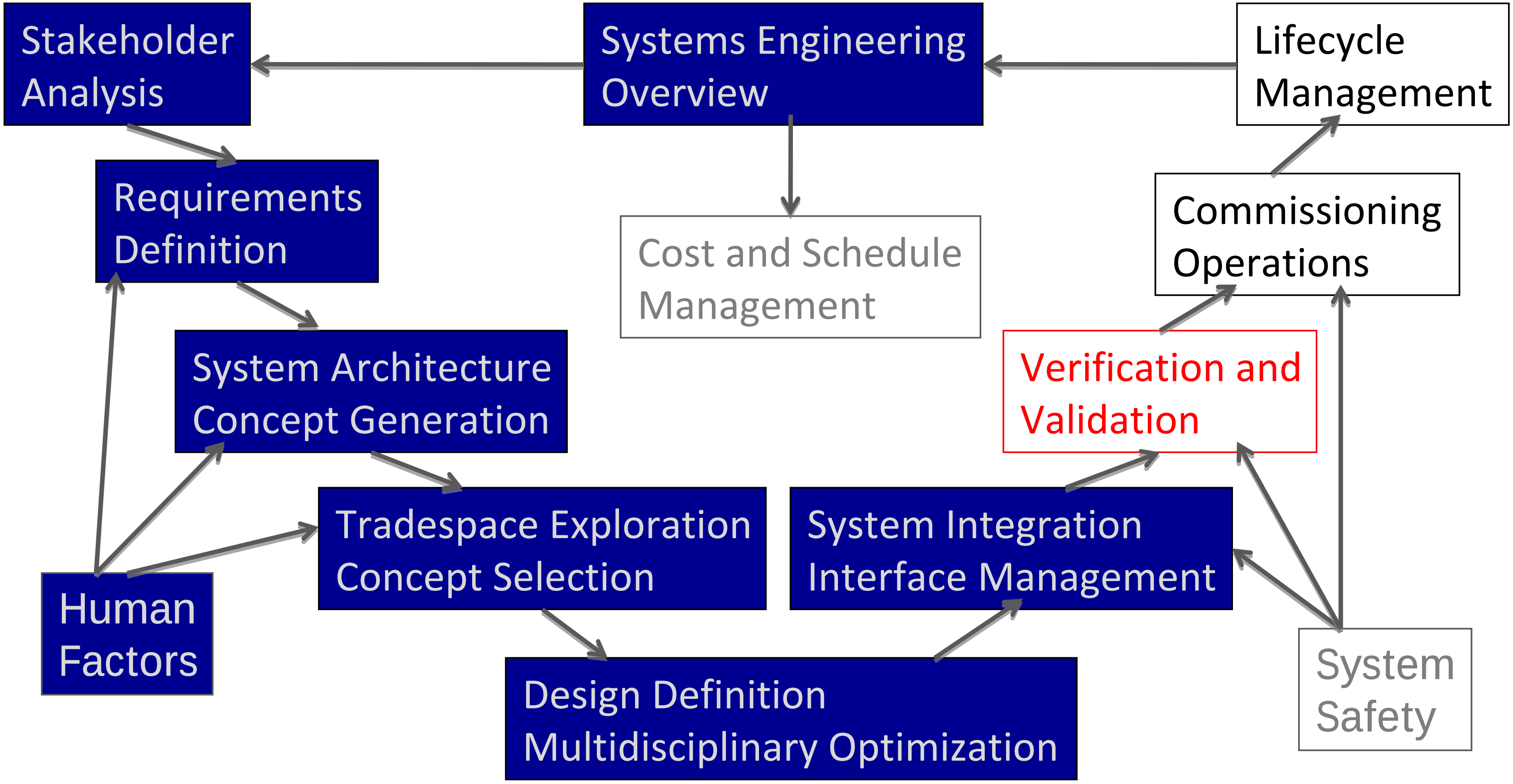
16.842 Fundamentals of Systems Engineering

Lecture 9 – Verification and Validation

Prof. Olivier de Weck

V-Model – Nov. 6, 2009



Outline

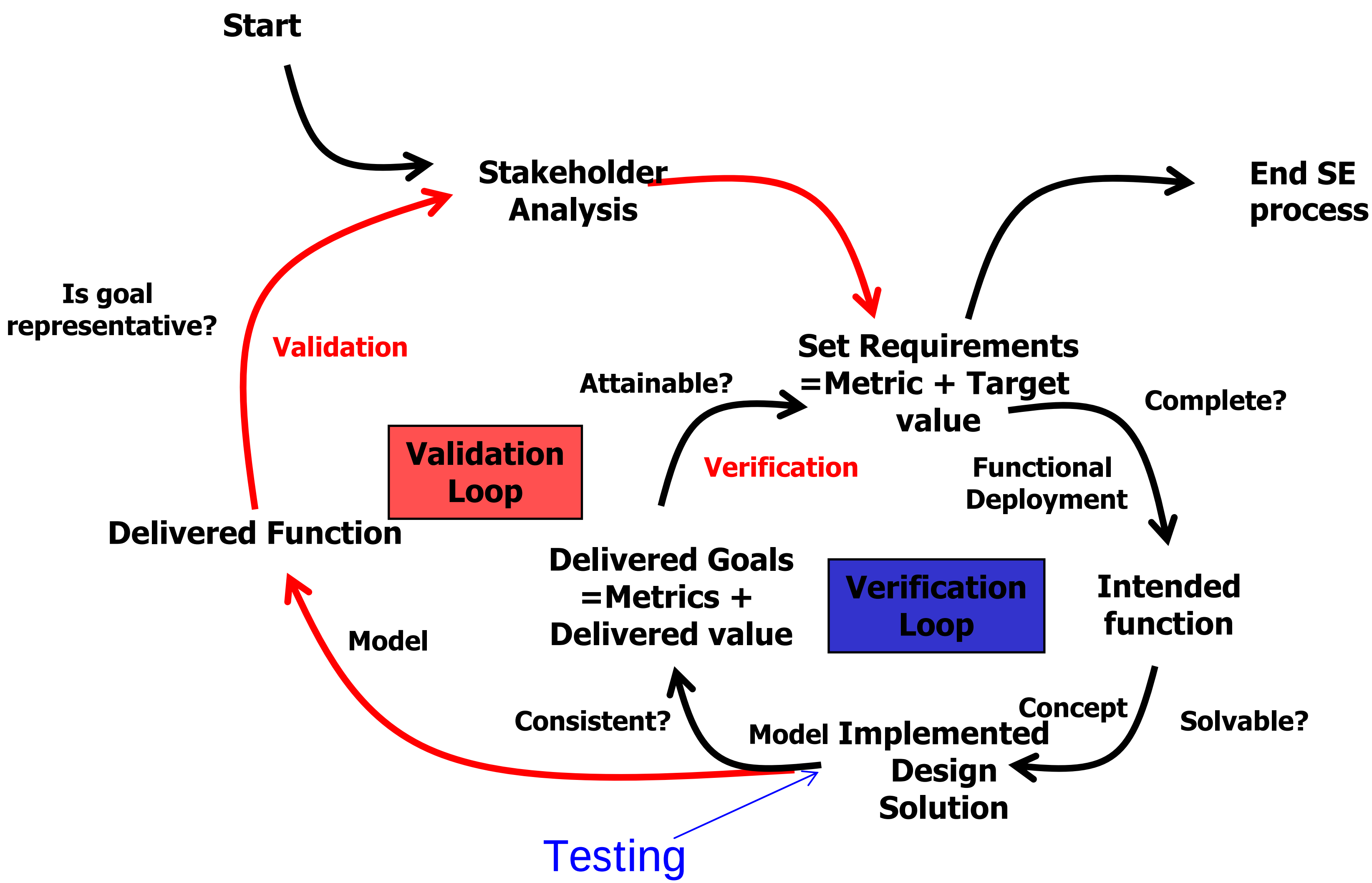
- Verification and Validation
  - What is their role?
  - Position in the lifecycle
- Testing
  - Aircraft flight testing (experimental vs. certification)
  - Spacecraft testing (“shake and bake”)
  - Caveats
- Technical Risk Management
  - Risk Matrix
  - Iron Triangle in Projects: Cost, Schedule, Scope > Risk
    - Lead-in to Faster-Better-Cheaper case study

Readings for Today

- NASA/SP-2007-6105
  - Section 5.3 (pp. 83-97)
  - Section 5.4 (pp. 98-105)
  - Appendix E (p. 284)
  - Appendix I (p. 301)

- HBS Case: 9-603-083 Mission to Mars (A)

Verification and Validation



Differences between V & V

Differences Between Verification and Validation Testing

Verification Testing

Verification testing relates back to the approved requirements set (such as an SRD) and can be performed at different stages in the product life cycle. Verification testing includes: (1) any testing used to assist in the development and maturation of products, product elements, or manufacturing or support processes; and/or (2) any engineering-type test used to verify the status of technical progress, verify that design risks are minimized, substantiate achievement of contract technical performance, and certify readiness for initial validation testing. Verification tests use instrumentation and measurements and are generally accomplished by engineers, technicians, or operator-maintainer test personnel in a controlled environment to facilitate failure analysis.

Validation Testing

Validation relates back to the ConOps document. Validation testing is conducted under realistic conditions (or simulated conditions) on any end product to determine the effectiveness and suitability of the product for use in mission operations by typical users and to evaluate the results of such tests. Testing is the detailed quantifying method of both verification and validation. However, testing is required to validate final end products to be produced and deployed.

Verification *Was the end product realized right?*

- During development
- Check if requirements are met
- Typically in the laboratory
- Component/subsystem centric

Validation *Was the right end product realized?*

- During or after integration
- Typically in real or simulated mission environment
- Check if stakeholder intent is met
- Full-up system

Product Verification Process

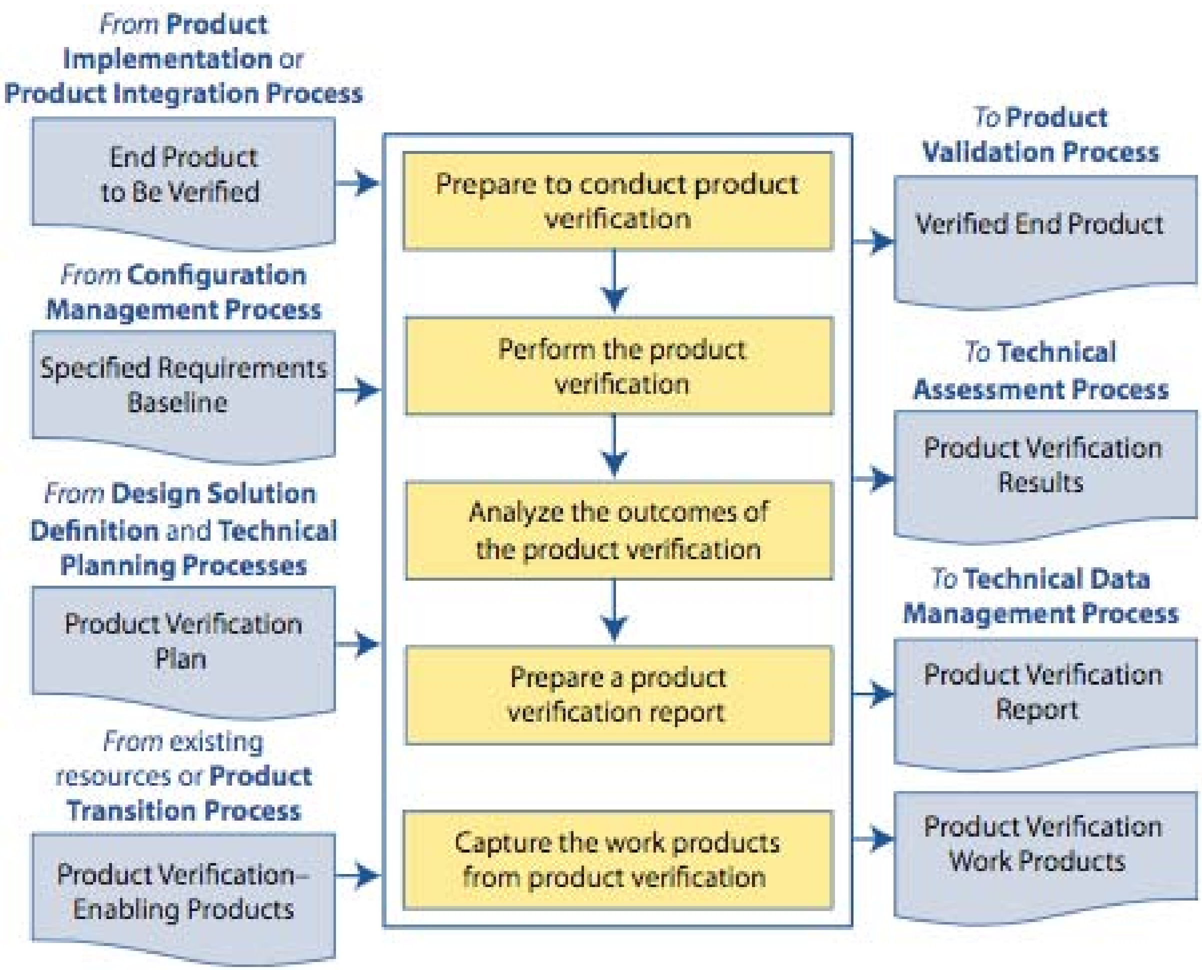


Figure 5.3-1 Product Verification Process

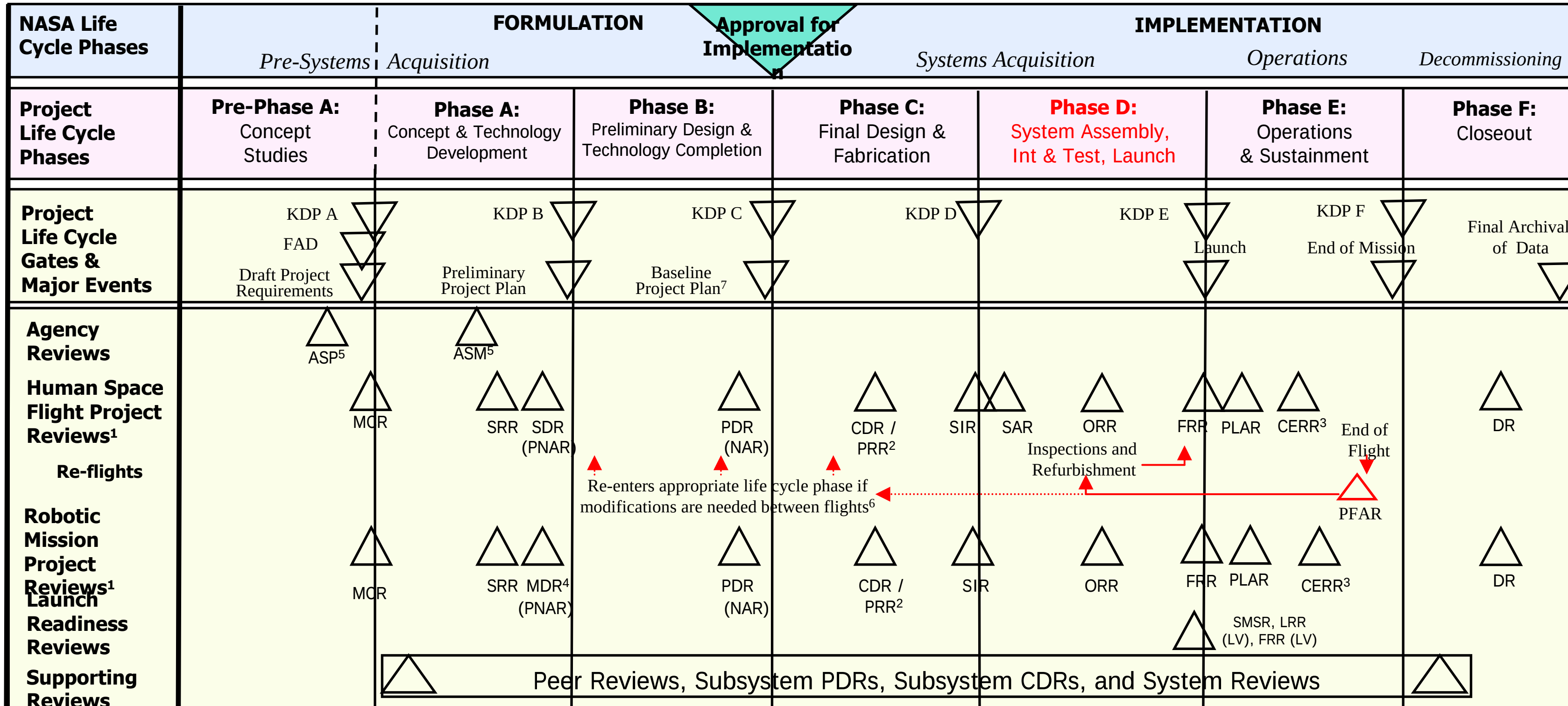
Types of verification

- -Analysis
- -Demonstration
- -Inspection
- -Test

Outputs:

- -Discrepancy reports
- -Verified product
- -Compliance documentation

NASA Life-Cycle Phases



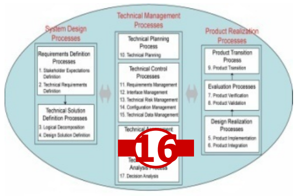
FOOTNOTES

1. Flexibility is allowed in the timing, number, and content of reviews as long as the equivalent information is provided at each KDP and the approach is fully documented in the Project Plan. These reviews are conducted by the project for the independent SRB. See Section 2.5 and Table 2-6.
2. PRR needed for multiple (≥4) system copies. Timing is notional.
3. CERRs are established at the discretion of Program Offices.
4. For robotic missions, the SRR and the MDR may be combined.
5. The ASP and ASM are Agency reviews, not life-cycle reviews.
6. Includes recertification, as required.
7. Project Plans are baselined at KDP C and are reviewed and updated as required, to ensure project content, cost, and budget remain consistent.

ACRONYMS

ASP—Acquisition Strategy Planning Meeting
ASM—Acquisition Strategy Meeting
CDR—Critical Design Review
CERR—Critical Events Readiness Review
DR—Decommissioning Review
FAD—Formulation Authorization Document
FRR—Flight Readiness Review
KDP—Key Decision Point
LRR—Launch Readiness Review
MCR—Mission Concept Review
MDR—Mission Definition Review
NAR—Non-Advocate Review
ORR—Operational Readiness Review
PDR—Preliminary Design Review
PFAR—Post-Flight Assessment Review
PLAR—Post-Launch Assessment Review
PNAR—Preliminary Non-Advocate Review
PRR—Production Readiness Review
SAR—System Acceptance Review
SDR—System Definition Review
SIR—System Integration Review
SMSR—Safety and Mission Success Review
SRR—System Requirements Review

Listing of NASA Life-Cycle Reviews



Review	Title	Purpose
P/SRR	Program Requirement Review	The P/SRR is used to ensure that the program requirements are properly formulated and correlated with the Agency and mission directorate strategic objectives
P/SDR	Program Definition Review, or System Definition Review	The P/SDR ensures the readiness of the program for making a program commitment agreement to approve project formulation startups during program Implementation phase.
MCR	Mission Concept Review	The MCR affirms the mission need and examines the proposed mission's objectives and the concept for meeting those objectives
SRR	System Requirement Review	The SRR examines the functional and performance requirements defined for the system and the preliminary program or project plan and ensures that the requirements and the selected concept will satisfy the mission
MDR	Mission Definition Review	The MDR examines the proposed requirements, the mission architecture, and the flow down to all functional elements of the mission to ensure that the overall concept is complete, feasible, and consistent with available resources
SDR	System Definition Review	The SDR examines the proposed system architecture and design and the flow down to all functional elements of the system.
PDR	Preliminary Design Review	The PDR demonstrates that the preliminary design meets all system requirements with acceptable risk and within the cost and schedule constraints and establishes the basis for proceeding with detailed design. It will show that the correct design options have been selected, interfaces have been identified, and verification methods have been described
CDR	Critical Design review	The CDR demonstrates that the maturity of the design is appropriate to support proceeding with full-scale fabrication, assembly, integration, and test. CDR determines that the technical effort is on track to complete the flight and ground system development and mission operations, meeting mission performance requirements within the identified cost and schedule constraints.
PRR	Production Readiness Review	A PRR is held for FS&GS projects developing or acquiring multiple or similar systems greater than three or as determined by the project. The PRR determines the readiness of the system developers to efficiently produce the required number of systems. It ensures that the production plans; fabrication, assembly, and integration enabling products; and personnel are in place and ready to begin production.

NPR 7123.1A, Chapter 3. & Appendix C.3.7. SP-2007-6105, Section 6.7

Listing of NASA Life-Cycle Reviews (Continued)

Review	Title	Purpose
SIR	System Integration Review	An SIR ensures that the system is ready to be integrated. Segments, components, and subsystems are available and ready to be integrated into the system. Integration facilities, support personnel, and integration plans and procedures are ready for integration.
TRR	Test Readiness Review	A TRR ensures that the test article (hardware/software), test facility, support personnel, and test procedures are ready for testing and data acquisition, reduction, and control.
SAR	System Acceptance Review	The SAR verifies the completeness of the specific end products in relation to their expected maturity level and assesses compliance to stakeholder expectations. The SAR examines the system, its end products and documentation, and test data and analyses that support verification. It also ensures that the system has sufficient technical maturity to authorize its shipment to the designated operational facility or launch site.
ORR	Operational Readiness Review	The ORR examines the actual system characteristics and the procedures used in the system or end product's operation and ensures that all system and support (flight and ground) hardware, software, personnel, procedures, and user documentation accurately reflect the deployed state of the system.
FRR	Flight Readiness Review	The FRR examines tests, demonstrations, analyses, and audits that determine the system's readiness for a safe and successful flight or launch and for subsequent flight operations. It also ensures that all flight and ground hardware, software, personnel, and procedures are operationally ready.
PLAR	Post-Launch Assessment Review	A PLAR is a post-deployment evaluation of the readiness of the spacecraft systems to proceed with full, routine operations. The review evaluates the status, performance, and capabilities of the project evident from the flight operations experience since launch. This can also mean assessing readiness to transfer responsibility from the development organization to the operations organization. The review also evaluates the status of the project plans and the capability to conduct the mission with emphasis on near-term operations and mission-critical events. This review is typically held after the early flight operations and initial checkout.
CERR	Critical Event Readiness Review	A CERR confirms the project's readiness to execute the mission's critical activities during flight operation.
PFAR	Post-Flight Assessment Review	The PFAR evaluates the activities from the flight after recovery. The review identifies all anomalies that occurred during the flight and mission and determines the actions necessary to mitigate or resolve the anomalies for future flights.
DR	Decommissioning Review	A DR confirms the decision to terminate or decommission the system and assesses the readiness of the system for the safe decommissioning and disposal of system assets.

NPR 7123.1A, Chapter 3. & Appendix C.3.7. SP-2007-6105, Section 6.7

Types of Testing

Types of Testing

There are many different types of testing that can be used in verification of an end product. These examples are provided for consideration:

- Aerodynamic
- Burn-in
- Drop
- Environmental
- High-/Low-Voltage Limits
- Leak Rates
- Nominal
- Parametric
- Pressure Limits
- Security Checks
- Thermal Limits
- Acceptance
- Characterization
- Electromagnetic Compatibility
- G-loading
- Human Factors Engineering/Human-in-the-Loop Testing
- Lifetime/Cycling
- Off-Nominal
- Performance
- Qualification Flow
- System
- Thermal Vacuum
- Acoustic
- Component
- Electromagnetic Interference
- Go or No-Go
- Integration
- Manufacturing/Random Defects
- Operational
- Pressure Cycling
- Structural Functional
- Thermal Cycling
- Vibration

Source: NASA SE Handbook, Section 5.3 Product Verification

Aircraft Testing

- Ground Testing
  - Weights and Balance (determine mass, CG ...)
  - Engine Testing (in “hush house”, outdoors)
  - Fatigue Testing (static and dynamic structural)
  - Avionics checkout
  - Pre-flight Testing (extended checklist)
- Flight Testing
  - Flight Performance Testing (rate of climb, range ...)
  - Stability and Controls (stall speed, trim, flutter ...)
  - Weapons testing (live fire tests, LO ..)

F/A-18 Wind Tunnel Testing

This photograph of a scale model of an F/A-18 has been removed due to copyright restrictions

$500k , 1:10 scale

F/A-18C Hush House Testing (ca. 1995)

This photograph of an F/A-18 in a testing chamber has been removed due to copyright restrictions

Live Testing

This photograph of an F/A-18 flying in air has been removed due to copyright restrictions

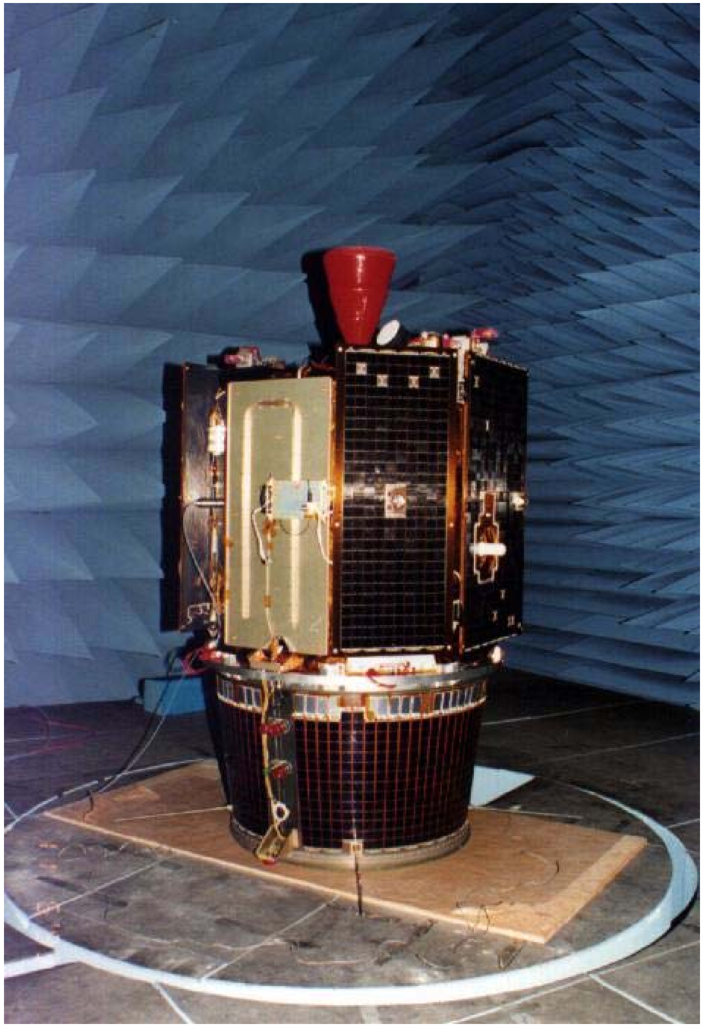
Spacecraft Testing

- Ground Testing
  - Weights and Balance
  - Antenna/Communications (in anechoic chamber)
  - Vibration Testing (“shake”)
  - Thermal and Vacuum chamber testing (“bake”)
  - Pre-launch testing (off pad, on pad)
- On-orbit Testing
  - Thruster testing (for station keeping)
  - Deployment of all mechanisms
  - Communications, Instruments ...

Spacecraft Integration Testing (NASA)

This photograph has been removed due to copyright restrictions.

Anechoic Chamber Testing



Radio Frequency Anechoic Chamber Facility

The radio frequency anechoic chamber is used to design, manufacture, and test spacecraft antenna systems. The facility is also used for electromagnetic compatibility and electromagnetic interference testing of spacecraft antenna systems

Clementine Spacecraft

JWST – On-Orbit Deployment

This photograph has been removed due to copyright restrictions.

Testing Caveats

- Testing is critical, but expensive
  - Test rig, chamber, sensors, DAQ equipment ...
- How much testing of components?
  - Trust parts vendors or retest everything?
- Calibration of sensors and equipment
  - If sensors are not calibrated properly can lead to erroneous conclusions
- "Test as you Fly, Fly as you test"
  - To what extent do the test conditions reflect actual operational usage?
- Simulated Tests
  - Use "dummy" components if the real ones are not available
  - Simulated operations (e.g. 0g vs. 1g) ... are they representative?
- Failures often occur outside any test scenarios

Appendix E: Validation Matrix

Table E-1 Validation Requirements Matrix

Validation Product #	Activity	Objective	Validation Method	Facility or Lab	Phase	Performing Organization	Results
Unique identifier for validation product	Describe evaluation by the customer/sponsor that will be performed	What is to be accomplished by the customer/sponsor evaluation	Validation method for the System X requirement (analysis, inspection, demonstration, or test)	Facility or laboratory used to perform the validation	Phase in which the verification/validation will be performed[a]	Organization responsible for coordinating the validation activity	Indicate the objective evidence that validation activity occurred
1	Customer/sponsor will evaluate the candidate displays	1. Ensure legibility is acceptable 2. Ensure overall appearance is acceptable	Test	xxx	Phase A	xxx	

a. Example: (1) during product selection process, (2) prior to final product selection (if COTS) or prior to PDR, (3) prior to CDR, (4) during box-level functional, (5) during system-level functional, (6) during end-to-end functional, (7) during integrated vehicle functional, (8) during on-orbit functional.

Appendix I : V&V Plan Outline

Appendix I: Verification and Validation Plan Sample Outline

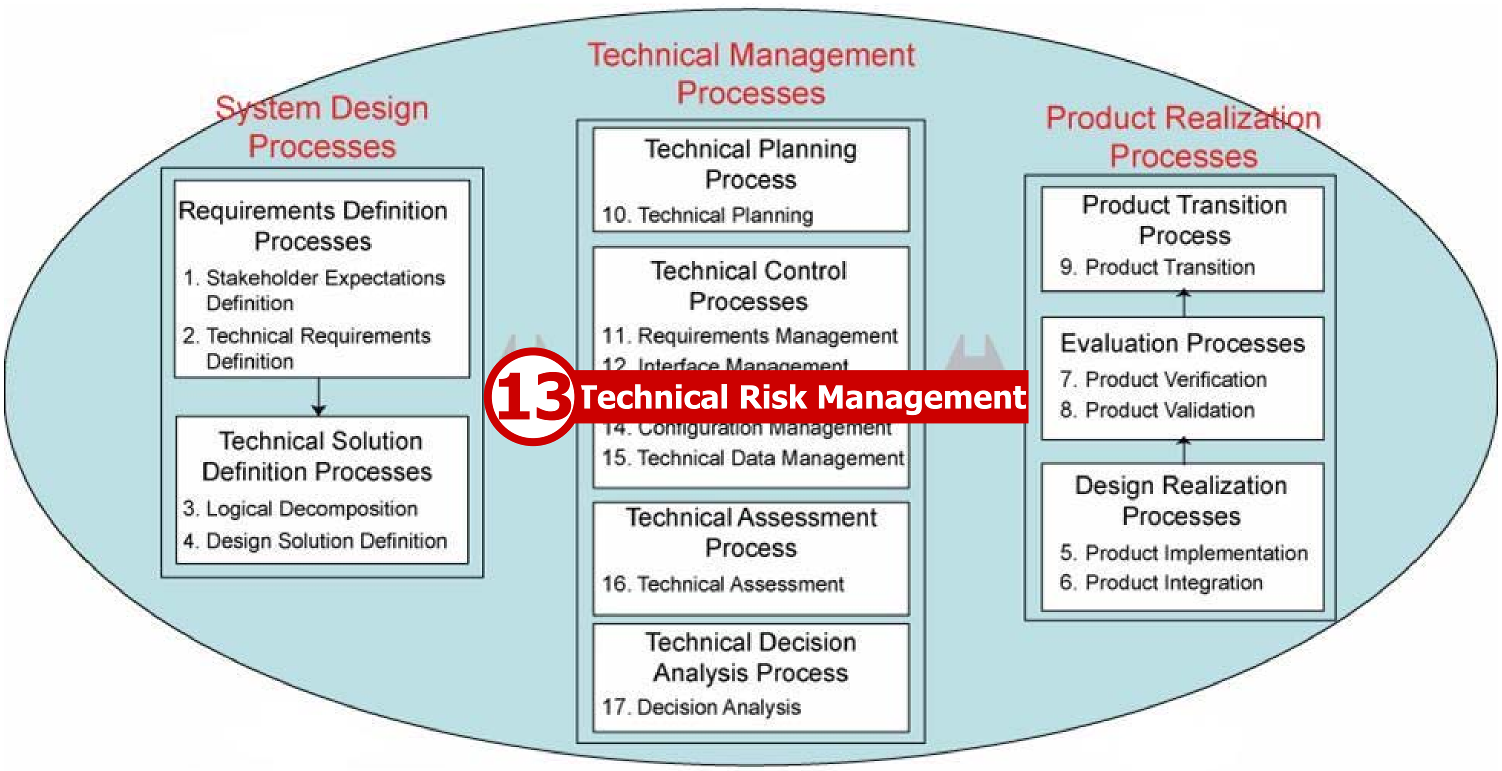
1. **Introduction**
   1.1 Purpose and Scope
   1.2 Responsibility and Change Authority
   1.3 Definitions
2. **Applicable and Reference Documents**
   2.1 Applicable Documents
   2.2 Reference Documents
   2.3 Order of Precedence
3. **System X Description**
   3.1 System X Requirements Flow Down
   3.2 System X Architecture
   3.3 End Item Architectures
      3.3.1 System X End Item A
      3.3.*n* System X End Item *n*
   3.4 System X Ground Support Equipment
   3.5 Other Architecture Descriptions
4. **Verification and Validation Process**
   4.1 Verification and Validation Management Responsibilities
   4.2 Verification Methods
      4.2.1 Analysis
      4.2.2 Inspection
      4.2.3 Demonstration
      4.2.4 Test
         4.2.4.1 Qualification Testing
         4.2.4.2 Other Testing
   4.3 Validation Methods
   4.4 Certification Process
   4.5 Acceptance Testing
5. **Verification and Validation Implementation**
   5.1 System X Design and Verification and Validation Flow
   5.2 Test Articles
   5.3 Support Equipment
   5.4 Facilities
6. **System X End Item Verification and Validation**
   6.1 End Item A
      6.1.1 Developmental/Engineering Unit Evaluations
      6.1.2 Verification Activities
         6.1.2.1 Verification Testing
            6.1.2.1.1 Qualification Testing
            6.1.2.1.2 Other Testing

The degree to which V&V is taken seriously and resources are made available is critical for project outcome:

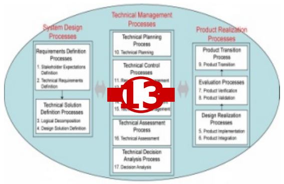
-# of dedicated QA personnel
-Interaction/working with suppliers
-Planning ahead for tests
-End-to-end functional testing
-Can often "piggy-back" on existing facilities, equipment ...
-Document outcomes well and follow-up with discrepancies

This work is often not glamorous (except for some flight testing) but critical !

Technical Risk Management

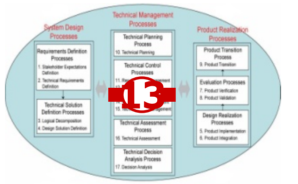


Importance of Technical Risk Management



- Risk is defined as the combination of:
  - The probability that a program or project will experience an undesired event and
  - The consequences, impact, or severity of the undesired event, were it to occur
- The undesired event might come from technical or programmatic sources (e.g. a cost overrun, schedule slippage, safety mishap, health problem, malicious activities, environmental impact, or failure to achieve a needed scientific or technological objective or success criteria)
- Technical Risk Management is an organized, systematic risk-informed decision-making discipline that proactively identifies, analyzes, plans, tracks, controls, communicates, documents, and manages risk to increase the likelihood of achieving project goals

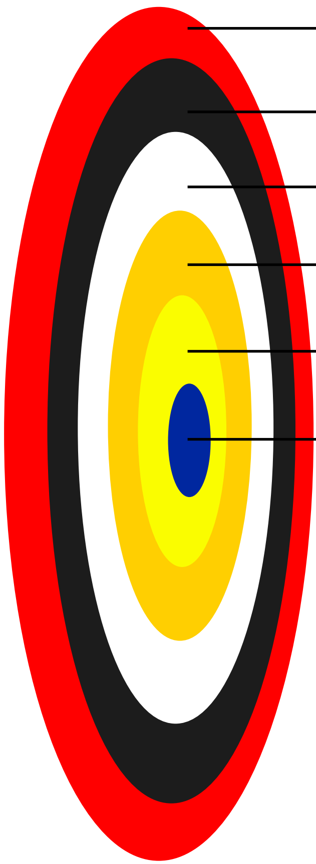
What is Risk?



- Risk is a measure of future uncertainties in achieving program technical performance goals within defined cost and schedule constraints
  - Risks can be associated with all aspects of a technical effort, e.g., threat, technology maturity, supplier capability, design maturation, performance against plan, etc., as these aspects relate within the systems structure and with interfacing products.
- Risks have three components:
  1. Future root cause
  2. Probability or likelihood of that future root cause occurring
  3. Consequences (or effect) of that future occurrence

NPR 7123.1A, Chapter 3. & Appendix C.3.4
SP-2007-6105, Section 6.4

Layers of Risk Model (e.g. for Mars Missions)



Natural Risks

- Cosmic Radiation
- Micro-Meteorites
- Uncertainty in Atmospheric Density of Mars

Market Risks

- ????
- New Science Requirements

Country/Fiscal

- Political stability
- 4 Year cycle
- Budget Priorities Human vs Robotic Space
- Working with IPs

Industry/Competitive

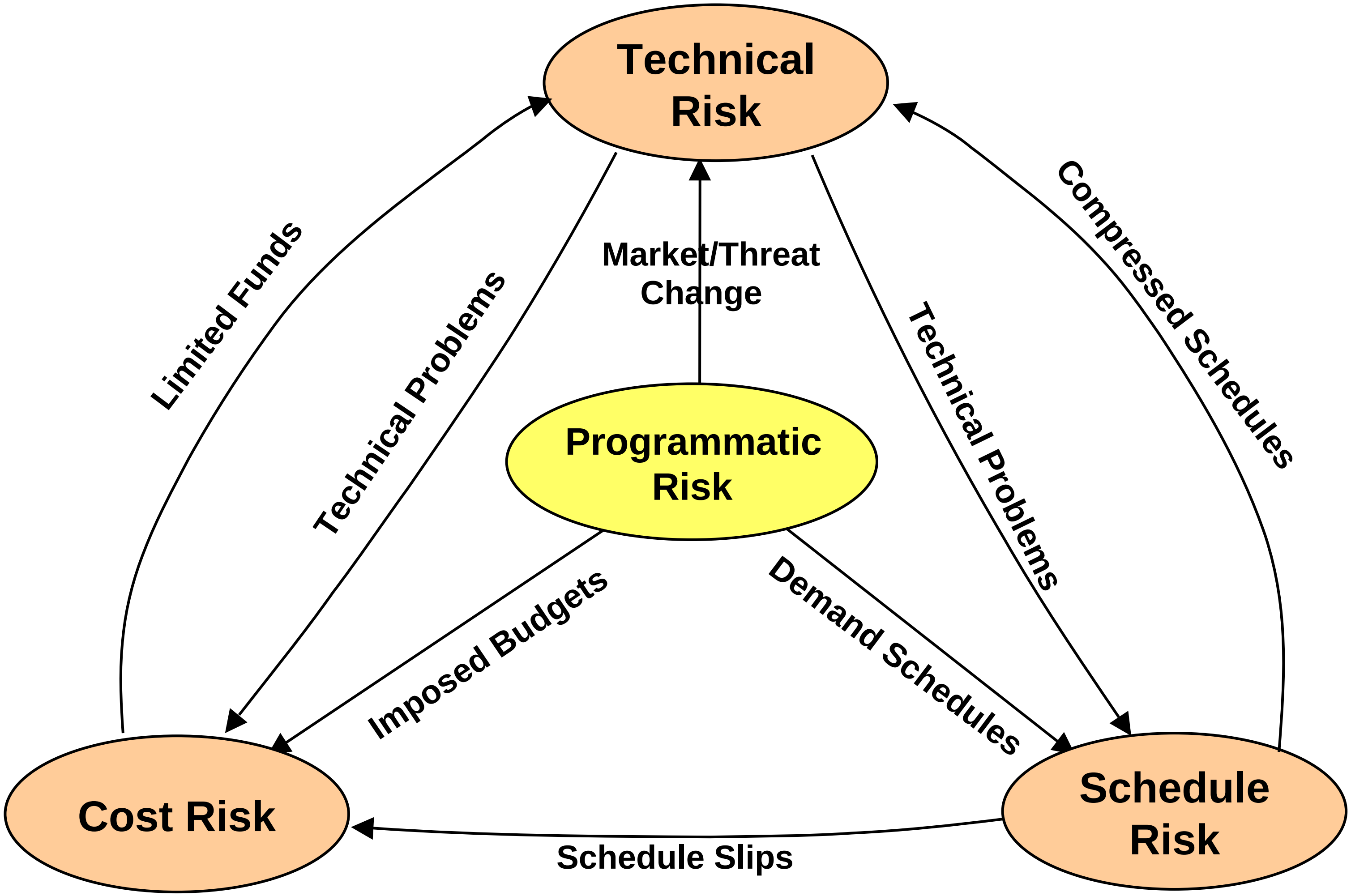
- Contractor Performance
- Budget Stability

Technical/ Project Risks

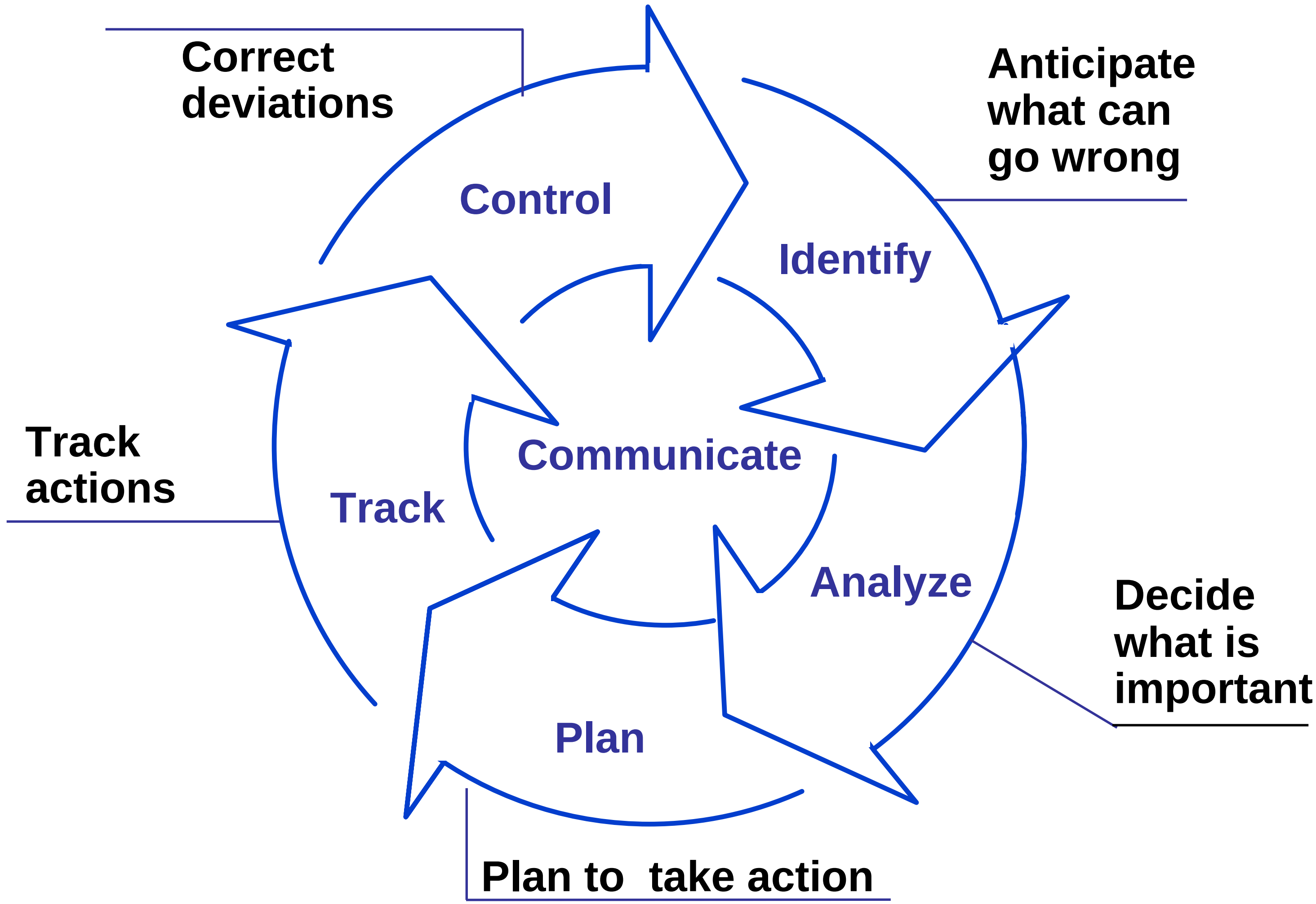
- Airbag Technology Maturity
- Rover Motor Performance
- Software Bugs

High Influence ⟷ Low Influence

Risk Categories



A Risk Management Framework



Risk ID/Assessment

- Brainstorm Risks
  - Probability that a particular event will occur
  - Impact or Consequence if the event does indeed occur
- Aggregate Into Categories
  - Rule of Thumb Limit @ N≈20
- Score (Based on Opinion & Data)
- Involve <u>All</u> Stakeholders

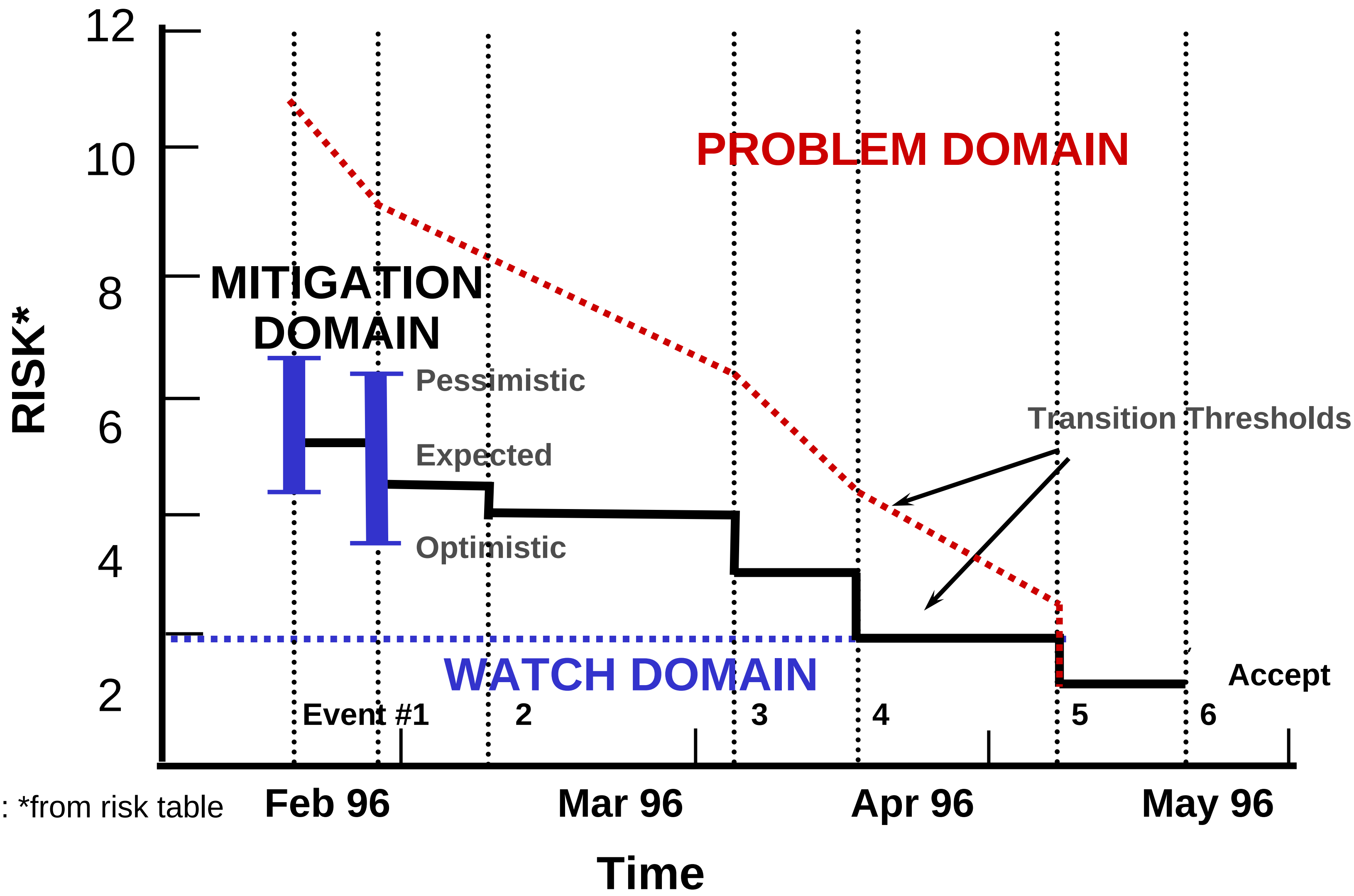
Risk Sector Plot (NASA)

Attribute: Probability		
Level	**Value**	**Criteria**
5	Near certainty	Everything points to this becoming a problem, always has
4	Very likely	High chance of this becoming a problem
3	Likely (50/50)	There is an even chance this may turn into a problem
2	Unlikely	Risk like this may turn into a problem once in awhile
1	Improbable	Not much chance this will become problem

Probability \ Impact	1	2	3	4	5
5	2	3	6	9	12
4	2	3	5	8	11
3	1	2	4	7	10
2	1	2	3	5	8
1	1	1	2	3	5

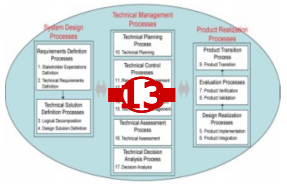
Attribute: Impact				
Level	**Value**	**Technical Criteria**	**Cost Criteria**	**Schedule Criteria**
5	Catastrophic	Can't control the vehicle OR Can't perform the mission	> $10 Million	Slip to level I milestones
4	Critical	Loss of mission, but asset recoverable in time	$ 10 M ≤ X < $ 5 Million	Slip to level II milestones
3	Moderate	Mission degraded below nominal specified	$ 5 M ≤ X < $ 1 Million	Slip to level III milestones
2	Marginal	Mission performance margins reduced	$ 1 M ≤ X < $ 100 K	Loss of more than one month schedule margin
1	Negligible	Minimum to no impact	Minimum to no impact	Minimum to no impact

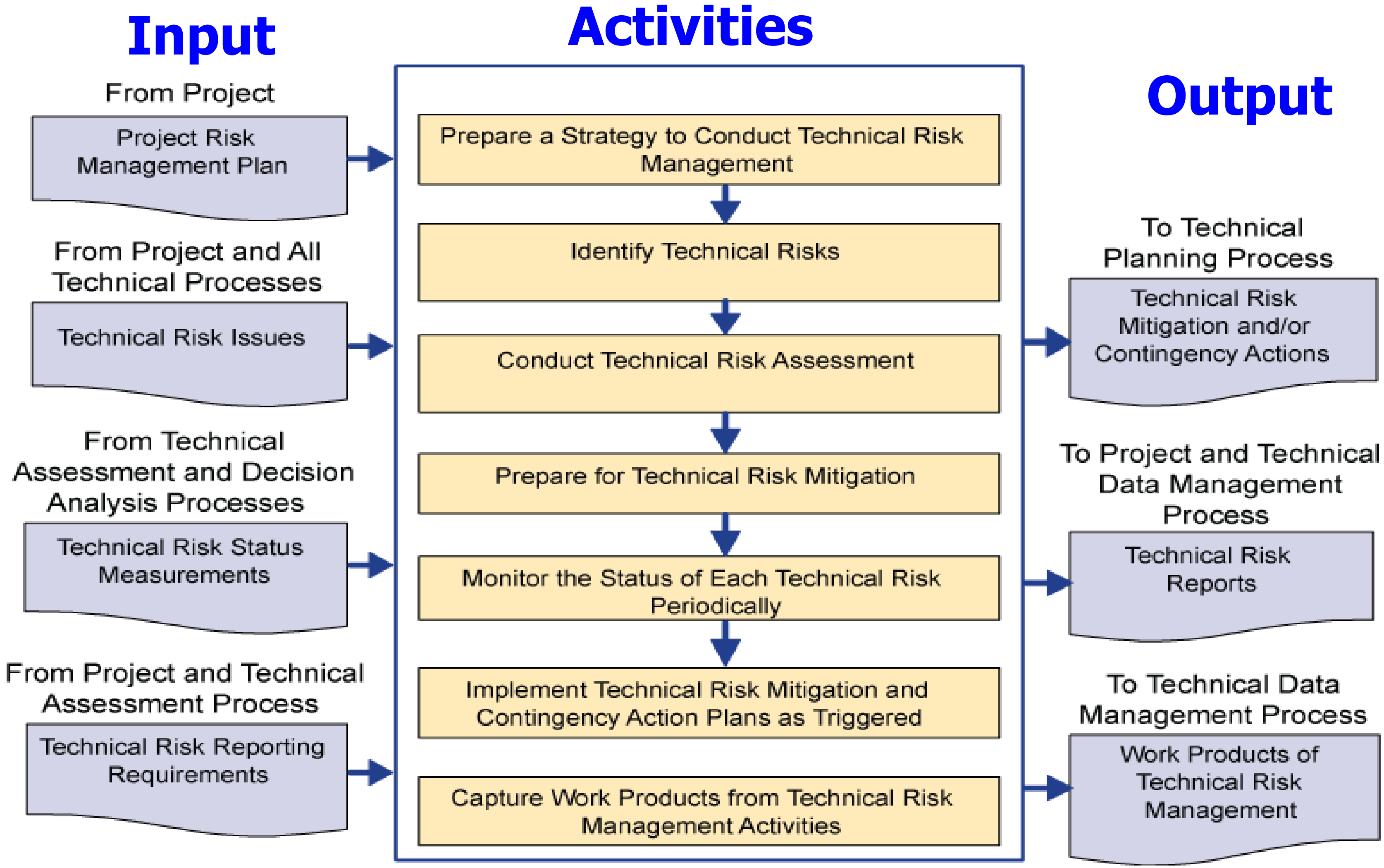
Threshold Risk Metric (NASA)



Note: *from risk table

Technical Risk Management – Best Practice Process Flow Diagram





Summary

- Verification and Validation are critical
  - Verification makes sure the product is built to spec
  - Validation assesses whether the spec is really what the customer wants
- Testing
  - Critical to project outcome, different types ....
  - Fundamentally a Q&A activity
  - Expensive, need to be done right
- Risk Management
  - Risk Matrix, Risk Identification, Mitigation
  - Tensions between cost, scope, schedule, risk

16.842 Fundamentals of Systems Engineering
Fall 2009