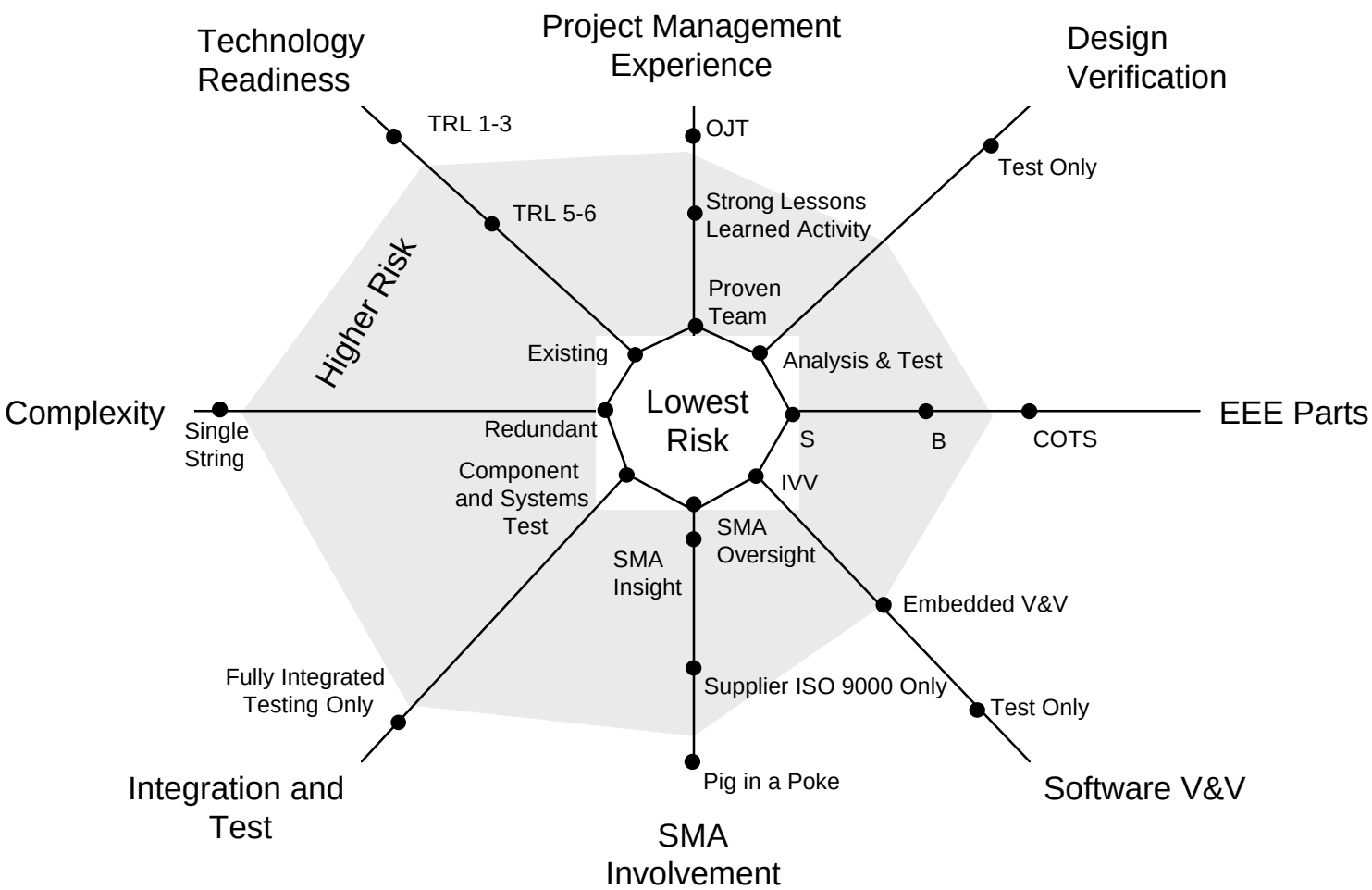
SMA Support Role

- Technology Readiness Assessment
- Reliability Estimates
- Co-participation in Qualification Plans
- Risk Assessments Support

Technology Infusion Risk

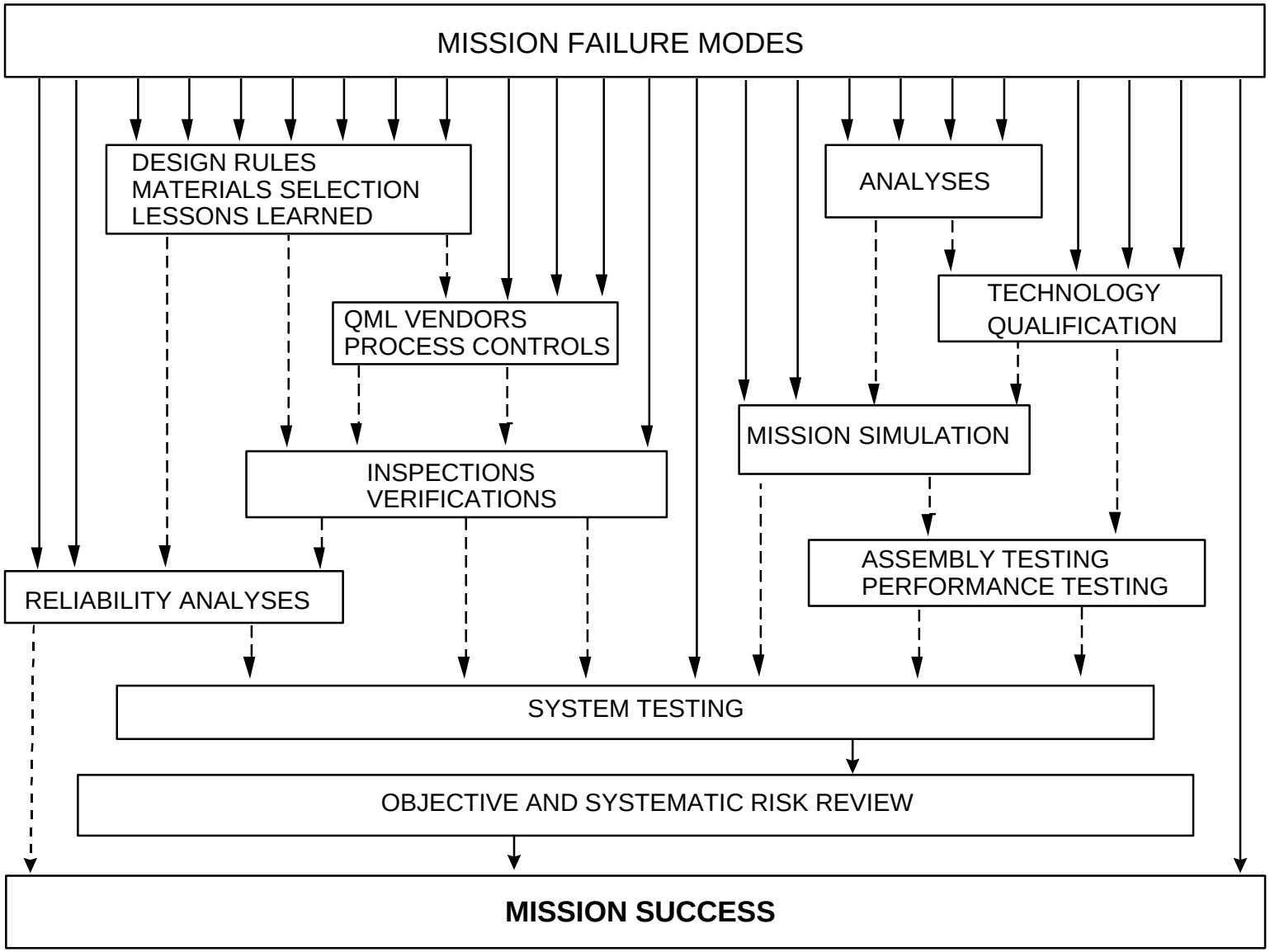


Risk Surface (Notional)



Overall Program Risk Need Not Increase

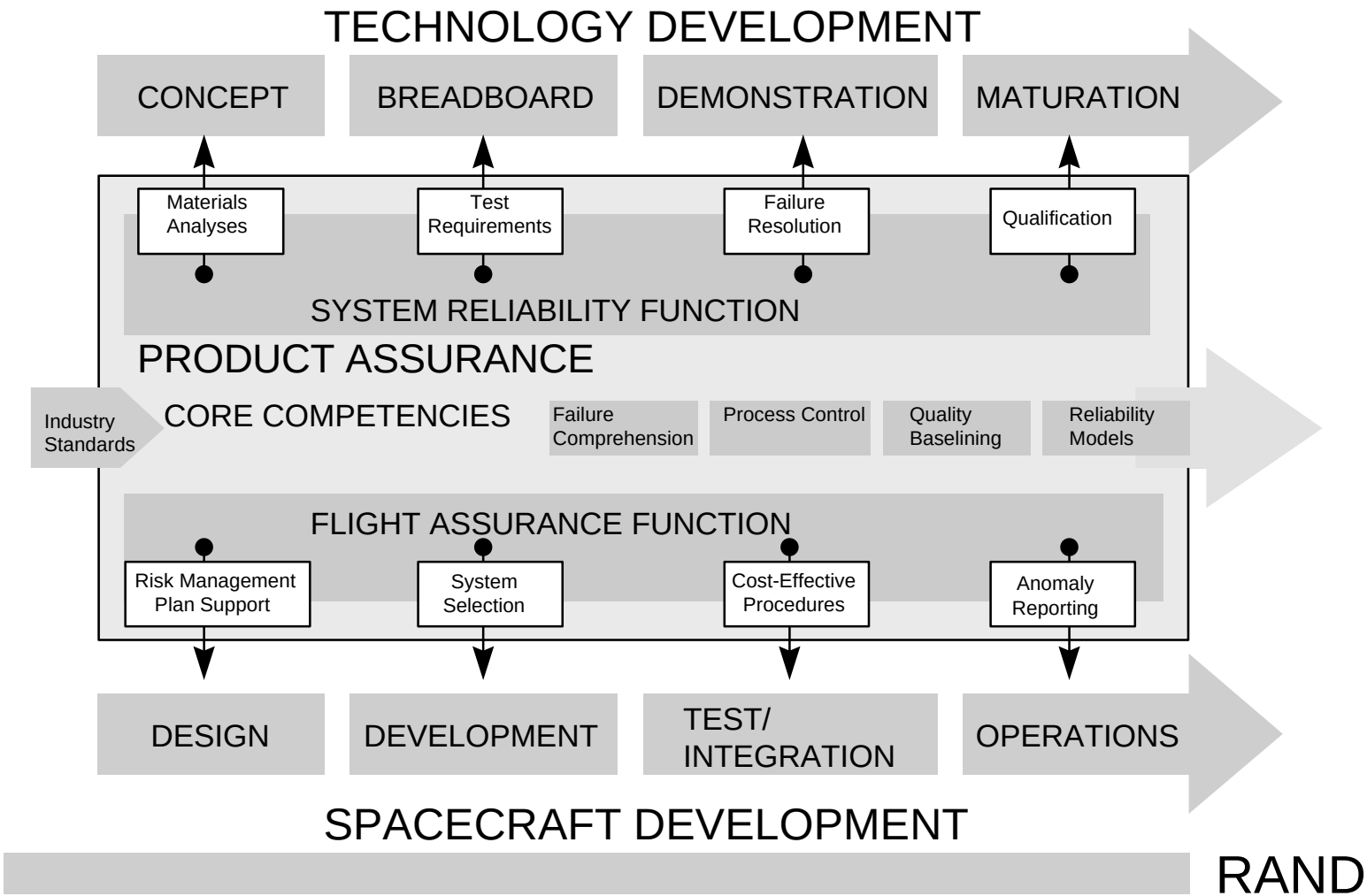
- Reliability is Approximately the Same Between Flagship Spacecraft and BFC Spacecraft but for Different Reasons
  - Complexity
    - Large Complex S/C Have More Money Available for Risk Avoidance But More Can Go Wrong
    - Simplier BFC S/C Allow for Better System Comprehension and More Informed Risk Trades
  - Development Time
    - Long Development Times Make Team Continuity Difficult. The Reasons for Previous Decisions May Be Lost
    - Short Development Times Can Keep the Team Together
  - Team Size
    - Large Teams Have Complex Communication Systems to Track and Trade Risks
    - Small Teams Have Easy Communication and Closer Technical Interaction
- Better, Faster, Cheaper Need NOT Be Dumber
  - Sound Project Management Techniques Must be Maintained


MISSION FAILURE MODES
DESIGN RULES
MATERIALS SELECTION
LESSONS LEARNED
ANALYSES
TECHNOLOGY
QUALIFICATION
QML VENDORS
PROCESS CONTROLS
MISSION SIMULATION
INSPECTIONS
VERIFICATIONS
ASSEMBLY TESTING
PERFORMANCE TESTING
RELIABILITY ANALYSES
SYSTEM TESTING
OBJECTIVE AND SYSTEMATIC RISK REVIEW
MISSION SUCCESS

SMA Role in Risk Management

- → SMA Has the Core Competencies to Serve as a Risk Management Consultant to the Project
  - → Support Risk Management Plan Development
  - → Provide Projects with Risk/Resource Trade-Offs: Strategies, Consequences, Benefits, Mitigation Approaches
- → Interact in All Phases of the Project Decision Process -- Planning, Design, Development, Operations
- → Provide Projects with Residual Risk Assessment During Project Lifecycle

A New Role for Product Assurance



RAND

Critical Technology Institute

SMA Role In Risk Management

SMA Area	Typical Areas Involved With Tradeoffs
QA	Documentation, Surveillance, Inspections, Certifications, Audits, MRB
Configuration Control	Drawings, Equipment Lists, Delivery Schedules, Approval Authority, Freeze Control, As Built Documentation
Environmental Requirements	Design Requirements, Test Requirements, Documentation, Approvals, Functional Test, Environmental Test , Programmatics (Component, Subsystem, System), Analysis
EEE Parts	Parts Lists, Policy, Part Class, Non-Standard Parts, Traceability, Derating, Failure Analysis, Burn-in, Selection, Acquisition, Upgrades, Lot Control, Screening, Destructive Physical Analysis, Vendor Control

Space Shuttle Program Surveillance Process **(as defined in SFOC contract)**

- Oversight Definition
  - Method of providing product assurance through direct participation in the process and is characterized by a flexibility in product definition based upon the direct tasking by the customer. Documented processes are used as guidance and are subject to customer “tailoring” in the course of executing the process. Expectations under this definition would focus on how well the contractor executed the customer’s technical direction.
- Insight Definition
  - Method of providing product assurance through direct measurements of end products or processes. Specifically defined and measurable requirements are utilized in defining the acceptability of the product or service to be delivered. Well documented processes are utilized and specific measurements of control are of focus.

SMA Role in Risk Management

SMA Area	Typical Areas Involved With Tradeoffs
Reliability	Single Failure Point Policy, Problem/Failure Reporting and Disposition, Design Performance Analysis (FMECA, FTA, Part Stress, Redundancy Switching, Worst Case, SEE), Reviews, Redundancy
Systems Safety	Documentation, Hazard Identification, Impact Analysis (FTA, Hazard, FMECA, Sneak Circuit), Structures/Materials Reviews, ESD Control, Tests, Inspections, Surveys
Software Product Assurance	Initiation, Problem/Failure Reporting and Disposition, Simulations, Criticality Analysis IVV, Tests

Summary

- → A Structured Risk Management Approach Is Critical to A Successful Project--This Is Nothing New
- → Risk Policy Must Be An Integral Part of the Program As Part of a Concurrent Engineering Process; Risk and Risk Drivers Must Be Monitored Throughout the Program
- → Risk May Also Be Managed As A Resource; the New Way of Managing Better, Faster, Cheaper Programs Encompasses Up-Front, Knowledge-Based Risk Assessment
- → S&MA Community Can Provide Valuable Support as Risk Management Consultants