Systems Engineering Cost/Risk Analysis Capability Roadmap Progress Review

Stephen Cavanaugh, NASA Chair
Dr. Alan Wilhite, External Chair
April 6, 2005
## Agenda

| Time   | Topic                                                                 | Speaker                                           |
|--------|-----------------------------------------------------------------------|                                                  |
| 7:30   | Continental Breakfast                                                 |                                                   |
| 8:00   | Welcome and Review Process, Panel Chair & NRC Staff                   |                                                   |
| 8:15   | NASA Capability Roadmap Activity                                      | Vicki Regenie, NASA                               |
| 8:30   | 15.0 Systems Engineering Cost/Risk Analysis Overview                 | Stephen Cavanaugh, NASA                           |
| 9:00   | 15.1 Systems Engineering                                              | Dr. Alan Wilhite, Georgia Tech                    |
|        | - Sub-Team Presentations -                                            |                                                   |
| 11:15  | 15.2 Life Cycle Costing                                               | Dr. David Bearden, Aerospace Corporation          |
| 12:00  | - Lunch -                                                            |                                                   |
| 12:45  | 15.3 Risk Management                                                  | Theodore Hammer, NASA                              |
| 1:30   | 15.4 Safety and Reliability Analysis                                  | Dr. Homayoon Dezfuli, NASA                        |
| 2:15   | Concluding Summary                                                   | Stephen Cavanaugh, NASA                           |
|        | - Break -                                                            |                                                   |
| 3:00   | Open Discussion                                                       | NRC Panel                                         |
Co-Chairs
NASA: Stephen Cavanaugh, LaRC
External: Dr. Alan Wilhite, Georgia Tech

Team Members
Government
Dr. Michael Gilbert, LaRC
Theodore Hammer, HQ
Dr. Homayoon Dezfuli, HQ
Stephen Creech, MSFC
Phil Napala, HQ
CAPT Daven Madsen, Navy/NSSO
Dr. Steve Meier, NRO
Richard Westermeyer, Navy/NSSO

Industry
Dr. David Bearden, Aerospace
Dr. Leonard Brownlow, Aerospace
Gaspare Maggio, SAIC
Steven Froncillo, SAIC

Academia
Dr. Alan Wilhite, Georgia Tech

Consultants
Stephen Kapurch, HQ
David Graham, HQ
Dale Thomas, MSFC
Stephen Prusha, JPL
Chuck Wiesbin, JPL
Ron Moyer, HQ

Coordinators
Directorate: Vicky Hwa, HQ Technical
Doug Craig, HQ Integration
Betsy Park, HQ Integration
APIO: Victoria Regenie, DFRC
• **Systems engineering** is a robust approach to see to it that the system is designed, built, and operated so that it accomplishes its purpose in the most cost-effective way possible, considering performance, cost, schedule, and risk.

• **Life-Cycle Cost** is an integrated, process-centered, and disciplined approach to life cycle management of projects providing real and tangible benefits to all project stakeholders.

• **Risk Management** identifies potential problem areas early enough to allow development and implementation of mitigation strategies to control cost, schedule and mission success.

• **Safety and Reliability Analysis** maximizes Mission Success while managing safety risk and affordably meeting mission objectives.
This Capability Roadmap scope does not include performing the integration of all fifteen Capability Roadmaps. Roadmap coordinators (MD, Center, & APIO) comprise the Integration Team and facilitate the integration process by capturing Roadmap data and dependencies and documenting in relational database tool.
The President has challenged NASA to undertake exploration of the solar system.

In the face of tight budgets and mission risks, it is critical that these missions be executed flawlessly.

- Requires sound approach to Systems Engineering
  - Tools, methods, processes
    - Continuous improvement
  - Best of industry and government
  - Standard processes
    - All centers
    - All missions
    - All programs/projects

System Engineering must be a “value added proposition” not an overhead burden.

Consistent with the spirit of CAIB Recommendation.

NASA’s new vision requires, more than ever, excellence in an integrated systems engineering cost/risk analysis capability.
Four Systems Engineering Essentials

1st – Processes & Concepts (What)

2nd – Performance Aids (How)

3rd – Workforce (Who)

4th – How well organization implements and supports the framework with:

- Policies & Procedures
- Process Improvement
- Human Resources
- Training
- Milestone & Decision Gate Review Criteria
- Management of Quality
Complexity is a Major Issue

• Systems-of-Systems are Complex
  – As More Systems Are Added, the Interfaces Grow in a Non-Linear Fashion
  – Many of the Existing Systems Are Old and Not Built for These Interfaces
  – Conflicting or Missing Interface Standards Make It Hard to Define Interface Interactions

• Systems Engineering Must Deal With This Complexity
  – End-to-End Systems Engineering Is Needed, Including “Reengineering” Of Old Systems
  – Robust M&S, Verification And Validation Testing Are A Must
  – Need To Upgrade Modeling And Simulation Tools For Both Concept Definition And Verification And Validation Phases

Northrop Grumman Integrated Systems
September 21, 2004 Letter from the National Academies

Dear RADM Steidle:

At your request, the National Research Council recently established the Committee on Systems Integration for Project Constellation. The following quotes were taken from the report:

“Strengthening the state of systems engineering is also critical to the long-term success of Project Constellation. A competent systems engineering capability must be resident within the government and industry”.

“NASA’s human spaceflight systems engineering capability has eroded significantly as a result of declining engineering and development work, which has been replaced by operational responsibilities”.

“The demand for experienced systems engineers, who can function credibly in a system-of-systems environment, is particularly acute”.

“Plans should be developed for maintaining a satisfactory base of systems engineering throughout the duration of this program”.

“Systems Integration” Will Take Place At Multiple Tiers
- Tiers structured around functional responsibilities
- Must be prepared to support with maximum efficiency, minimum bureaucracy
- Need to support Directorate and Technology Themes, as well as Constellation
- SE&I authority should reside at lowest possible level

System-of-Systems Integration Demands Creative Solution
- No single model evaluated by NRC offers complete solution
- Complete expertise and competence is not available in any one sector
- Certain functions can only be executed by government personnel
- “Hybrid model” using government, FFRDC, and industry is attractive

ESMD SE&I Capability Will Be Phased-In Over Time
- Government will perform SE&I work needed to complete Spiral 1 SRR
- Near-term solution may evolve to different Long-term solution
Capability Roadmapping
Process & Approach

National Standards and
State of Art Practices
for
SE, Risk, Cost, Safety

Develop Team Schedule
And
Deliverables

Develop Capability Model

Assess NASAs’
Capability
Requirements

Identify Capability
Readiness and Gaps

Develop Interrelationship
Matrix with Strategic and
Capability Roadmaps

Develop and Prioritize
Mitigation Strategies

Workshop 1
December 8-9, 2004

Workshop 2
February 1-2, 2005

SE Benchmarking
Activity @ Fort Belvoir
February 22-23, 2005

Workshop 3
March 2-3, 2005

Define Development
Schedule, Cost, Deliverables,
and Readiness Maturity for
Critical Capability Needs

Document Roadmap Plan

NASA Chief Engineer’s
SE Study
June 2005 Completion
Basis for Assessment

- Quality Function Deployment (QFD)
  - A quality system that implements elements of Systems Thinking (viewing the development process as a system) and Psychology (understanding customer needs)

- Benchmarking – Chief Engineers Fort Belvoir Workshop on February 22-23, 2005
  - Learning from the experience of others in Industry, DoD, and Other Agencies

- Literature Search – mostly Internet

- Limitations of Assessment
  - Budget limitations keep team small and limited in scope
  - QFD assessment limited to team size – small sample of NASA
  - Assessment more Qualitative vs. Quantitative
Capability readiness rating assignments are intended for future exploration missions and as such they should not be interpreted as capability ratings to perform the current missions.
Capability Team 15: Systems Engineering Top Level Capability Roadmap

Key Assumptions: Exploration & Science

- 2018: Deep Drill & Completed Initial Human Landing
- 2025: Extended Lunar Capability & Life Finder Telescope
- 2030: Prepare for Human Mars Mission

Capability Roadmap 15: Systems Engineering Risk/Cost Analysis

- 15.1 Systems Engineering
  - Decisions based on Economic LCC Models
- 15.2 Life Cycle Cost
  - LCC imbedded in all Agency Decisions
- 15.3 Risk Management
  - Interactive Risk Identification and Mitigation
  - Accurate Risk Analysis in Uncertain Environments
- 15.4 Safety & Reliability
  - Safety & Reliability Informed Decision making
  - Virtual Safety and SE Analysis capability

Legend
- PLM – Product Life Cycle Management
- SBM – Simulation Based Modeling
- CMMI – Capability Maturity Model Integration
- QRA - Quantitative Risk Assessment
- LCC - Life Cycle Cost
Future State Required to Meet NASA Exploration Vision

- **Process (What)** – Need a common process for Systems Engineering, Cost, Risk and Safety. NASA Policy Requirements, guidelines and handbooks for this Capability need to be developed along with a need for an audible process.

- **Tools (How)** – Need a standardized approach for Systems Analysis. This includes a framework for advanced tools.

- **People (Who)** – Need qualified personnel. Training & Education programs including certification tied to job criteria and performance standards.

"An immediate transformation imperative for all programs is to focus more attention on the application of Systems Engineering principles and practices throughout the system life cycle”

USAF Chief of Acquisition Memo, “Incentivizing Contractors for Better Systems Engineering, 9 Apr 03
Capability 15.1 Systems Engineering

Presenter:
Dr. Alan Wilhite
Benefits of Systems Engineering

- Requirements driven – build the right system
- Process driven – build the system right
- Integrated engineering and management for informed decisions
- Less cost / Less duration
Systems Management

- Requirements, Requirements flowdown, Interfaces and Integration
- Performance, Specifications, Verification and Validation
- Technical Risk, Cost

Systems Engineering and Integration

- Planning, Development, Production, Operations,
- Decision Analysis and Criteria, Cost and Schedule Risk
- Technology Selection, Performance trades, Requirements trades
- Min Performance Criteria, Investment Strategy, Best System,
- Verification and Validation, Technical Risk

Engineering and Analysis

Ref. GaTech AE 6322
The Systems Engineering Process
(Ref. Mil STD 499B)

Process Input
- Customer Needs/Objectives/Requirements
  - Missions
  - Measures of Effectiveness
  - Environments
  - Constraints
- Technology Base
- Output Requirements from Prior Development Effort
- Program Decision Requirements
- Requirements Applied Through Specifications and Standards

Requirements Analysis
- Analyze Missions & Environments
- Identify Functional Requirements
- Define/Refine Performance & Design Constraint Requirement

Functional Analysis/Allocation
- Decompose to Lower-Level Functions
- Allocate Performance & Other Limiting Requirements to All Functional Levels
- Define/Refine Functional Interfaces (Internal/External)
- Define/Refine/Integrate Functional Architecture

Synthesis
- Transform Architectures (Functional to Physical)
- Define Alternative System Concepts, Configuration Items & System Elements
- Select Preferred Product & Process Solutions
- Define/Refine Physical Interfaces (Internal/External)

System Analysis & Control (Balance)
- Trade-Off Studies
- Effectiveness Analysis
- Risk Management
- Configuration Management
- Interface Management
- Performance Measurement
  - SEMS
  - TPM
  - Technical Reviews

Verification
- Requirement Loop

Design Loop
- Process Output
  - Development Level Dependant
    - Decision Data Base
    - System/Configuration Item Architecture
    - Specification & Baseline

Related Terms:
- Customer = Organization responsible for Primary Functions
- Primary Functions = Development, Production/Construction, Verification, Deployment, Operations, Support Training, Disposal
- Systems Elements = Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques

The Systems Engineering Process
(Ref. Mil STD 499B)
**Scope of SE Standards**

- **IEEE 1220 Application & Management of the SE Process**
- **ANSI/EIA 632 Processes for Engineering Systems**
- **ISO/IEC 15288 System Life Cycle Processes**
- **MIL-STD-499B * Systems Engineering**

* Mil-Std-499C has more detail (similar to 15288) than Mil-Std 499B and has more breadth (similar to IEEE 1220)
CMMI – DoD developed integrated model for systems engineering, software engineering, integrated product process development, and supplier sourcing

CMMI used as initial basis for strategic planning
Overview of the “State”

- The Standish Group (which exists solely to track IT successes and failures) surveyed 13,522 projects in 2003 and showed the following:
  - 34% of projects succeed (these projects are defined as those which deliver the contracted capabilities on time and on budget).
  - 15% of projects are out and out failures (these projects are defined as those abandoned midstream).
  - The rest (51%) are "challenged", meaning over budget, and/or over schedule, and/or deliver less capability / functionality than agreed upon and contracted for.

- According to a Lake & Sheard paper:
  - Systems Engineering is practiced in a quagmire of SE Standards
    - MARC Proceedings 1999

- According to the AF Center for Systems Engineering:
  - “Systems Engineering is not broken.”
    - GEIA-G47 meeting January 2005

Systems Engineering is not broken but needs significant advancement to improve NASA’s program success rate.
System Engineering Processes
## SE Capability Team Assessment

### Integrated rollup of Importance and Present Capability

<table>
<thead>
<tr>
<th>SE-CMMI</th>
<th>Team Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ENGINEERING</strong></td>
<td></td>
</tr>
<tr>
<td>Requirements Development</td>
<td></td>
</tr>
<tr>
<td>Requirements Management</td>
<td></td>
</tr>
<tr>
<td>Technical Solution</td>
<td></td>
</tr>
<tr>
<td>Product Integration</td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td></td>
</tr>
<tr>
<td>Validation</td>
<td></td>
</tr>
<tr>
<td><strong>PROJECT MANAGEMENT</strong></td>
<td></td>
</tr>
<tr>
<td>Project Planning</td>
<td></td>
</tr>
<tr>
<td>Project Monitoring and Control</td>
<td></td>
</tr>
<tr>
<td>Supplier Agreement Management</td>
<td></td>
</tr>
<tr>
<td>Integrated Project Management</td>
<td></td>
</tr>
<tr>
<td>Integrated Supplier Management</td>
<td></td>
</tr>
<tr>
<td>Quantitative Project Management</td>
<td></td>
</tr>
<tr>
<td><strong>SUPPORT</strong></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td></td>
</tr>
<tr>
<td>Process and Product Quality Assurance</td>
<td></td>
</tr>
<tr>
<td>Measurement and Analysis</td>
<td></td>
</tr>
<tr>
<td>Decision Analysis and Resolution</td>
<td></td>
</tr>
<tr>
<td>Organizational Environment for Integration</td>
<td></td>
</tr>
<tr>
<td>Causal Analysis and Resolution</td>
<td></td>
</tr>
<tr>
<td><strong>PROCESS MANAGEMENT</strong></td>
<td></td>
</tr>
<tr>
<td>Organizational Process Focus</td>
<td></td>
</tr>
<tr>
<td>Organizational Process Definition</td>
<td></td>
</tr>
<tr>
<td>Organizational Training</td>
<td></td>
</tr>
<tr>
<td>Organizational Process Performance</td>
<td></td>
</tr>
<tr>
<td>Organizational Innovation and Deployment</td>
<td></td>
</tr>
</tbody>
</table>
Establish Evaluation Criteria
Identify and Analyze Risks
Select Solutions
Evaluate Alternatives
INTEGRATED TEAMING
Manage Corrective Action to Closure
Establish Estimates
Identify Alternative Solutions
Objectively Evaluate Work Products and Services
Evaluate Assembled Product Components
Obtain an Understanding of Requirements
ORGANIZATIONAL TRAINING
Balance Team and Home Organization Responsibilities
Identify Inconsistencies between Project Work and Requirements
ORGANIZATIONAL INNOVATION AND DEPLOYMENT
Establish Incentives for Integration
Establish the Organization’s Shared Vision
Establish Guidelines for Decision Analysis
### Other Identified SE Capability Gaps

<table>
<thead>
<tr>
<th>Capability</th>
<th>Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems of Systems Integration</td>
<td>Critical Gap</td>
</tr>
<tr>
<td>Experienced SE Personnel</td>
<td>Significant Gap</td>
</tr>
<tr>
<td>Standard Process/Process Improvement</td>
<td>Significant Gap</td>
</tr>
<tr>
<td>Facilitate Advanced Technology</td>
<td>No or Minor Gap</td>
</tr>
<tr>
<td>Estimate and Manage Costs</td>
<td>No or Minor Gap</td>
</tr>
<tr>
<td>Acquisition Strategy</td>
<td>No or Minor Gap</td>
</tr>
<tr>
<td>Advanced Collaborative Environment</td>
<td>No or Minor Gap</td>
</tr>
</tbody>
</table>

**Refs.**

- NRC SE&I Study, 2004
- NASA SE Workshop, 2005
Quagmire of SE Standards

- But SE standard writers can’t agree on what should be in a standard – Hence a quagmire!
Scope of SE Standards

- **IEEE 1220**: Application & Management of the SE Process
- **ANSI/EIA 632**: Processes for Engineering Systems
- **ISO/IEC 15288**: System Life Cycle Processes
- **MIL-STD-499B**: Systems Engineering

**CMMI/SE**

- *Mil-Std-499C has more detail (similar to 15288) than Mil-Std 499B and has more breadth (similar to IEEE 1220)*

Ref: Lake Briefing at February 2005 Ft Belvoir NASA Chief Engineer Workshop
SE Gap Assessment indicates that CMMI Maturity Levels 2 and 3 should be developed in parallel for NASA.
SE Gap Assessment also agrees with CMMI that Systems Engineering and Program Management must be integrated for NASA.
## Enterprise Systems versus Program Systems Engineering

### Single Systems Engineering (Stand Alone Systems)
- End state well defined
- Engineered and developed within a fixed budget and cost
- Well known schedule, technical, and benefit baseline
- Often replaces a “legacy” System
- Priority often
  - Technical/Security
  - Operational
  - Cost
  - Political

### Enterprise Systems Engineering (System-of-Systems)
- Dynamic end state System-of-Systems evolves over time
- Subject to annual budget revisions
- Facilitates Senior Decision Makers
- Priority often
  - Political
  - Cost
  - Operational
  - Security
  - Technical

### Competing Forces Addressed by Systems Engineering

![Diagram]

**Optimal Solution Space**
- Technical
- Cost
- Operational
- Security
Recommended NASA SE Process Development

- **Tier 1: SE Agency Policy and Process Improvement Processes**
  - Process application policy
  - Architecture, Base and General Processes
  - Knowledge Management and Continuous Process Improvement

- **Tier 2: Process Area Procedures**
  - Specific standards and references identified
  - Process interfaces (HQ-Center, HQ-Contractor, Center-Contractor)
  - System of Systems integration
  - Can be tailored to specific directorate

- **Tier 3: Detailed Guidebooks**
  Best practices of how to implement SE
  General tools and methods

- **Tier 4: System Engineering Management Plans**
  - Technical program
  - Specific plans on SE implementation
  - Engineering specialty integration
  - Specific tools and methods selected
  - Organizational and contract interfaces defined
### System Engineering Processes

#### Assessment and Vision

<table>
<thead>
<tr>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
<tbody>
<tr>
<td>- national standard processes exist but in a quagmire of interfaces</td>
<td>- A systems engineering policy, guidelines, and implementation strategies based on national standards and NASA/DoD/contractor best practices has been developed</td>
<td>- A collaborative / distributive advanced engineering environment for product life-cycle engineering and management has been developed based on system engineer and management processes for systems development and workforce training</td>
<td>- an expert system for systems engineering exists to aid in the training and use of the validated advanced engineering environment for complex systems-of-systems developments</td>
</tr>
<tr>
<td>- NASA has a SE guideline (NASA SP-6105) that is only sporadically followed</td>
<td>- Annual audits of NASA's systems engineering process model ensures best practices are used and distributed</td>
<td>- Systems engineering, life-cycle cost, risk, and safety have been integrated for robust solutions of complex systems-of-systems development</td>
<td>- Knowledge management has revolutionized the startup of new programs with reuse of processes and tools</td>
</tr>
<tr>
<td>- no NASA-wide policy on systems engineering exists</td>
<td>- A systems engineering certification program requiring continual education and training has been institutionalized</td>
<td>- All NASA centers have achieved the top level of systems engineering maturity</td>
<td>- All decisions are based on validated simulations and virtual and surgical physical testing for performance, cost, safety, uncertainty, and risk (and politics!!)</td>
</tr>
<tr>
<td>- NASA, DoD, and contractor teams use different processes and terminology</td>
<td>- A knowledge management system for capturing and reuse of best practices and knowledge repository for cost, reliability, validated systems analyses and simulations, software, and hardware has been initiated</td>
<td>- A certified (educated, trained, and experienced) systems engineering staff exists for engineering, management, and decision making</td>
<td>- a completed integrated international organization is optimized for the collaborative distributed environment</td>
</tr>
<tr>
<td></td>
<td>- A completely digital product life-cycle management system for systems engineering and management for program/project control has been developed</td>
<td>- the organization interfaces and throughput is optimized through dynamic simulations</td>
<td></td>
</tr>
</tbody>
</table>

Skills (Workforce)
Systems Engineering Architect/Specialist

- Definition of a Systems Engineering Architect/Expert
  - Architect network centric and systems of systems
  - System Integrator
  - Drives next generation of mission solutions
- Attributes
  - Experienced technical leader
  - Experienced in working with the customer, understand their needs and customer value and to serve as the customer’s primary technical interface
  - Expert in fundamentals – cost, schedule, risk, processes
  - System lifecycle experience from pre-proposal to logistics support
  - Understand hardware, software, mission and big picture
  - Solid interpersonal skills, verbal and written communications
- Lack of senior level experienced systems engineers/architects
  - Many self-proclaimed systems engineers
  - Exists both in industry and government
Degreed workforce is a shrinking pool.
The Resource Picture

- Degreed workforce is a shrinking pool
  - Many graduates are not US citizens
  - Total engineering enrollments continue to decrease
- 20-30 year cycle between major system developments and 10 year development cycle
  - Lack of SE experience on large complex systems
  - Experienced SE engineers are retiring faster than being trained
- NASA systems engineering for human spaceflight has eroded and systems of systems is particularly acute (NRC 2004 NASA Systems Integration Study)
- Existing university / industry partnerships are not having enough impact
  - SE is not a standard discipline (EE, ChemE, ME etc.)
  - More penetration at undergraduate level
- Need new ways to attract and develop system engineers
  - Additional learning
  - On-the-job experience
  - Virtual simulation
<table>
<thead>
<tr>
<th>Level</th>
<th>Experience</th>
<th>Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>2 yrs. SE</td>
<td>SE-501 Acquisition Systems Engineering and SE-502 Designing Space Missions or 6 SE-related graduate credits or SPRDE Level II Certified</td>
</tr>
<tr>
<td>II</td>
<td>4 yrs. SE</td>
<td>Complete 4 from below: Requirements Development/Management, Risk Management, Measurement &amp; Analysis, Concept &amp; Architecture Development, Formal Decision Making, Integration, Verification &amp; Validation or 12 SE-related graduate credits or 6 after Level 1 or SPRDE Level III Certified</td>
</tr>
<tr>
<td>III</td>
<td>7 yrs. SE</td>
<td>INCOSE Certification or 18 total SE-related graduate credits or 6 after Level 2</td>
</tr>
</tbody>
</table>

NASA needs to develop a SE certification program to develop systems engineering to meet future program requirements.
• Establish SE development policy including SE certification requirements for promotions

• Establish Government, industry, and academia SE education, training, and job experience partnerships

• Develop guidelines and process for SE graduated certification. Include integration with program management education and training

• Measure progress in SE workforce development and changes in program SE metrics
<table>
<thead>
<tr>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
</table>
| • "erosion of knowledge, experience and skills" in "systems engineering, project management discipline, cost, schedule management, and technology management". "particularly acute" for systems of systems integration. (NRC Systems Integration for Project Constellation, 2004) | • A systems engineering certification program requiring continual education and training has been institutionalized  
  • just-in-time training via intelligent tutoring and advisory systems  
  • training support using standard NASA and enterprise product and process models  
  • focused training tuned to new opportunities and the best match with different employee skills and working styles | • Technological obsolescence of workforce virtually eliminated by a certified (educated, trained, and experienced) systems engineering staff for engineering, management, and decision making  
  • learning centers at each of NASA’s Collaborative Engineering Environment facilities  
  • university use of collaborative, distributed- learning consortia  
  • practical experience of new engineers using validated system simulations  
  • technological obsolescence of workforce virtually eliminated | • Systems Engineering experience gained through simulation and on-the-job training  
• Advanced Engineering Environment technologies and systems replicated at the university and used for maintaining a strong fundamental core course structure, with simultaneous links to the math and science departments and virtual links to industry and government laboratories  
• national team teaching in engineering, math, science, management, and the humanities  
• personal learning experience emphasized — anytime, anywhere via an advanced Internet with high bandwidth  
• just-in-time personal/virtual training and tutoring |
| • DOD has "essentially eliminated its systems engineering capability". (NRC, 2004) | • courses taught in traditional classrooms  
• some video and Web-based Courses | • "erosion of knowledge, experience and skills" in "systems engineering, project management discipline, cost, schedule management, and technology management". "particularly acute" for systems of systems integration. (NRC Systems Integration for Project Constellation, 2004) | • A systems engineering certification program requiring continual education and training has been institutionalized  
  • just-in-time training via intelligent tutoring and advisory systems  
  • training support using standard NASA and enterprise product and process models  
  • focused training tuned to new opportunities and the best match with different employee skills and working styles |
| • only a single capstone design course in undergraduate engineering | • courses taught in traditional classrooms  
• some video and Web-based Courses | • "erosion of knowledge, experience and skills" in "systems engineering, project management discipline, cost, schedule management, and technology management". "particularly acute" for systems of systems integration. (NRC Systems Integration for Project Constellation, 2004) | • A systems engineering certification program requiring continual education and training has been institutionalized  
  • just-in-time training via intelligent tutoring and advisory systems  
  • training support using standard NASA and enterprise product and process models  
  • focused training tuned to new opportunities and the best match with different employee skills and working styles |

Systems Engineering Tools and Methods
Effect of Requirements Definition Investment on Program Costs

Target Cost Overrun, Percent

Requirements Cost/Program Cost, percent

PAY NOW OR PAY LATER
The Systems Engineering Process
(Ref. ANSI 499)

Process Input
- Customer Needs/Objectives/Requirements
  - Missions
  - Measures of Effectiveness
  - Environments
  - Constraints
- Technology Base
- Output Requirements from Prior Development Effort
- Program Decision Requirements
- Requirements Applied Through Specifications and Standards

Requirements Analysis
- Analyze Missions & Environments
- Identify Functional Requirements
- Define/Refine Performance & Design Constraint Requirement

Functional Analysis/Allocation
- Decompose to Lower-Level Functions
- Allocate Performance & Other Limiting Requirements to All Functional Levels
- Define/Refine Functional Interfaces (Internal/External)
- Define/Refine/Integrate Functional Architecture

System Analysis & Control (Balance)
- Trade-Off Studies
- Effectiveness Analysis
- Risk Management
- Configuration Management
- Interface Management
- Performance Measurement
  - SEMS
  - TPM
  - Technical Reviews

Trade-Off Studies
- Effectiveness Analysis
- Risk Management
- Configuration Management
- Interface Management
- Performance Measurement

Design Loop
- Transform Architectures (Functional to Physical)
- Define Alternative System Concepts, Configuration Items & System Elements
- Select Preferred Product & Process Solutions
- Define/Refine Physical Interfaces (Internal/External)

Verification

Process Output
- Development Level Dependant
  - Decision Data Base
  - System/Configuration Item Architecture
  - Specification & Baseline

Systems Analysis and Simulation drive the entire Systems Engineering Process
IPPD Defined: A management process that integrates all activities from product concept through production/field support, using a multi-functional team, to simultaneously optimize the product and its manufacturing and sustainment processes to meet cost and performance objectives. Its key tenets are as follows:

- Customer Focus
- Concurrent Development of Products and Processes
- Early and Continuous Life Cycle Planning
- Maximize Flexibility for Optimization
- Use of Contractor Unique Approaches
- Encourage Robust Design and Improved Process Capability
- Event Driven Scheduling
- Multidisciplinary Teamwork
- Empowerment
- Seamless Management Tools
- Proactive Identification and Management of Risk
Product Lifecycle Management (PLM)

**Product Life-Cycle Management**
- Systems Requirements
- Configuration Items Specifications
- CAD/CAM Standard Database
- Change/Configuration Management
- Virtual/Real System Models
- V/R Production Models
- V/R Verification Requirements and Management
- V/R Validation Requirements and Management
- Comprehensive Production and Quality History
- Resource Management
- Supply Chain Management
SBSE: The Challenge of Contracted Elements

Fully Integrate Total NASA/Industry Systems Engineering and Management
## Systems Engineering Tools and Gaps

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Gap Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engineering Discipline Tools</td>
<td>Mostly very good for detailed analysis; however needs standards for multidisciplinary integration for design and speed increases for optimization and uncertainty analyses.</td>
<td>Critical Gap</td>
</tr>
<tr>
<td>Specialty Engineering (&quot;ilities&quot;) Tools</td>
<td>Little confidence in prediction of causal relationships for reliability, maintainability, supportability, operability, availability, safety, etc.</td>
<td>Significant Gap</td>
</tr>
<tr>
<td>Life Cycle Cost</td>
<td>NASA has continually underestimated the life-cycle cost (technology, development, production, operations, logistics). Needs causal models to assist engineering system and lifecycle design.</td>
<td>Significant Gap</td>
</tr>
<tr>
<td>Program/Project Management</td>
<td>Many excellent tools available for cost, schedule, and configuration management; needs total integration including risk and engineering mitigation planning</td>
<td>Significant Gap</td>
</tr>
<tr>
<td>Product Life-cycle Management</td>
<td>Many new COTS capabilities are being developed. Need to assess and select for NASA applications. Integration with simulation based SE modeling required. NASA wide and industry integration required.</td>
<td>Significant Gap</td>
</tr>
</tbody>
</table>
Advanced Tools and Processes
- High Fidelity Numerical Simulations
- Non-Traditional Methods
- Rapid Synthesis Methods
- Life Cycle Frameworks
- Life Cycle Cost Simulations
- Risk Simulations

System of Systems
Life-Cycle Simulation and Modeling

Requirements, Flowdown, Trades, Sensitivities, and Validation
- Risk
- Sustainability
- Informed Decisions
- Performance
- Safety
- Reliability

Requirements, Concept Development, Design/Development, Test
- Manufacturing
- Integration/Verification

Ops/Maintenance
Disposal
Integration of risk analysis with decision processes
### Apollo Decision FOM Matrix (1962)

<table>
<thead>
<tr>
<th>Performance</th>
<th>Probability of Success</th>
<th>Schedule</th>
<th>Safety</th>
<th>R&amp;D Costs</th>
<th>Ops Costs</th>
<th>Growth Potential</th>
<th>Delivery Costs</th>
<th>Critical Development Problem Areas</th>
</tr>
</thead>
</table>
| EOR         | 15300                  | Aug 1969 | 18.2   | $6490 E6 | $1240     | 12               | $88.4 E6       | a. Earth orbit rendezvous  
b. propellant transfer  
c. C-5 launch vehicle  
d. standard apollo capsule |
| LOR         | 12,600 5,000 LEM       | Feb 1969 | 16.1 (CM) 22.0 (LEM) | $5840 E6 | $620      | 10*             | $77.4 E6*       | a. lunar orbit rendezvous  
b. LEM and personnel transfer  
c. C-5 launch vehicle  
d. standard apollo capsule |
| C-5 Direct  | 9210                   | Oct 1968 | 16.7   | $5690 E6 | $510      | 12               | $61.4 E6       | a. high energy return  
b. light weight capsule  
c. C-5 launch vehicle |
| Nova Direct | 15300                  | May 1970 | 18.0   | $6160 E6 | $630      | 15               | $55.4 E6       | a. Nova launch vehicle  
b. standard apollo capsule |
Objectives:
- Schedule
- Budget
- Reduce LCC
- Increase Affordability
- Increase Safety
- Increase Sustainability

Customer Satisfaction

Robust Solutions

Objectives:
- Schedule
- Budget
- Reduce LCC
- Increase Affordability
- Increase Safety
- Increase Sustainability

Customer Satisfaction
Technology Trends

Innovation Focus Throughout the Life Cycle

Optimizing the re-use of Data and Corporate Knowledge

Tomorrow's savings
Systems Engineering Evolution

Integrated Virtual and Real Design, Test, Production, and Operations

Knowledge Capture and Management

Product Life-Cycle Modeling

Integrated SE Processes

Manual SE Integration

Design & Manufacturing

3D Collaboration Tools

VPM

PPR

Knowledge Inside

3D

2D

• Early Requirements Development

• Analysis of Alternatives

• Reconfigurable Designs

• Real/Virtual Integration

• Human/Machine Performance

• Safety, Reliability, Cost Trades

• Systems of System Integrated Performance and Decision Analysis

Rapid Validation of Virtual Models for Confident Decision Analysis
Define, Monitor, and Control the Physical World

VIRTUAL

Product & Process Knowledge

INTELLECTUAL PROPERTY

REAL OPERATIONS

PHYSICAL

Production
• Design is Authored as Models

• Simulation Verifies the Design

• Physical Test Verifies the Simulation

Better Decisions / Shorter Development Times
Validated virtual simulation may compensate for lack of physical Systems Engineering experience.
Simulation Based Modeling (SBM) Build Progression

1. Subjective Assessments
   - QFD / AHP
   - System Engineering Tools

2. Engineer in the Loop
   - Conceptual/Prelim Engineering
   - Risk – Flight, Development, RMS
   - Cost – Complete Life-Cycle

3. Operator in the Loop
   - Ground Operations
   - Mission Operations
   - Supply Chain Management

4. Hardware/Software in the Loop
   - Test Program Def & Refinement
   - Hardware & Software Testing
   - System Integration Modeling

5. Pilot in the Loop
   - Ground and Flight Sims
   - Validate Engr Concepts & Techs

6. Manufacturer/Tester in the Loop
   - Technology / Producibility Plan
   - Factory Layout / Tooling
   - Virtual/Real Test Integration
A geographically distributed, integrated, secure, collaborative environment which enables life cycle design and analysis capability, enabling world-class engineering and science applications.
### Modeling Management Structure
For STS Logistics, Management and Planning ~70%

**Direct (Visible) Work**
- "Tip of the Iceberg"

**Support (Hidden)**
- Recurring Ops

---

#### STS Budget "Pyramid"
**(FY 1994 Access to Space Study)**

<table>
<thead>
<tr>
<th>Generic Operations Function</th>
<th>Total $M FY94</th>
<th>Total (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elem. Receipt &amp; Accept.</td>
<td>1.4</td>
<td>0.0%</td>
</tr>
<tr>
<td>Landing/Recovery</td>
<td>19.6</td>
<td>0.6%</td>
</tr>
<tr>
<td>Veh Assy &amp; Integ</td>
<td>27.1</td>
<td>0.8%</td>
</tr>
<tr>
<td>Launch</td>
<td>51.5</td>
<td>1.5%</td>
</tr>
<tr>
<td>Offline Payload/Crew</td>
<td>75.9</td>
<td>2.3%</td>
</tr>
<tr>
<td>Turnaround</td>
<td>112.3</td>
<td>3.3%</td>
</tr>
<tr>
<td>Vehicle Depot Maint.</td>
<td>237.5</td>
<td>7.1%</td>
</tr>
<tr>
<td>Traffic/Flight Control</td>
<td>199.4</td>
<td>5.9%</td>
</tr>
<tr>
<td>Operations Support Infra</td>
<td>318.6</td>
<td>9.5%</td>
</tr>
<tr>
<td>Concept-Uniq Logistics</td>
<td>842.7</td>
<td>25.1%</td>
</tr>
<tr>
<td>STS Ops Plan’g &amp; Mgmt</td>
<td>1477.4</td>
<td>43.9%</td>
</tr>
<tr>
<td><strong>Total ($M FY94)</strong></td>
<td><strong>3363.4</strong></td>
<td><strong>100.0%</strong></td>
</tr>
<tr>
<td>Percent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

CM McCleskey/NASA KSC
Management and Organization integration is a major percentage of program costs.

Information flow, decision paths, and process graphs can be stochastically modeled for duration, human capital, and impact on total program costs.

Currently, no organizational model has been developed to analyze NASA program organizational performance.

Validated organizational simulations may have as much impact as system simulation and optimization.
<table>
<thead>
<tr>
<th>Steps in the Design and Development of Products and Processes</th>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
</table>
| 1. Mission Requirements Analysis/Product System Strategy     | • traditional systems engineering methods / non-standard application across NASA  
• little integration and reuse of engineering analyses  
• late trades of requirements versus system specs, performance, and cost | • establishment of NASA-wide policy and guidelines for systems engineering  
• integrated life-cycle analysis tools for system and requirements trades for acquisition | • integrated systems engineering and management systems for technical and programmatic risk  
• validated life-cycle simulation of all mission requirements  
• seamless transitioning of technical simulations to management and control simulation  
• systems of systems requirements are understood and validated | • all life-cycle engineering functions are seamlessly integrated for system design, development, manufacture, and operation  
• all mission and enterprise requirements can be traded with functional and physical models for the systems of systems environment  
• complete emersion of stakeholder in the design/requirements process |
| 2. Product Specification                                     | • competitive comparisons  
• projections of future products  
• interviews and focus groups of customers and others  
• demonstrations  
• output is written documentation | • complete linkage of customer requirements, functional requirements, physical architecture, and operational requirements  
• virtual prototypes for specification validation  
• strategic decision models and analyses based on uncertainty and risk  
• product life-cycle model for management of complete digital product database | • knowledge base for construction of systems analyses for a proposal with a "selected" level risk  
• reliable specifications even for first-of-a-kind products  
• systems of systems impact of specifications are known | • reliable “batch of one” methods for unique products  
• product created on demand  
• ability to write in preferences and requests  
• maximum reuse of hardware, software, infrastructure, and knowledge for the enterprise |

### Systems Engineering Tools and Methods Assessment and Vision

<table>
<thead>
<tr>
<th>Steps in the Design and Development of Products and Processes</th>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
<tbody>
<tr>
<td>3. Concept Development</td>
<td>• target setting</td>
<td>• integrated, predictive life-cycle cost and profitability models</td>
<td>• complete life-cycle optimizations trading safety, performance, life-cycle cost, technical/performance risk, and schedule</td>
<td>• concept is optimized to meet mission and enterprise requirements (hardware, software, and knowledge reuse known)</td>
</tr>
<tr>
<td></td>
<td>• brainstorming on product and process alternatives</td>
<td>• expert opinion for concept initiation</td>
<td>• full automation of subsystem and component tracking and trade-offs</td>
<td>• sensitivities, robustness, uncertainties are automatically generated for decision analysis</td>
</tr>
<tr>
<td></td>
<td>• development of product and process concepts</td>
<td>• rules of thumb</td>
<td>• collaborative engineering environment for complete enterprise participation in engineering and management with contractors</td>
<td>• expert system generates alternatives</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• innovation relies on experienced practitioners</td>
<td>• virtual prototyping for manufacturing, integration, testing, ground and fight operations</td>
<td>• optimized, top-down concept development process</td>
</tr>
</tbody>
</table>

Steps 3, 4, and 5 combined

- **Steps 3, 4, and 5 combined**
  - concept is optimized to meet mission and enterprise requirements (hardware, software, and knowledge reuse known)
  - sensitivities, robustness, uncertainties are automatically generated for decision analysis
  - expert system generates alternatives
  - optimized, top-down concept development process
  - automatic analytical evaluation of all product and process attributes (including risk and uncertainty)
  - global collaborative engineering environment

<table>
<thead>
<tr>
<th>Steps in the Design and Development of Products and Processes</th>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-Year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>4. Preliminary Product and Process Design</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• high-level definition of product and process designs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• evaluation of product and process designs vs. targets</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• high-level system trade-offs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• iterative, largely manual, largely bottom-up, heuristic</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• derivations of existing designs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• progressive definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• coarse definition, mostly manual from scratch</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• unequal levels of definition for new and reused parts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 20% of product and process attributes evaluated analytically using simplified models</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• reliance on physical prototypes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• rapid iteration of product and process design</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• object-oriented models scalable from macro to micro levels</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• single interoperable data set</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• automated process model creation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• analytical evaluation of all attributes, including cost</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• full automation of subsystem and component tracking</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• virtual manufacturing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 20% of product and process attributes evaluated analytically using simplified models</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• some degree of iteration implied, but guided by optimization capability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• analytical evaluation of all attributes, 200 to 300 times faster than current methods</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• integrated; single data source</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• full automation of subsystem and component tracking and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• virtual manufacturing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• single-pass product and process design and concurrent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• automated generation of details about component and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• single product life-cycle data source</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• single-pass product and process design and concurrent</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• virtual manufacturing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• single product life-cycle data source</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Steps in the Design and Development of Products and Processes</th>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Refinement and Verification of Detailed Product and Process Designs</td>
<td>• detailed process and product definition mostly manual and from scratch</td>
<td>• distributed, collaborative processes within NASA</td>
<td>• automatic configuration control and tracking of system and processes</td>
<td>• automatic verification of the system and processes generated within the NASA advanced engineering environment</td>
</tr>
<tr>
<td>• development of designs for components, subsystems, and manufacturing processes</td>
<td>• limited reuse of design geometries for new parts</td>
<td>• physical prototypes essentially eliminated</td>
<td>• distributed, collaborative processes (NASA and contractors)</td>
<td>• immersive design and evaluation environment from the total NASA/contractor engineers, managers, and decision makers</td>
</tr>
<tr>
<td>• geometry creation</td>
<td>• analytical evaluation of one-third of product and process attributes using detailed models</td>
<td>• real-time sharing of design information</td>
<td>• design advisors</td>
<td>• international distributed, collaborative processes</td>
</tr>
<tr>
<td>• prediction and evaluation of all product and process attributes</td>
<td>• some model sharing</td>
<td></td>
<td>• minimal, “surgical” testing</td>
<td></td>
</tr>
<tr>
<td>• tracking and trade-offs of subsystems and components</td>
<td>• reliance on physical prototypes</td>
<td>• no late trade-offs and no errors</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• attribute prediction and evaluation partially automated, but not integrated with design evolution</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Steps in the Design and Development of Products and Processes</th>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-Year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6. System Prototype Development</strong></td>
<td>• analytical evaluation required for more than half of all product attributes</td>
<td>• integrated database for development of rapid prototypes</td>
<td>• complete virtual prototyping of system, systems, manufacturing, integration, tests, and operations</td>
<td>• validated virtual models - limited experiments required</td>
</tr>
<tr>
<td>• experimental refinement of product attributes that do not meet targets</td>
<td>• real and virtual prototypes available for form, fit, and function demonstrations and tests</td>
<td>• virtual prototypes becoming the norm for NASA</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7. Production, Testing, Certification, and Delivery</strong></td>
<td>• virtual shop floor modeled</td>
<td>• product life-cycle model used to integrate production with resources, supply chain, workforce, and management</td>
<td>• all production hardware, software, infrastructure, workforce, and processes developed and tested virtually</td>
<td>• complete integrated virtual environment for supply chain, production, integration, verification, and validation</td>
</tr>
<tr>
<td>• discrete event optimized production flow</td>
<td>• on-line statistical process control</td>
<td>• products with 100% quality—getting it right the first time</td>
<td>• complete supply chain modeled and integrated with production</td>
<td>• virtual design and manufacturing process with zero defects</td>
</tr>
<tr>
<td>• on-line statistical process control</td>
<td></td>
<td></td>
<td>• off-line robust design</td>
<td>• only minor facility reconfigurations required for single product runs</td>
</tr>
</tbody>
</table>
### Systems Engineering Tools and Methods
#### Assessment and Vision

**Steps in the Design and Development of Products and Processes**

<table>
<thead>
<tr>
<th>Typical Today</th>
<th>5-Year Vision</th>
<th>10-year Vision</th>
<th>15-Year Vision</th>
</tr>
</thead>
</table>
| 8. Operation, Support, Decommissioning, and Disposal | • sequential, historically based modeling approach  
• a lot of manual operations | • consideration of remanufacturing in design  
• limited autonomous systems  
• simulation models based on operational processes  
• improved automation of support activities  
• supply chain modeled for impacts on design | • autonomous systems  
• operations driven supply chain fully modeled and managed  
• design for easy repair  
• design for disassembly  
• design for reuse and remanufacture | • autonomous systems  
• self-healing  
• self-disassembly  
• self-disposal |

Capability 15.1 Systems Engineering Roadmap

Key Assumptions: Exploration & Science

2008 CEV Initial Flight
2011 James Webb
2013 Comet Surface Sample Return
2015 Prepare for Human Lunar Missions

Capability Roadmap 15: Systems Engineering Risk/Cost Analysis

Initial Life-Cycle Management Capability
Integrated System Engineering and Management Capability
Collaborative/Distributive PLEM Simulation-Based Capability

15.1 Systems Engineering Implementation

15.1.1 Processes
15.1.2 Skills
15.1.3 Tools and Methods

NASA HQ SE Policy
SE Certification Policy & Program
Initial PLM Implementation

NASA HQ SE Standard With Systems of Systems
NASA HQ SE Guidelines
Integrated SE, PM, & RM (CMMI Level 3)
Integrated SE Environment
Validated, Integrated SE Environment
Distributed SE’s Throughout NASA
Collaborative/Distributive PLEM Simulation-Based Capability

Initial SE Implementation
Initial Certified Class
Validated PLM
SBM Build 1 SBM Build 2

Integrated System Engineering and Management Capability
Initial SKilled SE Architects
CMMI Level 5
Integrated PLM
Hardware in Loop SBM Build 4
Pilot in Loop SBM Build 5

Systems of Systems
SBM Build 3

Legend
PLM – Product Life Cycle Management
SBM – Simulation Based Modeling
CMMI – Capability Maturity Model Integration
QRA - Quantitative Risk Assessment
LCC - Life Cycle Cost

Major Decision
Major Event / Accomplishment / Milestone
Ready to Use
Key Assumptions: Exploration & Science

2018 Deep Drill & Completed Initial Human Landing

2025 Extended Lunar Capability & Life Finder Telescope

2030 Prepare for Human Mars Mission

Capability Roadmap 15: Systems Engineering Risk/Cost Analysis

Initial International Collaborative Engineering / Management Simulation Based Capability

Legend
PLM – Product Life Cycle Management
SBM – Simulation Based Modeling
CMMI – Capability Maturity Model Integration
QRA - Quantitative Risk Assessment
LCC - Life Cycle Cost

15.1 Systems Engineering

15.1.1 Processes
International SE Standards

15.1.2 Skills
International Certified SE’s

15.1.3 Tools and Methods
Validated SE L5 PLM Environment

International Collaborative Total PLM Environment

15.1 Systems Engineering Risk/Cost Analysis

Legend
Major Decision
Major Event / Accomplishment / Milestone
Ready to Use

2020

2025

2030
Summary

- Systems Engineering in NASA needs to be improved for large complex systems of systems projects

- Standard system engineering policy needs to be developed at the Agency level for guidance to Centers

- The training and education of systems engineering needs to be institutionalized

- Advanced Engineering Environment can greatly enhance program execution, workforce training, and search for innovation and improved science
Capability - 15.2 Life Cycle Cost

Presenter:
Dr. David Bearden
What is a Life Cycle Cost (LCC)?

• An integrated, process-centered, and disciplined approach to life cycle management of projects provides real and tangible benefits to all project stakeholders.

• A LCC estimate includes total cost of ownership over the system life cycle, all project feasibility, project definition, system definition, preliminary and final design, fabrication and integration, deployment, operations and disposal efforts.

• A LCC estimate provides an exhaustive and structured accounting of all resources necessary to identify all cost elements including development, deployment, operation and support and disposal costs.

* Definitions provided by the NASA Cost Estimation Handbook, 2004
Benefits of the Life Cycle Cost

- “Ensure cost realism and accuracy”
  - The President’s Commission

- Improve confidence in selection process
  - Enables better budgeting

- Predict cost impact of change

- Limit potential for significant overruns
  - Increases mission success

- Gauge economic impact of decisions
Cost Team Process

• Evaluated current Capability Readiness Level (CRL) of cost discipline, at the lowest cost team WBS level
  – Cost Analysts at NASA HQ, MSFC, JPL, SAIC and The Aerospace Corporation evaluated the readiness level and importance of the current State of the Practice
  – Scored Robotic Spacecraft and Human Space Flight separately

• Interviewed Agency cost estimating leaders for current status / initiatives

• Identified remaining near-term gaps after implementation of current initiatives
  – Recommended additional measures for near-term

• Envisioned ideal state for cost estimating
  – Five and twenty year horizons
Current State-of-the-Practice for Life Cycle Cost

• Tools
  – Primarily system level parametric models with broad application
  – Medium fidelity models for development and operations
  – Low fidelity requirements (Physics) based models for instruments
  – High fidelity component models limited in application
  – Immature technology development capability
  – Scattered, sparsely-populated databases deployed across centers and industry
  – Databases with limited content, pre full-cost accounting and not normalized

• Skills
  – Limited formal cost training in academia
  – Limited career path

• Process
  – Program costs rolled up from several models
  – Costs validated through comparison of bottom’s up to parametric (top down)
  – Periodic intersection of cost estimation with project development
  – Immature linkage to Schedule Analysis
  – Minimal understanding of relationship of LCC to mission risk and safety
**Maturity Level** – State of the Practice for 15.2 Life Cycle Cost

### Robotic Spacecraft

<table>
<thead>
<tr>
<th>Estimate Life Cycle Cost</th>
<th>Tools</th>
<th>Skills</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Maturation</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Development</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Production</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Operations</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

### Human Spaceflight

<table>
<thead>
<tr>
<th>Estimate Life Cycle Cost</th>
<th>Tools</th>
<th>Skills</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology Maturation</td>
<td>Yellow</td>
<td>Green</td>
<td>Yellow</td>
</tr>
<tr>
<td>Development</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Production</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Operations</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
</tbody>
</table>

Results indicate a strong need for Technology Maturation Cost Estimation Capabilities
Observations on Maturity

- Capability ratings trended higher for Robotic Spacecraft than Human Spaceflight primarily because of better data availability (function of more recent, relevant missions)
- Capability ratings for Technology maturation cost estimating low in all areas
- Production and Development estimating limited by data available in Human Spaceflight area
- Operations cost estimating readiness low due to less mature tools and processes and availability of fewer estimators
Missions Driving Requirements
  - Primarily driven by ESMD
    • Prometheus
    • Crew Exploration Vehicle
    • Human Exploration of Moon/Mars
  - Large SMD Projects
    • James Webb Space Telescope
  - Scale of large ESMD and SMD projects increases budgetary impact of overruns, poor estimation, and requirements creep

Additional reports that drive capability
  - NPR 7120.5C
Elements of LCC Roadmap

• **Tools**
  – One NASA Cost Engineering (ONCE) Database
  – Technology Development Estimation Capability
  – Integrated Cost, Risk, & Schedule Models
  – Integrated Life Cycle Models with Improved Operations Models
  – Requirements (Physics) based Models
  – Economic Modeling

• **Skills**
  – Continuous Development
  – Formal Academic Education

• **Process**
  – CADRe (Cost Analysis Data Requirement) feeds data to ONCE
  – CCRM (Continuous Cost Risk Management)
  – Standard WBS
  – CAIG-like (Cost Analysis Improvement Group) implementation
“Enable a more agile cost estimating capability that interacts effectively with the project management function”

- **Improved models**
  - Representative Initiative: Integrated Life Cycle parametric system level models
  - Remaining Gap: Importance of accurate cost information justifies more investment to build higher fidelity integrated models

- **Improved database**
  - Representative Initiative: CADRe -> ONCE
  - Remaining Gap: Better coordination and cooperation by data owners (data sharing by centers/involved parties), data availability is a long-term problem

- **Enhanced process to enable use of LCC estimating as an input to the project management function**
  - Representative Initiative: CCRM
  - Remaining Gap: CCRM implementation will be challenging
Capability 15.2 Life Cycle Cost Roadmap

Key Assumptions: Exploration & Science

2008 CEV Initial Flight
2011 James Webb
2013 Comet Surface Sample Return
2015 Prepare for Human Lunar Missions

Capability Roadmap 15: Systems Engineering Risk/Cost Analysis

15.2 Life Cycle Cost
Agency-wide LCC Models & Process
Continuous Cost Risk Management
Integrated Life Cycle Cost Models
Life Cycle Cost linked to Project Management

15.2.1 Tools
ONCE start
Current Center Databases Linked
ONCE IOC
Industry Databases Linked
Expanded ONCE IOC
Initial Integrated LCC Tool

15.2.2 Skills
Training program established
Experienced team at HQ
Expanded teams at Centers

15.2.3 Process
CADRe & CCRM start
Std. WBS
Continuous Cost Risk Management Established
Expanded CADRe Start

15.2 Life Cycle Cost
Key Assumptions:
Exploration & Science

2005
2010
2015

Major Decision
Major Event / Accomplishment / Milestone
Ready to Use

Academic Offering Cost in SE Curriculum

 pololeds Plem Simulation-Based Capability
“Create a cost estimating capability that simulates the economic system and interacts seamlessly with management and systems engineering throughout the project”

- Understand the whole economic system and simulate to understand the effects of design and programmatic decisions have at the industry base level
  - Model not only design solution, but economic business case for industry

- Link the project management and systems engineering process with cost analysis
  - Simulate technology changes, process changes, etc.

- Improve tools and databases to allow for high-fidelity analysis
  - Cost as a function of safety, risk, schedule, and technology
Capability 15.2 Life Cycle Cost Roadmap

Key Assumptions:
- Exploration & Science

2018
- Deep Drill & Completed Initial Human Landing

2025
- Extended Lunar Capability & Life Finder Telescope

2030
- Prepare for Human Mars Mission

Capability Roadmap 15: Systems Engineering Risk/Cost Analysis

15.2 Life Cycle Cost

Decisions based on Economic LCC Models

Linked LCC Models for all phases of project

Open Economic based LCC models

Higher Fidelity Databases Available

LCC Skills readily available

Continuous cost risk analysis broadly used within agency

LCC used for all Agency decisions

2020
- Deep Drill & Completed Initial Human Landing

2025
- Extended Lunar Capability & Life Finder Telescope

2030
- Prepare for Human Mars Mission

Major Decision

Major Event / Accomplishment / Milestone

Ready to Use
## Life Cycle Cost Goals

<table>
<thead>
<tr>
<th>Capability</th>
<th>Year 5</th>
<th>Year 10</th>
<th>Year 25</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MODELS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost Accuracy</td>
<td>30%</td>
<td>20%</td>
<td>10%</td>
</tr>
<tr>
<td>Schedule Accuracy</td>
<td>30%</td>
<td>20%</td>
<td>10%</td>
</tr>
<tr>
<td><strong>DATABASE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of Programs w/ Complete CADRe</td>
<td>50%</td>
<td>90%</td>
<td>100%</td>
</tr>
<tr>
<td><strong>SKILLS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% Staff w/ Formal Training within NASA</td>
<td>50%</td>
<td>75%</td>
<td>90%</td>
</tr>
<tr>
<td><strong>PROCESS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% Programs implementing full CCRM process</td>
<td>30%</td>
<td>60%</td>
<td>90%</td>
</tr>
</tbody>
</table>
Summary

- Evaluated current capability of cost estimation discipline
- Envisioned ideal future state for cost estimating
- Performed gap analysis taking into account current initiatives
- Developed roadmap from current state-of-practice to envisioned state
Capability – 15.3 Risk Management

Presenter:
Theodore Hammer
• Risk Management identifies potential problem areas early enough to allow development and implementation of mitigation strategies. This includes contingency planning, descope approaches, and qualitative and quantitative assessments. As complexity of systems grows the importance of risk analysis increases in managing cost, schedule and mission success.

• The Risk Management sub-element needs to be thoroughly integrated with other aspects of systems engineering

• Risk management includes tools, processes, and skills
Key Points/Benefits

- Risk Management most effective when integrated with program/project and technical management

- Gaps exist within the present risk management state of the practice

- First End State targets elimination of existing gaps

- End States target delivery of capabilities five years prior to a milestone

- Regular evaluation critical

- A formal integrated risk management capability benefits implementation of highly complex systems by
  - Enabling cost effective implementation and problem avoidance
  - Increasing probability of mission success
  - Reducing programmatic problems (e.g., cost and schedule)
Current State-of-the-Practice for Risk Management Within NASA

- Risk Management policy and requirements exist
- Conduct annual NASA Risk Management conference
- Risk Management planning widely used
- Assessments are highly qualitative
- Quantitative assessments using such tools as PRA are limited
- Risk mitigation planning and implementation widely used, but not well integrated into the project planning (e.g., cost/work breakdown, integrated schedules)
- Various risk management tools have been used, however, based on NASA trade studies ESMD has selected a state-of-the-art risk tool as the Directorate standard: Active Risk Manager (Strategic Thought, LLP)
- Formal risk management training exists based on Software Engineering Institute risk management process

Evaluation based on OSMA and NASA Center RM POC assessments.
<table>
<thead>
<tr>
<th>Risk Management</th>
<th>Skill</th>
<th>Tool</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepare for Risk Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Determine Risk Sources and Categories</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define Risk Parameters</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establish a Risk Management Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify and Analyze Risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identify Risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantitative</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qualitative</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate, Categorize, and Prioritize Risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Track/Control/Communicate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mitigate Risks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Risk Mitigation Plans</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement Risk Mitigation Plans</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Critical Gap
Significant Gap
No or Minor Gap
**Gaps**

- **Prepare R**
  - Insufficient level of integration of risk management and risk assessment with other capabilities
  - Lack of regular collection of data to assess the level of compliance and practice of risk management and assessment
  - Limited skill, tools and process for in-depth identification of risk sources
  - Limited skill, tools and process for an integrated risk strategy
- **Identify R**
  - Lack of standardization in risk management tools used
  - Inconsistent level of skill and knowledge for Risk Management practitioners
  - Insufficient application of quantitative techniques to identify risks, and limited qualitative assessment skills
  - Insufficient skills and tools for a consistent approach to monitoring, tracking, control/feedback and communication (e.g., external) of risks
- **Mitigate Y**
  - Limited skill and tools for mitigation planning
  - Limited skill, tools and process for the implementation of mitigation activities
Requirements/Assumptions for 15.3 Risk Management

- Key Assumption is capability to support key milestones must be in place 5 years prior:
  - 2011 James Webb Telescope
  - 2015 Prepare for Human Lunar Missions
  - 2018 Initial Human Lunar Landings
  - 2025 Extended Lunar Capability
  - 2030 Prepare for Human Mars Mission

- Requirements and assumptions for increased risk management capabilities
  - Increased complexity of systems
  - Increased inter-dependency of complex systems
  - Distributed implementing organizations
  - Environment uncertainty
  - Longer mission durations/complex logistics requirements
  - Tougher science requirements
  - Challenge of implementation and verification of advanced instrument technology (e.g., increased detector sensitivity)
  - Increase future IT capabilities at lower costs
FY 2010 Lunar Support

• **Prepare**
  – Change process and skills to effect integration of risk management
  – Regular collection of self assessment data
  – Institute skills, tools and process for:
    • In-depth identification of risk sources
    • Integrated risk strategies

• **Identify**
  – Standardize risk management tools used
  – Define skills/knowledge criteria for risk practitioners; conduct training
    • Including quantitative techniques
  – Institute skills, tools: Monitoring, tracking, control/feedback and communication (e.g., external) of risks

• **Mitigate**
  – Institute skill and tools for mitigation planning
  – Institute skill, tools and process for the implementation of mitigation activities
Integration of risk analysis with decision processes

Risk-informed Decision-making
(Integrated Consideration of all Performance Measures and Deliberation)

TECHNICAL RISK

INTEGRATION OF QUALITATIVE AND QUANTITATIVE SYSTEM SAFETY ANALYSIS

Risk Metric (Loss of Crew)  Risk Metric (Loss of Science)  Risk Metric (Injury to Public)

FM EFFECT CR
Device A Fails Loss of X 1
Device B Fails Loss of Y 3

Performance Measures
(Quantities of Interest to Decision-Maker)

Key Uncertainties

Decision Option
FY 2014 Human Lunar Landing Support

• **Prepare**
  – Improved risk source identification; expanded to include routine operational environment challenges
  – Risk sensitivity analysis for interdependent complex systems

• **Identify**
  – Simulation-based risk identification
  – Increased depth and fidelity of quantitative techniques
  – Improved risk communication, including risk uncertainties

• **Mitigate**
  – Integration of mitigation activities into project schedules
End States (Continued)

FY 2020 Extended Lunar Support

• **Prepare**
  – Risk sensitivity analysis techniques for interdependent systems
  – Improved risk source identification; plans for expanded extended lunar operational environment challenges

• **Identify**
  – Predictive risk capability and tools
  – Interactive risk identification; knowledge based providing a connection to risk decisions made in the past

• **Mitigate**
  – Capture of risk mitigation successes/failures to predict mitigation approach probability
FY 2025 Human Mars Support

• **Prepare**
  – Improved risk sensitivity analysis techniques for interdependent complex systems
  – Improved risk source identification; plans for expanded Mars operational environment challenges

• **Identify**
  – Improved predictive risk capability and tools
Capability 15.3 Risk Management Roadmap

Key Assumptions: Exploration & Science

**2008 CEV Initial Flight**

**2011 James Webb**

**2013 Comet Surface Sample Return**

**2015 Prepare for Human Lunar Missions**

**Capability Roadmap 15: Systems Engineering Risk/Cost Analysis**

Integrated Risk Tools and Mitigation plans

Integrated System Engineering and Management Capability

Collaborative/Distributive PLEM Simulation-Based Capability

15.3 Risk Management

15.3.1 Prepare

Integrated Risk Process

Data base of Self Assessment Established

Generic Risk Strategies Data Base Developed

Operational Environment included in Risk Analysis

15.3.2 Identify

Risk ID Tools Developed

Standardized Risk Tools Used

Simulation Based Risk Identification

Probabilistic/Sensitivity Analysis Risk Identification

15.3.3 Mitigate

Risk Mitigation Plans Routinely Used

Risk Mitigations Tracked against Identified Risks

Risk Mitigations Integrated into Project Schedules

Legend
PLM – Product LC Management
SBM – Sim. Based Modeling
CMMI – Capability Maturity Model Integration
QRA - Quantitative Risk Assessment

Major Event / Accomplishment / Milestone

Major Decision

Ready to Use
Capability 15.3 Risk Management Roadmap

Key Assumptions: Exploration & Science

2020
- 15.3.1 Prepare
- 15.3.2 Identify
- 15.3.3 Mitigate

2025
- 15.3.1 Prepare
- 15.3.2 Identify
- 15.3.3 Mitigate

2030
- 15.3.1 Prepare
- 15.3.2 Identify
- 15.3.3 Mitigate

Legend:
- PLM – Product LC Management
- SBM – Sim. Based Modeling
- CMMI – Capability Maturity Model Integration
- QRA - Quantitative Risk Assessment

15.3.1 Prepare
- Interdependent Systems Risk analysis
- Extra-terrestrial operational environments included in risk analysis
- Interdependent System of Systems Risk analysis

15.3.2 Identify
- Predictive tools/Processes
- Interactive Risk Identification
- Project-based Real-time risk identification and mitigation

15.3.3 Mitigate
- Generic Risk Mitigations data base developed
- Interactive Risk Identification and Mitigation
- Accurate Risk Analysis in Uncertain Environments

Major Event / Accomplishment / Milestone
- Ready to Use

- 2018 Deep Drill & Completed Initial Human Landing
- 2025 Extended Lunar Capability & Life Finder Telescope
- 2030 Prepare for Human Mars Mission
## Maturity Goals

### RISK MANAGEMENT

#### Prepare for Risk Management

<table>
<thead>
<tr>
<th>Objective</th>
<th>2009</th>
<th>2015</th>
<th>2020</th>
<th>2025</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change process and skills to effect integration of RM</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Regular collection of self assessment data</td>
<td>1/YR</td>
<td>1/YR</td>
<td>1/YR</td>
<td>1/YR</td>
</tr>
<tr>
<td>Institute skills, tools and process</td>
<td>80%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Improved risk source identification</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Risk sensitivity analysis for interdependent complex systems</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Sensitivity analysis techniques for interdependent complex systems</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Improved risk source id; extended lunar operations</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Improved risk source identification; expanded Mars ops</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

#### Identify and Analyze Risks

<table>
<thead>
<tr>
<th>Objective</th>
<th>2009</th>
<th>2015</th>
<th>2020</th>
<th>2025</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardize risk management tools used</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Define skills/knowledge criteria for risk practioners</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Institute skills, tools: Monitoring, tracking, control/feedback and communication</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Simulation-based risk identification</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Increased depth and fidelity of quantitative techniques</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Improved risk communication, including risk uncertainties</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Predictive risk capability and tools</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Interactive risk identification; knowledge based connection to risk decisions made in the past</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Improved predictive risk capability and tools</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>

#### Mitigate Risks

<table>
<thead>
<tr>
<th>Objective</th>
<th>2009</th>
<th>2015</th>
<th>2020</th>
<th>2025</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institute skills and tools for mitigation planning</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Institute skill, tools and process for the implementation of mitigation activities</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Integration of mitigation activities into project schedules</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Capture of risk mitigation successes/failures to predict mitigation approach probability</td>
<td>6</td>
<td>7</td>
<td>7</td>
<td>7</td>
</tr>
</tbody>
</table>
Risk Management most effective when integrated with program/project and technical management.

First End State targets achieving RM integration with program/project and technical management, and elimination of existing gaps.

End States target delivery of capabilities five years prior to milestone that would benefit most from those capabilities.

Regular evaluation critical to determining capability maturity and success in meeting end state objectives.
Capability - 15.4 Safety & Reliability Analysis

Presenter:
Homayoon Dezfuli, Ph.D, NASA
Team Lead
Objectives of System Safety & Reliability Analysis

- Evaluation and management of
  - Safety risk
  - Mission success

- Includes processes and techniques used to provide organized, disciplined approach to:
  - Identify and resolve risks as effectively as possible
    - Personnel
    - Equipment
    - Mission success
  - Assess safety and reliability through all phases of the life cycle
  - Risk-informed management of safety & reliability

- Assessment tools and processes should provide integrated evaluation of the entire system:
  - Hardware
  - Software
  - Physical environments
  - Operations
  - Human
  - Interactions of systems
Ensuring Safety and Mission Success in an Ideal Decision-making Framework

The Focus of this Presentation

PREREQUISITE: A SAFETY CULTURE IN WHICH MISSION OBJECTIVES ARE CLEARLY STATED AND PROMOTES QUALITY, ACCOUNTABILITY, COLLABORATION, AND COMMUNICATION.
Benefits of Safety & Reliability Analysis

- Benefit: Ensure safety and mission success while affordably meeting program objectives

- This benefit will be realized when safety, reliability and risk analyses are standardized and are integrated with decision processes under a single decision-making framework
  - Integrate information on safety, reliability and risk under one umbrella (integration)
    - Elimination of organizational and process barriers
  - Systematize the hazard identification process (modeling standardization)
  - Analyze safety and mission risk (measurement of safety and mission performance)
    - Assessment of aggregate risks
    - Identification of weaknesses and vulnerabilities
    - Identification and assessment of uncertainties
  - Manage safety and mission risk (decision-making)
    - Performance of trade-off studies
    - Development of risk reduction strategies
• **Hazard analysis is widely used**
  – Focuses on specific contributors
  – Limited applicability to complex systems-of-systems
    • generally the result of brainstorming

• **Fault Tree Analysis and Failure Modes and Effects Analysis are widely used**
  – Typically applied when completed design information is available
  – Primarily applied at subsystem level
  – Limited ability to affect early design decisions

• **Risk Matrix is widely used**
  – Applied to top-level risk issues
  – Interaction between risk items is difficult to discern
  – Is unsuitable for combining risks to obtain aggregate risk
  – Uncertainties are not formally accounted for
Example Application of Risk Matrix

A Typical State-of-Practice System Safety Assessment Technique

- Analyst postulates a failure or a deviation and assesses its consequences
  - Typically one failure or deviation is analyzed at a time
- Analyst qualitatively judges how often a failure or deviation can occur
- Analyst qualitatively judges the severity of the outcome or assumes the worst-case outcome
- Analyst maps each analyzed failure into one of three risk categories (Green, Yellow, Red)
Current State-of-the-practice for 15.4 Safety & Reliability Analysis (Cont.)

- The state-of-practice safety analyses do not readily reveal whether safety is improving, declining or staying the same.
  - Not designed to measure safety.
  - Without safety performance measures (safety risk metrics) one cannot manage safety risk design and operational system.

System safety and risk analyses are organizationally remote from design.
They are add-on to traditional engineering analysis.
“System safety engineering and management is separated from mainstream engineering, is not vigorous enough to have an impact on system design, and is hidden in the other safety disciplines at NASA Headquarters.”
NASA has begun applying probabilistic risk assessment (PRA) techniques for evaluating safety performance

- PRA is shown to be an effective tool
  - To integrate qualitative and quantitative safety models
  - To quantify risk metrics relating to the likelihood and severity of events adverse to safety or mission success including gaining an understanding of uncertainties

Probabilistic risk models have not yet been used for design decisions

- Models for software-intensive systems, unique space environment, and human decision-making and human-automation interactions have not been fully developed
- Model developments are hampered by lack of PRA skills and limited and fragmented safety-related reliability databases
Robust and effective Safety and Reliability Assessment will be necessary to safely and affordably meet all the goals in the mission framework:

- ~ 14 launches FY05 - FY10 (not including Shuttle and ISS)
- Over a hundred launches between FY10 - FY 30
- Planetary missions using nuclear technology
- Human mission to Mars by 2030
- Sample & return missions to Mars in 2014
- Potential for 3 month stay on the Moon
- Complex science missions (telescopes and solar exploration)

Not limited to human safety and crew survival,

- Must include loss of mission, loss of equipment, and adverse environmental impacts
# Maturity Level – Capabilities for 15.4 Safety & Reliability Analysis

<table>
<thead>
<tr>
<th>Risk and Safety Management</th>
<th>Skills</th>
<th>Tools</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Tradeoffs, Risk Acceptance and Risk Communication</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Appreciation and Quantification of Uncertainties</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Mishap Investigation</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Trend and Precursor Analysis</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Dissemination of Lessons Learned</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Systems Safety</th>
<th>Skills</th>
<th>Tools</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualitative Systems Safety Analysis (hardware, software, phenomenological, human)</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Quantitative Systems Safety Analysis (hardware, software, phenomenological, human)</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>System Reliability</th>
<th>Skills</th>
<th>Tools</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability Prediction Models</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
<tr>
<td>Reliability Database</td>
<td>Green</td>
<td>Green</td>
<td>Green</td>
</tr>
</tbody>
</table>

**Key:**
- **Minor or No Gap**
- **Significant Gap**
- **Critical Gap**

Text in red indicates a gap.
Objective: Integration of qualitative and probabilistic methods to support design evaluation

- Integrated qualitative and probabilistic methods are usually not conducted until late in the system life-cycle.

Applying integrated system safety and reliability analyses for assessment and trade-off studies early in the design process to improve the effectiveness of decision-making.

State-of-practice focuses at this stage.
Integration of risk analysis with decision processes

Risk-informed Decision-making
(Integrated Consideration of all Performance Measures and Deliberation)

Key Uncertainties

Decision Option

Performance Measures
(Quantities of Interest to Decision-Maker)

FY10

INTEGRATION OF QUALITATIVE AND QUANTITATIVE SYSTEM SAFETY ANALYSIS

<table>
<thead>
<tr>
<th>FM</th>
<th>EFFECT</th>
<th>CR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device A Fails</td>
<td>Loss of X</td>
<td>1</td>
</tr>
<tr>
<td>Device B Fails</td>
<td>Loss of Y</td>
<td>3</td>
</tr>
</tbody>
</table>
MAKING A DECISION: Consideration of all pertinent performance measure with their appropriate importance and their interrelationships

Decision
Choose the most suitable option or reduce uncertainty (do more research)

Assess the Impact of Each Decision Option on Performance Measures (Quantities of Interest to Decision-maker)

With Knowledge of
- Requirements,
- Engineering Insights,
- Engineering Standards and Operational Experience

With Knowledge of
- Technical Risk Metrics,
- Their Uncertainties, and
- Stakeholders' Preferences (relative weights of performance indicators)

Stakeholders Deliberation

Analysis

Feedback

Decision Options

Metric for Crew Safety
Metric for Public Safety
Metric for Mission Success
Metric for schedule
Metric for cost
FY15 Vision for 15.4
Safety & Reliability Analysis

- **Safety, consistent with mission requirements, is designed into the system in a timely and cost-effective manner**
  - Standardization of safety and reliability analyses and processes and their integration with systems engineering process
  - Ability to trade safety & reliability against performance, cost, design options, diverse management paths
  - Extend analysis philosophy to development stages of system design
  - Developing risk acceptance process and criteria
  - Ability to assess and quantify uncertainties
  - Ability to perform trend and precursor analysis
  - Systems knowledgeable safety experts

- **Physics-based Probabilistic Risk Assessment Models that fully integrate all elements of risk; including technical, organizational, and cost**
  - Centralize existing safety, reliability, system design/operating limitations, and risk focused database
  - Assessing expected performance of a design / operational strategy, based on probabilistic simulation of time histories and explicit evaluation of performance (risk) metrics for those time histories
  - User-friendly, intuitive safety & reliability tool interfaces
  - Risk models linked directly to database with automated evaluation updates
Defining acceptable risk regions specific to the program

Risk assessment of decision options

Assessment of uncertainties

consideration of risk results including their uncertainties in decision-making
Example Integrated Future Capability

Architecture Definition

Mission Profile

Operational Parameters

Failure Modeling

Failure Event Response Model

RTLS initiated

OMS Dump

Pitchover

RCS

Failure Modeling

Probability Aggregation

\[ P_{LOV} = P_{ICF}(1-R_{HCE}) + P_{AIF}(1-P_{SIA})(1-R_{LCE}) \]

Uncertainty Assessment

Loss-of-Crew (LOC) Probability Distribution

Loss-of-Vehicle (LOV) Probability Distribution

Loss-of-Mission (LOM) Probability Distribution

Other Risk Metrics

Data Analysis

Reliability Database

Inputs

Outputs
• **System safety and reliability activities incorporated in a risk-informed decision-making framework, capable of**
  – Responding to mishaps in real time
  – Allocating resources (presents solutions, evaluates mitigation options)
  – Effective communication of safety issues
  – Monitoring performance using well defined risk metrics

• **Virtual life-cycle simulation model of safety & reliability**
  – Next-generation hazard analysis techniques that evaluate
    • New hardware technology
    • Software
    • Human performance
    • Organizational factors
  – Safety and reliability models that interface with
    • Quality control processes
    • Testing processes
    • Assembly and manufacturing
    • Maintenance and operational processes
Example of a Simulation-based Risk Model

Branch Points (BP)
- System Hardware State BP
- Physical Variables BP
- Human Action BP
- Software BP
- End State

$P_i \equiv \text{Branch Probability}$

$Prob.(\text{End State}) = P_1 P_2 P_3 P_4 P_5$

Source: UMD Presentation: April 04
15.4 Safety & Reliability Analysis

Key Assumptions: Exploration & Science

15.4.1 System Safety

15.4.2 System Reliability

15.4.3 Safety Management

2008 CEV Initial Flight

2011 James Webb

2013 Comet Surface Sample Return

2015 Prepare for Human Lunar Missions

Capability Roadmap
15: Systems Engineering Risk/Cost Analysis

Integrated Hazard & Reliability Data Bases

Integrated Hazard & Reliability Model Based Analysis

Knowledgeable technical experts performing safety analysis

Complete Set of Risk Metrics

Complete Integration of Risk Analysis with Decision Processes (Risk-informed Decision Making)

15.4 Safety & Reliability

Advanced Physics-based QRA

Next Generation Hazard Analysis Techniques


Model-based Hazard Analysis

Integrated System Engineering and Management Capability

Integrated Reliability database

Integrated Assessment and Management of Technical Risk

Model-based Reliability Analysis

Initial Product Life-Cycle Capability

Collaborative/Distributive PLEM Simulation-Based Capability

Legend

PLM – Product Life Cycle Management
CMMI – Capability Maturity Model Integration
QRA - Quantitative Risk Assessment
LCC - Life Cycle Cost

Major Event / Accomplishment / Milestone

Ready to Use

2005

2010

2015
15.4 Safety & Reliability Analysis

**Key Assumptions:**
- Exploration & Science
- Initial International Collaborative Engineering / Management Simulation Based Capability
- Next Generation of Safety & Reliability Management System
- Engine for Integrated Predictive Safety & Reliability model-based analysis
- Virtual Safety analysis capability

**Capability Roadmap 15: Systems Engineering Risk/Cost Analysis**
- Deep Drill & Completed Initial Human Landing 2018
- Extended Lunar Capability & Life Finder Telescope 2025
- Prepare for Human Mars Mission 2030

**Engine for Integrated Predictive Safety & Reliability model-based analysis**

**Integrated Virtual Safety and SE analysis capability**

**Legend**
- PLM – Product Life Cycle Management
- SBM – Simulation Based Modeling
- CMMI – Capability Maturity Model Integration
- QRA - Quantitative Risk Assessment
- LCC - Life Cycle Cost

---

**Major Decision**
**Major Event / Accomplishment / Milestone**
**Ready to Use**
Concluding Summary

Presenter:
Stephen Cavanaugh
## Capabilities Current State

### Systems Engineering

<table>
<thead>
<tr>
<th>SE-CMMI</th>
<th>Team Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>REQUIREMENTS DEVELOPMENT</td>
<td>X</td>
</tr>
<tr>
<td>REQUIREMENTS MANAGEMENT</td>
<td>X</td>
</tr>
<tr>
<td>TECHNICAL SOLUTION</td>
<td>X</td>
</tr>
<tr>
<td>PRODUCT INTEGRATION</td>
<td>X</td>
</tr>
<tr>
<td>VERIFICATION</td>
<td>X</td>
</tr>
<tr>
<td>VALIDATION</td>
<td>X</td>
</tr>
<tr>
<td>PROJECT MANAGEMENT</td>
<td>X</td>
</tr>
<tr>
<td>PROJECT PLANNING</td>
<td>X</td>
</tr>
<tr>
<td>PROJECT MONITORING AND CONTROL</td>
<td>X</td>
</tr>
<tr>
<td>INTEGRATED PROJECT MANAGEMENT FOR IPPD</td>
<td>X</td>
</tr>
<tr>
<td>RISK MANAGEMENT</td>
<td>X</td>
</tr>
<tr>
<td>INTEGRATED LEANING</td>
<td>X</td>
</tr>
<tr>
<td>INTEGRATED SUPPLIER MANAGEMENT</td>
<td>X</td>
</tr>
<tr>
<td>QUANTITATIVE PROJECT MANAGEMENT</td>
<td>X</td>
</tr>
<tr>
<td>CONFIGURATION MANAGEMENT</td>
<td>X</td>
</tr>
<tr>
<td>PROCESS AND PRODUCT QUALITY ASSURANCE</td>
<td>X</td>
</tr>
<tr>
<td>MEASUREMENT AND ANALYSIS</td>
<td>X</td>
</tr>
<tr>
<td>DECISION ANALYSIS AND RESOLUTION</td>
<td>X</td>
</tr>
<tr>
<td>ORGANIZATIONAL ENVIRONMENT FOR INTEGRATION</td>
<td>X</td>
</tr>
<tr>
<td>CAUSAL ANALYSIS AND RESOLUTION</td>
<td>X</td>
</tr>
<tr>
<td>ORGANIZATIONAL PROCESS FOCUS</td>
<td>X</td>
</tr>
<tr>
<td>ORGANIZATIONAL PROCESS DEFINITION</td>
<td>X</td>
</tr>
<tr>
<td>ORGANIZATIONAL TRAINING</td>
<td>X</td>
</tr>
<tr>
<td>ORGANIZATIONAL PROCESS PERFORMANCE</td>
<td>X</td>
</tr>
<tr>
<td>ORGANIZATIONAL INNOVATION AND DEPLOYMENT</td>
<td>X</td>
</tr>
</tbody>
</table>

### Life Cycle Costing

#### Robotic Spacecraft
- Estimate Life Cycle Cost
- Technology Maturation
- Development
- Production
- Operations

#### Human Spaceflight
- Estimate Life Cycle Cost
- Technology Maturation
- Development
- Production
- Operations

### Safety & Reliability Analysis

#### Risk and Safety Management
- Risk Tradeoffs
- Risk Acceptance and Risk Communication
- Appreciation and Quantification of Uncertainties
- Mishap Investigation
- Trend and Precursor Analysis
- Dissemination of Lessons Learned

#### Systems Safety
- Qualitative Systems Safety Analysis (hardware, software, phenomenological, human)
- Quantitative Systems Safety Analysis (hardware, software, phenomenological, human)

#### System Reliability
- Reliability Prediction Models
- Reliability Database

### Key
- **Minor or No Gap**
- **Significant Gap**
- **Critical Gap**
- Text in red indicates a gap

### Risk Management

#### Prepare for Risk Management
- Determine Risk Sources and Categories
- Define Risk Parameters
- Establish a Risk Management Strategy

#### Identify and Analyze Risks
- Identify Risks
  - Quantitative
  - Qualitative
- Evaluate, Categorize, and Prioritize Risks
  - Planning
  - Track/Control/Communicate

#### Mitigate Risks
- Develop Risk Mitigation Plans
- Implement Risk Mitigation Plans
• **Development Metrics (process, skills, tools)**
  - Annual SE NASA modified CMMI audit of maturity (levels 1-5) and capability readiness (levels 1-5)
  - Number of NASA certified engineers in Systems Engineering, Life-Cycle Costing, Risk Management, and Safety
  - Percentage of programs using integrated Systems Engineering, Project Management, Life-Cycle Costing, Risk Management, and Safety tools

• **Performance Metrics (implementation)**
  - Number of cancelled programs and termination reviews per year
  - Average percent cost of overrun per year
  - Accuracy of cost and schedule predictions
  - Percent of program cost dedicated to Systems Engineering
  - Number of mission failures per total number of missions
  - Number of hits (requests) from Knowledge Management databases in Cost, Reliability, Safety, Risk, and Systems Engineering
• Do the Capability Roadmaps provide a clear path way to technology and capability development?
  – Yes. All Roadmap sections address skills, tools (including Database creation from which Models are developed to address current gaps), and new process.

• Are technology maturity levels accurately conveyed and used?
  – Yes. CRL were assessed by the community, and programs created to address areas with low level CRLs.

• Are proper metrics for measuring advancement of technical maturity included?
  – Yes. The development and performance metrics assigned are appropriate to measure progress towards increasing the validity of the discipline, and reflect current Government criticism.

• Do the Capability Roadmaps have connection point to each other when appropriate?
  – Yes. The capability is a discipline which connects to all other roadmaps.
An active Senior Sponsor is absolutely essential due to the complexity of future NASA Exploration missions.

Develop an integrated organization of Systems Engineering, Cost, Risk, & Safety.

- Application needs to be strategic and tactical implementation
- Capability to integrate across Agency are currently uneven

Develop a Systems Engineering, Cost, Risk and Safety Professional Certification program to develop a qualified skill base.

- Require SE certification level for all SE positions
- Require as a performance objective in personnel reviews
- Reward progress

Establish an independent review process for each program that provides a gatekeeping process to ensure project success.

Create a centralized archival database with best practices, skill base, processes, and lessons learned.

The state of systems engineering as practiced at NASA needs to be improved to successfully achieve the Exploration Vision.
DoD Partnering Possibilities

- Both part of the U.S. government with all the general rules, regulations and procedures that entails
- Share a common industrial base
- Anticipate a large turn over of the workforce in the near future
- Funding constraints, including uncertainties from budget cuts
- Moving towards capabilities-based acquisition and evolutionary development
- Increasing complexity with more system-of-systems and families-of-systems
- Share some technology overlap
- Need a strong role of Systems Engineering Systems Engineering, Cost, Risk and Safety within our programs to be successful

Opportunity exists to collaborate with DoD & NROs Systems Engineering Professional Development Program and the established Systems Engineering Education programs at DAU & AFIT.
Next Steps/Forward Work

Make changes to roadmaps based on NRC feedback
Review and Assess all applicable Strategic Roadmaps and their requirements for Systems Engineering capabilities
- Suggest possible opportunities for Strategic Roadmaps

Make changes to roadmaps to ensure consistency with Strategic Roadmaps requirements
- Additional metrics to determine if achievements will be reached

Continue to work with other Capability roadmaps to ensure consistency and completeness

Develop rough order of magnitude cost estimates for the Systems Engineering, Cost, Risk and Safety Capability Roadmap

Prepare for 2nd NRC Review which will address 4 additional questions:
- Are there any important gaps in the capability roadmaps as related to the strategic roadmap set?
- Do the capability roadmaps articulate a clear sense of priorities among various elements?
- Are the capability roadmaps clearly linked to the strategic roadmaps, and do the capability roadmaps reflect the priorities set out in the strategic roadmaps?
- Is the timing for the availability of a capability synchronized with the scheduled need in the associated strategic roadmap?
7 – Commercial processes/tools widely used by industry and NASA

6 – Commercial processes/tools sparsely used by NASA

5 – Specialized NASA developed processes/tools used in current programs

3 – Processes/tools under development for existing projects/programs

1 – Ideas of processes/tools that could enhance NASAs Systems Engineering