Fundamentals of Systems Engineering

Session 9
Verification and Validation
## General Status Update

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Topic</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 (group)</td>
<td>Team Formation, Definitions, Stakeholders, Concept of Operations (CONOPS)</td>
<td>12.5%</td>
</tr>
<tr>
<td>A2 (group)</td>
<td>Requirements Definition and Analysis</td>
<td>12.5%</td>
</tr>
<tr>
<td></td>
<td>Margins Allocation</td>
<td></td>
</tr>
<tr>
<td>A3 (group)</td>
<td>System Architecture, Concept Generation</td>
<td>12.5%</td>
</tr>
<tr>
<td>A4 (group)</td>
<td>Tradespace Exploration, Concept Selection</td>
<td>12.5%</td>
</tr>
<tr>
<td>A5 (group)</td>
<td>Preliminary Design Review (PDR) Package and Presentation</td>
<td>20%</td>
</tr>
<tr>
<td>Quiz (individual)</td>
<td>Written online quiz</td>
<td>10%</td>
</tr>
<tr>
<td>Oral Exam (individual)</td>
<td>20’ Oral Exam with Instructor 2-page reflective memorandum</td>
<td>10%</td>
</tr>
</tbody>
</table>

A5 is due next week!
The "V-Model" of Systems Engineering

1. Stakeholder Analysis
2. Requirements Definition
3. System Modeling Languages - MBSE
4. System Architecture Concept Generation
5. Tradespace Exploration Concept Selection
6. Design Definition Multidisciplinary Optimization
7. System Integration Interface Management
8. System Integration Interface Management
9. Verification and Validation
10. Commissioning Operations
11. Lifecycle Management

Numbers indicate the session # in this class

*optional
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
  - System Safety

- Flight Readiness Review (FRR)
Readings related to this lecture

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

Verification and Validation

Start

Stakeholder Analysis

Is goal representative?

Validation

Delivered Function

Validation Loop

Delivered Goals = Metrics + Delivered value

Attainable?

Verification Loop

Set Requirements = Metric + Target value

Complete?

Functional Deployment

Intended function

Solvable?

Concept

Model Implemented

Design Solution

Testing
Differences between V & V

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

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

Was the end product realized right?

Was the right end product realized?

This image is in the public domain.
### Concept Question 9

What is your name?

---

How would you classify the following activities? *

<table>
<thead>
<tr>
<th>Activity</th>
<th>Verification</th>
<th>Validation</th>
<th>No sure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing handling of a new car in snow conditions in Alaska</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frontal crash test in the lab</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing of a new toy in a Kindergarten</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vehicle emissions testing on a dynamo</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Satellite vibration testing on a shake table</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Field testing of Google glasses with 1,500 pilot users</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Answer Concept Question 9 (see supplemental files)
Product Verification Process

Types of verification:
- Analysis
- Demonstration
- Inspection
- Test

Outputs:
- Discrepancy reports
- Verified product
- Compliance documentation
## NASA Life-Cycle Phases

<table>
<thead>
<tr>
<th>Project Life Cycle Phases</th>
<th>FORMULATION</th>
<th>IMPLEMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Life Cycle Gates &amp; Major Events</strong></td>
<td><strong>Pre-Phase A:</strong> Concept Studies</td>
<td><strong>Phase A:</strong> Concept &amp; Technology Development</td>
</tr>
<tr>
<td></td>
<td>Pre-Phase B: Preliminary Design &amp; Technology Completion</td>
<td><strong>Phase C:</strong> Final Design &amp; Fabrication</td>
</tr>
<tr>
<td></td>
<td><strong>Phase D:</strong> System Assembly, Int &amp; Test, Launch</td>
<td><strong>Phase E:</strong> Operations &amp; Sustainment</td>
</tr>
<tr>
<td></td>
<td><strong>Phase F:</strong> Closeout</td>
<td><strong>Final Archival of Data</strong></td>
</tr>
</tbody>
</table>

### Agency Reviews
- **Human Space Flight Project Reviews**
  - **Re-flights**
- **Robotic Mission Project Reviews**
- **Launch Readiness Reviews**
- **Supporting Reviews**

### Human Space Flight Project Reviews
- **KDP A:** Draft Project Requirements
- **KDP B:** Preliminary Project Plan
- **KDP C:** Baseline Project Plan
- **KDP D:**
- **KDP E:**
- **KDP F:**
- **Launch**
- **End of Mission**
- **Final Archival of Data**

### Robotic Mission Project Reviews
- **KDP B:**
- **KDP C:**
- **KDP D:**
- **KDP E:**
- **KDP F:**

### Agency Reviews
- **ASP**
- **ASM**
- **MCR**
- **SRR**
- **SDR**
- **PDR**
- **CDR / PRR**
- **SAR**
- **ORR**
- **PLAR**
- **CERR**
- **DR**
- **PFAR**

### Supporting Reviews
- **Peer Reviews, Subsystem PDRs, Subsystem CDRs, and System Reviews**

### 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, LRR**—Safety and Mission Success Review
- **SRR**—System Requirements Review

### 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.
## NASA Life-Cycle Reviews

<table>
<thead>
<tr>
<th>Review</th>
<th>Title</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>P/SRR</td>
<td>Program Requirement Review</td>
<td>The P/SRR is used to ensure that the program requirements are properly formulated and correlated with the Agency and mission directorate strategic objectives</td>
</tr>
<tr>
<td>P/SDR</td>
<td>Program Definition Review, or System Definition Review</td>
<td>The P/SDR ensures the readiness of the program for making a program commitment agreement to approve project formulation startups during program Implementation phase.</td>
</tr>
<tr>
<td>MCR</td>
<td>Mission Concept Review</td>
<td>The MCR affirms the mission need and examines the proposed mission’s objectives and the concept for meeting those objectives</td>
</tr>
<tr>
<td>SRR</td>
<td>System Requirement Review</td>
<td>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</td>
</tr>
<tr>
<td>MDR</td>
<td>Mission Definition Review</td>
<td>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</td>
</tr>
<tr>
<td>SDR</td>
<td>System Definition Review</td>
<td>The SDR examines the proposed system architecture and design and the flow down to all functional elements of the system.</td>
</tr>
<tr>
<td>PDR</td>
<td>Preliminary Design Review</td>
<td>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</td>
</tr>
<tr>
<td>CDR</td>
<td>Critical Design review</td>
<td>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.</td>
</tr>
<tr>
<td>PRR</td>
<td>Production Readiness Review</td>
<td>A PRR is held for FS&amp;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.</td>
</tr>
</tbody>
</table>

NPR 7123.1A, Chapter 3. & Appendix C.3.7  
SP-2007-6105, Section 6.7  
This image is in the public domain.
### Listing of NASA Life-Cycle Reviews (Continued)

<table>
<thead>
<tr>
<th>Review</th>
<th>Title</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIR</td>
<td>System Integration Review</td>
<td>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.</td>
</tr>
<tr>
<td>TRR</td>
<td>Test Readiness Review</td>
<td>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.</td>
</tr>
<tr>
<td>SAR</td>
<td>System Acceptance Review</td>
<td>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.</td>
</tr>
<tr>
<td>ORR</td>
<td>Operational Readiness Review</td>
<td>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.</td>
</tr>
<tr>
<td>FRR</td>
<td>Flight Readiness Review</td>
<td>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.</td>
</tr>
<tr>
<td>PLAR</td>
<td>Post-Launch Assessment Review</td>
<td>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.</td>
</tr>
<tr>
<td>CERR</td>
<td>Critical Event Readiness Review</td>
<td>A CERR confirms the project’s readiness to execute the mission’s critical activities during flight operation.</td>
</tr>
<tr>
<td>PFAR</td>
<td>Post-Flight Assessment Review</td>
<td>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.</td>
</tr>
<tr>
<td>DR</td>
<td>Decommissioning Review</td>
<td>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.</td>
</tr>
</tbody>
</table>
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
  - System Safety

- Flight Readiness Review (FRR)
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
Turn-to-your-partner Exercise (5 min)

- What kind of testing have you been involved in in the past? What was the purpose? What where the challenges? What went well? What were the results?

- Discuss for 5 min.

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

This image is in the public domain.
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)
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

code8200.nrl.navy.mil/rfanechoic.html
JWST – On-Orbit Deployment

This image is in the public domain.
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
## Table E-1 Validation Requirements Matrix

<table>
<thead>
<tr>
<th>Validation Product #</th>
<th>Activity</th>
<th>Objective</th>
<th>Validation Method</th>
<th>Facility or Lab</th>
<th>Phase</th>
<th>Performing Organization</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique identifier for validation product</td>
<td>Describe evaluation by the customer/sponsor that will be performed</td>
<td>What is to be accomplished by the customer/sponsor evaluation</td>
<td>Validation method for the System X requirement (analysis, inspection, demonstration, or test)</td>
<td>Facility or laboratory used to perform the validation</td>
<td>Phase in which the verification/validation will be performed⁴</td>
<td>Organization responsible for coordinating the validation activity</td>
<td>Indicate the objective evidence that validation activity occurred</td>
</tr>
</tbody>
</table>

| 1 | Customer/sponsor will evaluate the candidate displays | 1. Ensure legibility is acceptable 2. Ensure overall appearance is acceptable | Test | xxx | Phase A | xxx | |

---

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.

---

This image is in the public domain.
Appendix I : V&V Plan 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
      3.3.2. System X End Item B
   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!
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
  - System Safety

- Flight Readiness Review (FRR)
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**
  - Political stability
  - New Science Requirements

- **Country/Fiscal**
  - ????

- **Industry/Competitive**
  - Contractor Performance
  - Budget Stability

- **Technical/Project Risks**
  - Airbag Technology Maturity
  - Rover Motor Performance
  - Software Bugs

High Influence | Low Influence
Risk Categories – “Iron” Triangle

- Technical Risk
- Cost Risk
- Schedule Risk

Relations:
- Limited Funds
- Technical Problems
- Compressed Schedules
- Imposed Budgets
- Technical Problems
- Demand Schedules
- Schedule Slips
- Market/Threat Change
A Risk Management Framework

Correct deviations

Anticipate what can go wrong

Control

Identify

Plan

Plan to take action

Analyze

Track actions

Track

Communicate
**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 All Stakeholders**
Risk Sector Plot (NASA)

**Attribute: Probability**

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

**Attribute: Impact**

<table>
<thead>
<tr>
<th>Level</th>
<th>Value</th>
<th>Technical Criteria</th>
<th>Cost Criteria</th>
<th>Schedule Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Can’t control the vehicle OR Can’t perform the mission</td>
<td>&gt; $10 Million</td>
<td>Slip to level I milestones</td>
</tr>
<tr>
<td>4</td>
<td>Critical</td>
<td>Loss of mission, but asset recoverable in time</td>
<td>$ 10 M ≤ X &lt; $ 5 Million</td>
<td>Slip to level II milestones</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Mission degraded below nominal specified</td>
<td>$ 5 M ≤ X &lt; $ 1 Million</td>
<td>Slip to level III milestones</td>
</tr>
<tr>
<td>2</td>
<td>Marginal</td>
<td>Mission performance margins reduced</td>
<td>$ 1 M ≤ X &lt; $ 100 K</td>
<td>Loss of more than one month schedule margin</td>
</tr>
<tr>
<td>1</td>
<td>Negligible</td>
<td>Minimum to no impact</td>
<td>Minimum to no impact</td>
<td>Minimum to no impact</td>
</tr>
</tbody>
</table>
Technical Risk Management – Best Practice

Process Flow Diagram

**Input**

- From Project
  - Project Risk Management Plan
- From Project and All Technical Processes
- Technical Risk Issues
- From Technical Assessment and Decision Analysis Processes
  - Technical Risk Status Measurements
- From Project and Technical Assessment Process
  - Technical Risk Reporting Requirements

**Activities**

1. Prepare a Strategy to Conduct Technical Risk Management
2. Identify Technical Risks
3. Conduct Technical Risk Assessment
4. Prepare for Technical Risk Mitigation
5. Monitor the Status of Each Technical Risk Periodically
7. Capture Work Products from Technical Risk Management Activities

**Output**

- To Technical Planning Process
  - Technical Risk Mitigation and/or Contingency Actions
- To Project and Technical Data Management Process
  - Technical Risk Reports
- To Technical Data Management Process
  - Work Products of Technical Risk Management

This image is in the public domain.
Systems Safety: Types of Accidents

- **Component Failure Accidents**
  - Single or multiple component failures
  - Usually assume random failure

- **Component Interaction Accidents**
  - Arise in interactions among components
  - Related to
    - Interactive complexity and tight coupling
    - Use of computers and software
    - Role of humans in systems

Traditional Safety Thinking:

Chain-of-events example

May only work for traditional (mechanical) component failure events

© The MIT Press. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/help/faq-fair-use/.
STPA: A New Hazard Analysis Technique Based on STAMP

More powerful for complex software-enabled human-in-the-loop systems
Turn to your Partner Exercise (5 min)

- Turn to your Partner Exercise
- How can the 2014 Virgin Galactic accident be explained using STAMP/STPA?

Virgin Galactic crash: co-pilot unlocked braking system too early, inquiry finds

A nine-month investigation by the National Transportation Safety Board has found human error and inadequate safety procedures caused the violent crash

A piece of debris near the crash site of Virgin Galactic's SpaceShipTwo in California on 1 November 2014. Photograph: Lucy Nicholson/Reuters


© Guardian News and Media Limited or its affiliated companies. All rights reserved. This content is excluded from our Creative Commons license. For more information, see http://ocw.mit.edu/help/faq-fair-use/.
System’s Theoretic View of Safety

- Safety is an emergent system property
  - Accidents arise from interactions among system components (human, physical, social)
  - That violate the constraints on safe component behavior and interactions

- Losses are the result of complex processes, not simply chains of failure events

- Most major accidents arise from a slow migration of the entire system toward a state of high-risk

- Based on systems theory rather than reliability theory
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
  - System Safety

- Flight Readiness Review (FRR)
Figure 3.0-1 NASA program life cycle

- CDR: Critical Design Review
- CERR: Critical Events Readiness Review
- DR: Decommissioning Review
- FRR: Flight Readiness Review
- KDP: Key Decision Point
- MCR: Mission Concept Review
- MDR: Mission Definition Review
- ORR: Operational Readiness Review
- PDR: Preliminary Design Review
- PFAR: Post-Flight Assessment Review
- PIR: Program Implementation Review
- PLAR: Post-Launch Assessment Review
- PRR: Production Readiness Review
- P/SRR: Program/System Requirements Review
- P/SRR: Program/System Requirements Review
- P/SDR: Program/System Definition Review
- PSR: Program Status Review
- SAR: System Acceptance Review
- SDR: System Definition Review
- SIR: System Integration Review
- SRR: System Requirements Review
- TRR: Test Readiness Review

PSRs, PIRs, and KDPs are conducted ~ every 2 years.
Flight Readiness Review (FRR)

- Last Milestone before Launch
  - Have all the V&V activities been passed successfully?
  - Are there any waivers that need to be granted?
  - What are the residual risks?
  - Start Countdown (T- X days Y hours Z seconds)

### Table 6.7-15  FRR Entrance and Success Criteria

<table>
<thead>
<tr>
<th>Entrance Criteria</th>
<th>Success Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Receive certification that flight operations can safely proceed with acceptable risk.</td>
<td>1. The flight vehicle is ready for flight.</td>
</tr>
<tr>
<td>2. The system and support elements have been confirmed as properly configured and ready for flight.</td>
<td>2. The hardware is deemed acceptably safe for flight (i.e., meeting the established acceptable risk criteria or documented as being accepted by the PM and DGA).</td>
</tr>
<tr>
<td>3. Interfaces are compatible and function as expected.</td>
<td>3. Flight and ground software elements are ready to support flight and flight operations.</td>
</tr>
<tr>
<td>4. The system state supports a launch Go decision based on Go or No-Go criteria.</td>
<td>4. Interfaces are checked out and found to be functional.</td>
</tr>
<tr>
<td>5. Flight failures and anomalies from previously completed flights and reviews have been resolved and the results incorporated into all supporting and enabling operational products.</td>
<td>5. Open items and waivers have been examined and found to be acceptable.</td>
</tr>
<tr>
<td>6. The system has been configured for flight.</td>
<td>6. The flight and recovery environmental factors are within constraints.</td>
</tr>
<tr>
<td></td>
<td>7. All open safety and mission risk items have been addressed.</td>
</tr>
</tbody>
</table>
Summary Lecture 9

- **Verification and Validation are critical**
  - Verification makes sure the product is built to requirements
  - Validation assesses whether the product/system is really what the customer wants, i.e. whether it satisfies his or her needs

- **Testing**
  - Critical to project outcome, different types of testing ....
  - Fundamentally a Q&A activity
  - Expensive, need to be done right

- **Risk Management**
  - Risk Matrix, Risk Identification, Mitigation
  - Tensions between cost, scope, schedule, risk

- **Systems Safety**
  - Violation of Safety Constraints, not simply chains of events
  - STAMP / STPA

- **Flight Readiness Review (FRR)**
  - Last chance to raise any “red flags”
Questions?
16.842 Fundamentals of Systems Engineering
Fall 2015

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.