Modern Risk Management For Systems Engineering

VICTOR ABUNDEZ
MAY 6, 2014
INTEGRATIVE PROJECT

Agenda & Topics of Discussion

Abstract
Project Objectives
Relation of Topic to Systems Engineering
Systems Engineering Discussion
Risk Management Discussion
Reference Case Studies
Benefit to Systems Engineering
Approach Used
Results Vs. Objectives
Summary
Abstract – What is “Modern” Risk Management?

This project will introduce an improvement on the traditional approach of risk management as applied in the field of systems engineering.

“Risk management is traditionally taught and implemented as the avoidance of negative consequences. A better way to think about risk is that it has both opportunity and failure dimensions. This project will attempt to focus on how to embed both the opportunity (creation of value), and failure (destruction of value) within systems engineering projects so that decisions across the life-cycle are characterized in these two opposing dimensions. An approach that manages the balance of these two dimensions enables teams, at any point within the life-cycle, to seek opportunities for value creation while making calculated investments to mitigate potential negative consequences that result in failure.”
Abstract – What is “Modern” Risk Management?

Traditional
- The avoidance of negative consequence.
- The avoidance of loss.
- Good approach, but modern systems engineering requires more.
- Modern Lean Systems Engineering is highly value-driven.
- Risk management is no exception.

Modern
- The avoidance of loss or negative consequence, in order to create value and remove waste.
- Value can come in different forms.
- Money saved = value for stakeholders and customers.
- Time earned = value for engineering organization and customers.
- Problems and problem areas identified and removed = value for all stakeholders of system.
- Opportunity gained = value for engineering organization.
- Integrate opportunities and failures in system lifecycles.

Project Outcome

Demonstrate Knowledge of the Systems Engineering Process.
Demonstrate Knowledge of Lean Principles and Initiatives.
Demonstrate Why Risk Management Should Create Value for Systems Engineering Projects:
- Systems will become more and more complex.
- Many different subsystems incur many more risks.
- Customers continue to demand higher performance.
- Systems will expand to global operations.
- An effective risk approach will make the SE more effective overall.

Present Two Case Studies and their Systems Engineering Process
- With emphasis on the Risk Approach and how it created value or waste.

Improve the Traditional Approach and Introduce a Modern Approach for Better Success in Future Systems Engineering Programs.
Risk Management is Important Because

Many past & current systems engineering projects have been riddled with failure.
- F-35
- Boston Central Artery/Tunnel Project
- FAA Advanced Automation System for Air Traffic Control, 1994 (Scrapped at a Cost of $3-6B)

Some, however, have been highly successful.
- SR-71 Blackbird
- B2 Spirit
- San Francisco Golden Gate Bridge

There are several reasons for successful programs:
- Disciplined Systems Engineering processes.
- Experienced and knowledgeable program leadership.
- Effective Lean practices.

Risk Management is Important Because

Effective Implementation of Risk Management
- Not knowing where the risks lie is one of the single biggest contributors to program failure.
- Improper identification of risk causes unpleasant surprises late down the program lifecycle.
- Failure to manage risks can cause a drastic effect on program resources in a desperate attempt to "put out the fires."

Therefore, risk management is as important to Systems Engineering as any of its other functions.

Just as Lean Principles has impacted engineering practices, Risk Management should become more Lean to be more effective.
- Lean has proven itself in aerospace and automobile industries.
- "Modern" Risk Management is based on Lean beliefs — creation of value and elimination of waste throughout the lifecycle.
Systems Engineering Discussion

Systems engineering takes customer/user requirements and develops them into a functional system deliverable.

From Need to Solution

Systems Engineering Process consists of:
- Requirements
- Research & Development
- Sub-system & System Integration
- Modeling
- Test
  - Validate
  - Verify
- System Launch

The SE's job is to seek different ways of satisfying system requirements.
SE Provides Structured Processes for Entire Lifecycle

Begins Before Requirements Are Established.
- Capabilities
- Resources
- Planning

SE Provides Structured Processes for Entire Lifecycle

Continues After System Deliverable.
- Support
- Lifecycle Operations
- Maintenance and Upgrade
- Deactivation and End-of-Life Operations
Systems Engineering Process

Other Systems Engineering Diagrams
Before Moving On

INCOSE: "An interdisciplinary approach and means to enable the realization of successful systems."

Three Aspects:
1. Interdisciplinary
2. Realization
3. Successful

Risk

The Systems Engineering Process must manage risk: both internal and external; known and unknown.
Risk is Defined As

- A situation involving danger or loss.
- The possibility that something unpleasant or harmful will happen.
- A threat or source of danger.

For Systems Engineering Programs, Risk Is

- The possibility of a negative occurrence.
- The likelihood of a loss.
- The probability of a system not performing as expected.
- Probability of a system not performing at all.
Risk is Present Across the Entire System Lifecycle

At Program Conception
- Poor planning.
- Poor requirements definition and development.

During Systems Engineering
- Insufficient resources.
- Technical risks.
- Inadequate SE processes.

At System Delivery
- Wrong system delivered.
- System does not function as expected.

At System Operations and End-Of-Life
- Poor, no system support.
- Poor, no end-of-life and system deactivation plan.

Technical Risk
System delivery does not meet the technical requirements set forth by the user/customer.

By far most complex.

Typically caused by:
- State of the art technology.
- Environments that quickly degrade system performance.
- Inadequate requirements.
- Poor systems engineering practices.

Can result in:
- System failure.
- System over-budget
- System behind schedule.
**Cost Risk**

System cost exceeds estimated amount.

Most common.

Typically caused by:
- Improper cost estimates.
- Schedule overrun.
- High technology.

Can result in:
- System shutdown.
- Legislative action.
- Financial loss to SE team and organization.

---

**Schedule Risk**

System likelihood of failing to meet project milestones, including final delivery date, and the effect of that failure.

- Internal milestones also considered a risk.

Typically caused by:
- Internal schedule conflicts.
- Long-lead times.
- Late deliveries by suppliers and vendors.

Can result in:
- Late system delivery.
- Poor system performance as tasks are rushed.
- Added expenditures in an attempt to meet deadlines.
- Penalties or fines imposed by customers.
Risk of the Unknown

Factors and threats that are outside of the System, and outside of the System Engineer’s realm of control.

Unknown factors include:
- Political
- Environmental
- Economic
- Social

This risk can cripple or destroy a system, change requirements, or lead to an increase in cost, among other consequences.

Unknown risks are an exceptional threat because they are difficult to assess and therefore mitigate.

Interaction of Risks

![Diagram showing the interaction of Technical, Unknown, Schedule, and Cost]

- Technical
- Unknown
- Schedule
- Cost
Risk Analysis

Systems Engineers should, at a minimum, carry out a thorough risk analysis. The results of the analysis should be included in the SEMP or SEP. Risk analysis must be performed for the lifecycle of the System.

Two Major Factors of a Risk Analysis

1. The likelihood that a high-risk event (or set of) will occur.
2. The consequences of said event (or set of).

<table>
<thead>
<tr>
<th>Effect</th>
<th>Low Probability</th>
<th>Medium Probability</th>
<th>High Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High-Low</td>
<td>High-Medium</td>
<td>High-High</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium-Low</td>
<td>Medium-Medium</td>
<td>Medium-High</td>
</tr>
<tr>
<td>Low</td>
<td>Low-Low</td>
<td>Low-Medium</td>
<td>Low-High</td>
</tr>
</tbody>
</table>

Risk Matrix
Risk Management is

The practice of controlling risk drivers that affect the program (NASA).

The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level (The MITRE Corp.)
Risk Management Process

Risk Management Plan

Introduction
Summary
Definitions
Risk management strategy and approach
Organization
Risk management Processes and procedures
Typical Risk Assessment

<table>
<thead>
<tr>
<th>Type / Area</th>
<th>Risk</th>
<th>Possible Consequence</th>
<th>Probability</th>
<th>Impact</th>
<th>Total</th>
<th>Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>Employed tools, more expensive than assumed.</td>
<td>Program cost increase.</td>
<td>M</td>
<td>H</td>
<td>MH</td>
<td>Accurate cost estimates. Proper capabilities assessment.</td>
</tr>
<tr>
<td>Technical</td>
<td>Sub-system integration problems.</td>
<td>Top level system not working as intended.</td>
<td>H</td>
<td>H</td>
<td>HH</td>
<td>Apply the SE process at every level of design.</td>
</tr>
<tr>
<td>Schedule</td>
<td>PDR took 1 mo. longer than anticipated.</td>
<td>Milestone delays cause system delivery to be later.</td>
<td>L</td>
<td>M</td>
<td>LM</td>
<td>Ensure capabilities &amp; performance are where they need to be prior to agreement of scheduled commitments.</td>
</tr>
</tbody>
</table>

Mitigation Strategies and Tools

Compliance with ISO 9001.
Effective process management and execution.
Supply chain integration.
Industry best practices:
- Manufacturing
- Engineering
- Design
Implementation
Independent assessments.
Traditionally, Risk Approach Has Been Good

Needs to be improved.

Systems are becoming
- More complex
- More technical
- Higher in scope (global)

Customers expect higher performance, better results

The risk approach needs to be "Modernized."

Lean & Quality

Auto and general manufacturing practices have become more Lean in response to changing engineering systems and climate.

Product engineering, too, has adopted Lean.

A direct result of Lean approaches have yielded:
- Higher quality
- Better efficiency
- Less waste

A high-quality system/process is one that:
- Works right upon delivery.
- Has minimal to no waste.
- Is high value

Systems Engineering Top Quality Objective: Total Quality Management
- Effort to continuously improve the ability to deliver high-quality systems and service to customers.
To Modernize Risk Management, Therefore

Must integrate two important dimensions into the risk approach:
- Value
- Waste

Balance the opportunities and failures across entire system lifecycle.
- Opportunities = creation of value
- Failures = Not only waste, but destruction of value. Double loss!

This “Modern” approach achieves two things:
- Enables Systems Engineering effort to seek opportunities for value creation.
- Assists in making calculated investments to mitigate potential negative consequences that result in failure.

This suggested approach yields the same results as a solid traditional risk management plan, but also helps deliver value to the organization, process, and customer.

Case Example: Creation of Value Through Risk Management

Highly Complex
- Many sub-systems form entire “Weapons System.”
- Cutting edge technology.
- Multi-organizational effort to achieve program objective.

Joint effort
This type of system is highly vulnerable to all types of SE risks.

The SE effort proved that a structured and disciplined effort can overcome these risks and deliver a system of value with minimal waste.
Why the B2 RM Approach Succeeded

Systems Engineering was applied that was consistent with the level of maturity for the discipline for the time.

• Value: Technology Maturity was up to par with the time, resulting in a technically advanced system.
• Waste Eliminated: Effort and resources were not wasted on later attempts to mature the technology.

Customer requirements were integrated into the design and development process.

• Value: Air Force was delivered exactly what it asked. (From Need to Solution). Requirements were integrated from the beginning of the lifecycle to system delivery.
• Waste Eliminated: Time, money, resulting from an attempt to align with the requirements much later in the lifecycle.

Specialists assessed specific performance level of a requirement to enhance effectiveness or trade for a lower level of performance to reduce cost or risk. The SE effort balanced the benefit of achieving performance level against the impact on cost and risk.

• Value: Reduction of cost and risk.
• Waste Eliminated: Too high or too low performance (thru-trade studies), negative cost and risk impact, and the resources needed to mitigate the impacts.

Key Takeaways From B2 System Approach

Do not overemphasize the value of a solid risk approach:

• Single effort, one objective.
• Jointly developed.
• Program-wide employment of risk strategies.
• Shared and understood by all.

The SE team’s risk management plan was a major contributor to overall program success.

Good Systems Engineering cannot exist without good Risk Management, one complements the other.

The Risk Approach in the B2 Program did not single-handedly save the program, but it would have been greatly waste-ridden without it.

• Schedule delays.
• Cost overrun.
• Threat of program shutdown.
• Time wasted.
• Effort wasted in non-valued added tasks.
Case Example: Destruction of Value Through Risk Management

Highly complex, technical, and unknown environment.

User and customer very different than DoD systems.

Requirements came from diverse sources.

Powerful influences outside the system domain.

Despite setbacks due to risk threats, HST enjoyed overall program success.

Why HST Risk Approach Was Not as Robust as B2

Risk Area: Program was heavily reliant on sub-contractors.
- Contractors “owned” their share of the risk area.
- Waste: This effort was not system-wide, but instead, very specific to the respective portion of the program. This goes against a "shared" risk effort.

Risk Area: Technical
- NASA counted on sub-contractor LMSC as integrator for critical optical system of telescope, including risk.
- Waste: LMSC was not the technical expert, but P-E was. LMSC is managing risk in a domain where they are not fully capable of assessing risk.

Risk Area: Insufficient program oversight
- LMSC’s primary role was to integrate the telescope onto the S/C.
- P-E was entirely in charge of telescope with no oversight from LMSC, or NASA.
- This leads to lack of oversight, checks, poor quality assurance.
- Waste: System is delivered and launched with flawed primary mirror array, which system test would have caught.
Key Takeaways from Hubble Space Telescope

HST Risk Approach was not structured accordingly to the risk factors involved.

Demonstrates case of good SE, but weak Risk Approach.

- Good requirements definition created value by delivering system that addressed the needs of scientific community and academia.
- Use of verification and validation (key Risk strategies) helped throughout the lifecycle but ultimately failed to catch the primary mirror defect.
- Communications challenges are often overlooked, yet they are a risk area too. This was not properly addressed in HST, creating waste through poor communications flow-down to sub-contractors and other parties involved.

NASA underestimated the scope of technology required to design, build, and test a system as complex as HST.

- Destruction of value: level of technology-readiness was discovered throughout the lifecycle of HST, not before. High-value task of end-to-end test was ignored, leading to mirror defect.
- NASA had no ability to verify if the telescope was correct upon agreement to proceed without system test.

An Important Note

B2 was not without setbacks, but continues to support mission requirements to this day 20 yrs. after deployment

- Suffered slight setbacks.
- Program mid-cycle redesign.
- Slight cost increase.

Hubble Telescope, despite the flawed risk approach, is considered an engineering success.

- Much has been learned from its application, essentially delivering value.
- Considering the technical scope involved, HST succeeded in delivering a system that was capable of satisfying two customers.

These cases were selected to illustrate the Project Objective: Creation of Value through Risk Management.

- Lapses in HST’s risk approach destroyed opportunities for value. These led to big failure
- B2 SE effort’s value-driven risk approach overcame obstacles and solidified the overall systems engineering effort.
Risk In Technology Maturity

Probability of failure to:
- Reach maturity for system integration.
- Meet Technical Goals and Objectives.

Impact on entire system and all tasks downward in the Process Flow Map.
Impact on System Performance

To measure readiness level, systems engineers can refer to NASA's TRL Chart.

---

NASA Technology Readiness Level

Technology Readiness Levels (TRLs)

- TRL 9: Actual system "flight proven" through successful mission operations
- TRL 8: Actual system completed and "flight qualified" through test and demonstration (Ground or Flight)
- TRL 7: System prototype demonstration in a space environment
- TRL 6: System/subsystem model or prototype demonstration in a relevant environment (Ground or Space)
- TRL 5: Component and/or breadboard validation in relevant environment
- TRL 4: Component and/or breadboard validation in laboratory environment
- TRL 3: Analytical and experimental critical function and/or characteristic proof-of-concept
- TRL 2: Technology concept and/or application formulated
- TRL 1: Basic principles observed and reported
Using TRL for Risk Assessment

To prevent other Risks (Cost and Schedule)

- Cost: Define and establish cost criteria at each level.
- Schedule: Provide adequate time in development if at all possible, especially at higher TRLs (Schedule).
- Total: Involve Program Management and Systems Engineering for overall Risk Mitigation at each TRL.

To help Management & Engineering make decisions concerning development and readiness of program’s maturity.

Identify which technologies need assessment.

Gather evidence of maturity.

Devise a Technical Readiness Assessment.

Department of Defense Typical TRA

1. Purpose of TRA
2. Program Overview (System Objective and Description)
3. Program Technology Risk Summary
   1. Identification
   2. Mitigation
   3. Results
4. Summary
The Value of a TRA

Establishes a systemic plan of action.
Can be used as a point of reference.
Sets forth a specific process for technical risk.

Benefit of This Project To Systems Engineering

The Project demonstrates the various elements of a successful Risk Management approach.

Builds on the “traditional” approach that was been taught and implemented but introduces new elements:

- To adapt to future Systems Engineering programs, Risk Management must do its share in creating value for the organization, the system, and the customer.
- Trend for “modernizing” Systems Engineering becomes evident in Lean Engineering and Manufacturing.

This new Risk Approach will vastly improve quality of systems just as Lean and Quality Management Principles have done so.

Introducing this new Risk Approach enables Systems Engineers to think about risk as method of creating value throughout the lifecycle, simultaneously eliminating risk and waste.
Undertaken Approach

Author proposed new approach to Risk Management based on Lean Principles and Systems Engineering concepts.

The author reviewed material from entire course of study for references and relevant material.

All material from classes used to support the author’s proposed approach.

Author selected two case studies (also from previous classes) to help prove the benefit of this approach and this project.

Referenced industry documents and standards:
- INCOSE
- NASA
- DoD

Author compiled all research into a written document format and PowerPoint presentation to explain and justify the Project Deliverable.

Project Objective vs. Outcome

Demonstrate Knowledge of the Systems Engineering Process.

Demonstrate Knowledge of Lean Principles and Initiatives.

Demonstrate how Risk Management Should Create Value for any Systems Engineering Projects due to:
- High complexity.
- Many different subsystems incur many more risks.
- High technical expectations.
- More global operations.
- The human factor.

Present Two Case Studies and their Systems Engineering Process
- With emphasis on the risk approach and how it created value or waste.

Improve the Traditional Approach and Introduce a Modern Approach for Better Success in Future Systems Engineering Programs.

Discuss SE Discipline and Processes.

Integrate Lean Principles and Concepts to Project Objective.
- Modern Risk Management has strong foundation in Lean.

Recommend how Risk Management can be used to create value and remove waste.

Illustrate the premise with two real-world example and the undertaken risk approach.

Justify how the proposed approach is of benefit to the Systems Engineering Domain.
Summary

A complete Systems Engineering Approach must have three concepts:
- Lifecycle Support
- System & Program Management
- Risk Assessment & Management

The Systems Engineer's duty is to achieve a need to a solution by:
- Performing trade-studies.
- Analyzing different ways of satisfying requirements.
- Understanding the risks of each option.
- Seeing where value is greatest.
- Reviewing the performance, technical requirements, and designs being considered for inclusion in the program.

Systems Engineers must implement a new risk approach for future Systems Engineering endeavors, one which:
- Balances opportunities against failures.
- Creates value throughout lifecycle as engineers seek opportunities for value creation.
- Eliminates waste as risk obstacles are removed from the system and lifecycle support.

The Risk Approach should be systemic, system-wide, with shared objectives.

The Approach should strive to create value.

References


Acknowledgements

Sincere thanks to the faculty and Professors of the Loyola Marymount Systems Engineering Program for their knowledge, help, and guidance throughout the course.

Thanks to Dr. Brown for his role as Advisor to the author.

End