MFPT

ANNUAL CONFERENCE

Diagnostics, Prognostics, and Failure Prevention

Where Theory Meets Practice

PRODUCED BY

ASNT

Systems Engineering Tutorial with Case Studies

John M. Lucero

NASA Glenn Research Center

5/9/2024

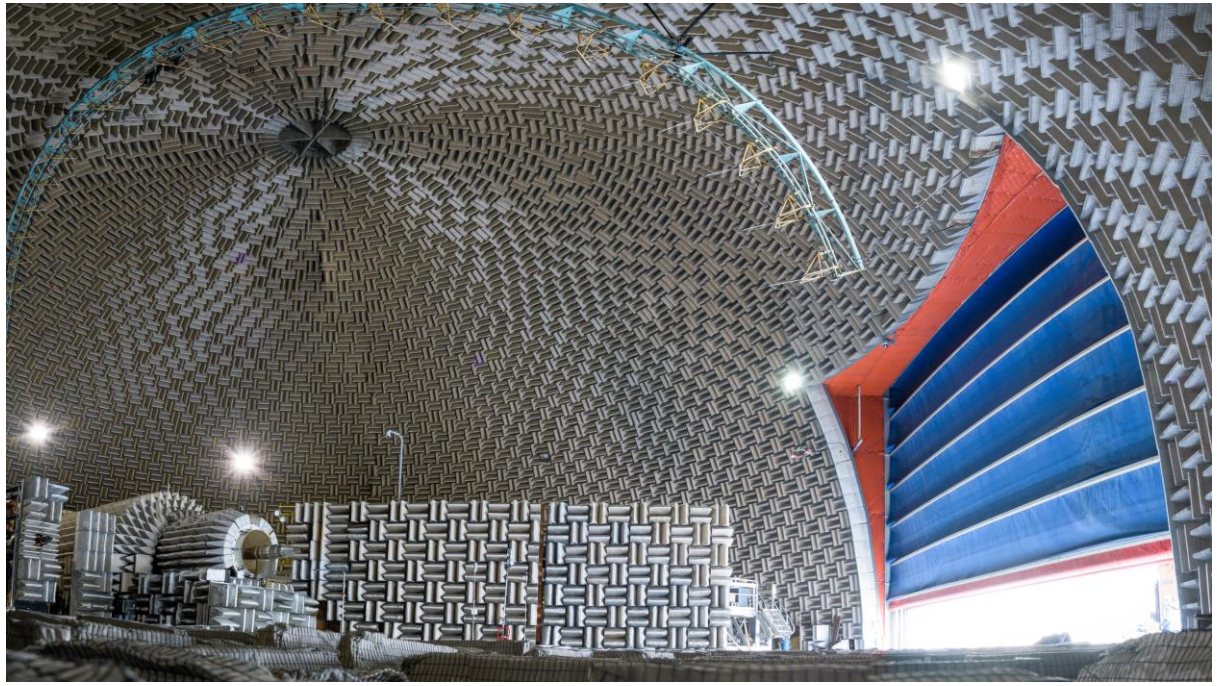


Image Credit: NASA/ Rami Daud, Alcyon Technical Services

Outline

- Goal and objective
- SE history and definitions
- SE benefits and key points
- NASA SE processes
- MFPT and SE
- Design Reviews
- Phases of the project
- Requirements Development
- Verification and Validation
- Risk Management - Analysis & Mitigation
- Model Based Systems Engineering
- Conclusions

Goal

- Educate the MFPT community and partners on Systems Engineering and how it pertains to failure prevention

Objective

- Communicate successful processes to perform project design and implementation through real life examples for minimizing **design** failure

- Why are we sitting here?

Possible Answer

- Seeking greater success in project endeavors.

Proposed solution

Question to audience

- Performing activities defined by Systems Engineering methods will greatly increase project success.

- Robust Verification and Validation processes in place, two schools of thought.
  - Plan for initial success with minimal failures along the way
  - use agile development — where engineers confirm a minimally viable design and then develop a minimally viable product very quickly.

Design Engineering Dilemma

Engineers want a solution NOW!

- General statements lead to detailed design on first step.
- Difficult to step back and look at BIG picture
- Up front requirements definition and systems engineering planning are PARAMOUNT before designs start getting built.
- Late design changes cost $$$$$
- Communication is KEY.

Definitions and Terms

System:

- NASA: A set of interrelated components which interact with one another in an organized fashion toward a common purpose.

- DOD: An integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.

- INCOSE: A construct or collection of different elements that together produce results not obtainable by the elements alone.

SE history

1. Systems Engineering can be traced back to Bell Telephone Laboratories in the 1940s

2. 1950s and 60s DoD and NASA led the development and identification of new SE methods and modeling techniques

3. International Council on Systems Engineering (INCOSE) 1995

4. 2000s - The conception, design, development, production and operation of physical systems through Model Based Systems Engineering (MBSE)

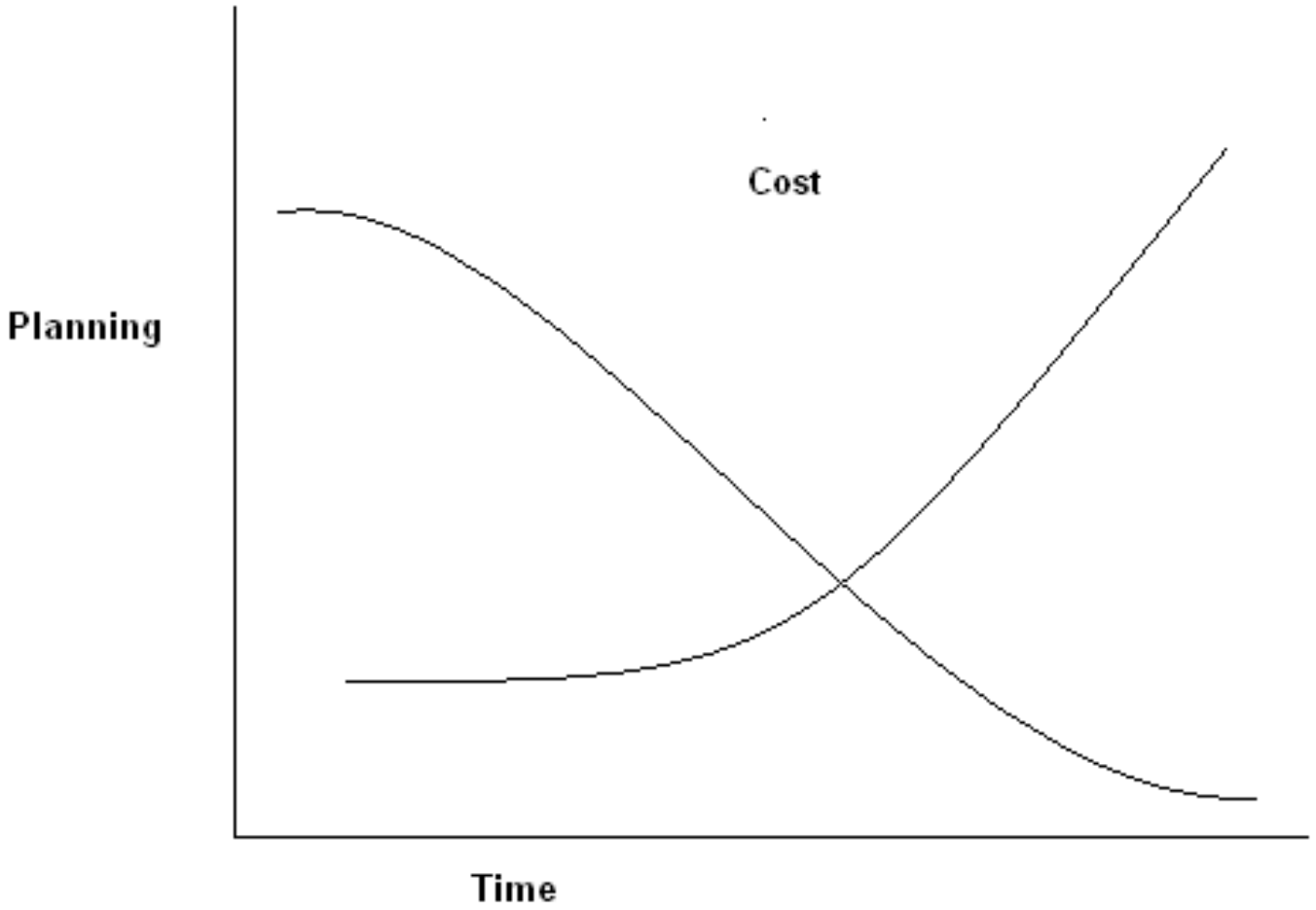
Systems Engineering Definition (NASA SP-6105)

***Systems engineering is* a robust approach to the design, creation, and operation of systems**. In simple terms, the approach consists of identification and quantification of system goals, creation of alternative system design concepts, performance of design trades, selection and implementation of the best design, verification that the design is properly built and integrated, and post-implementation assessment of how well the system meets (or met) the goals. An important aspect of this role is the creation of system models that facilitate assessment of the alternatives in various dimensions such as cost, performance, and risk.

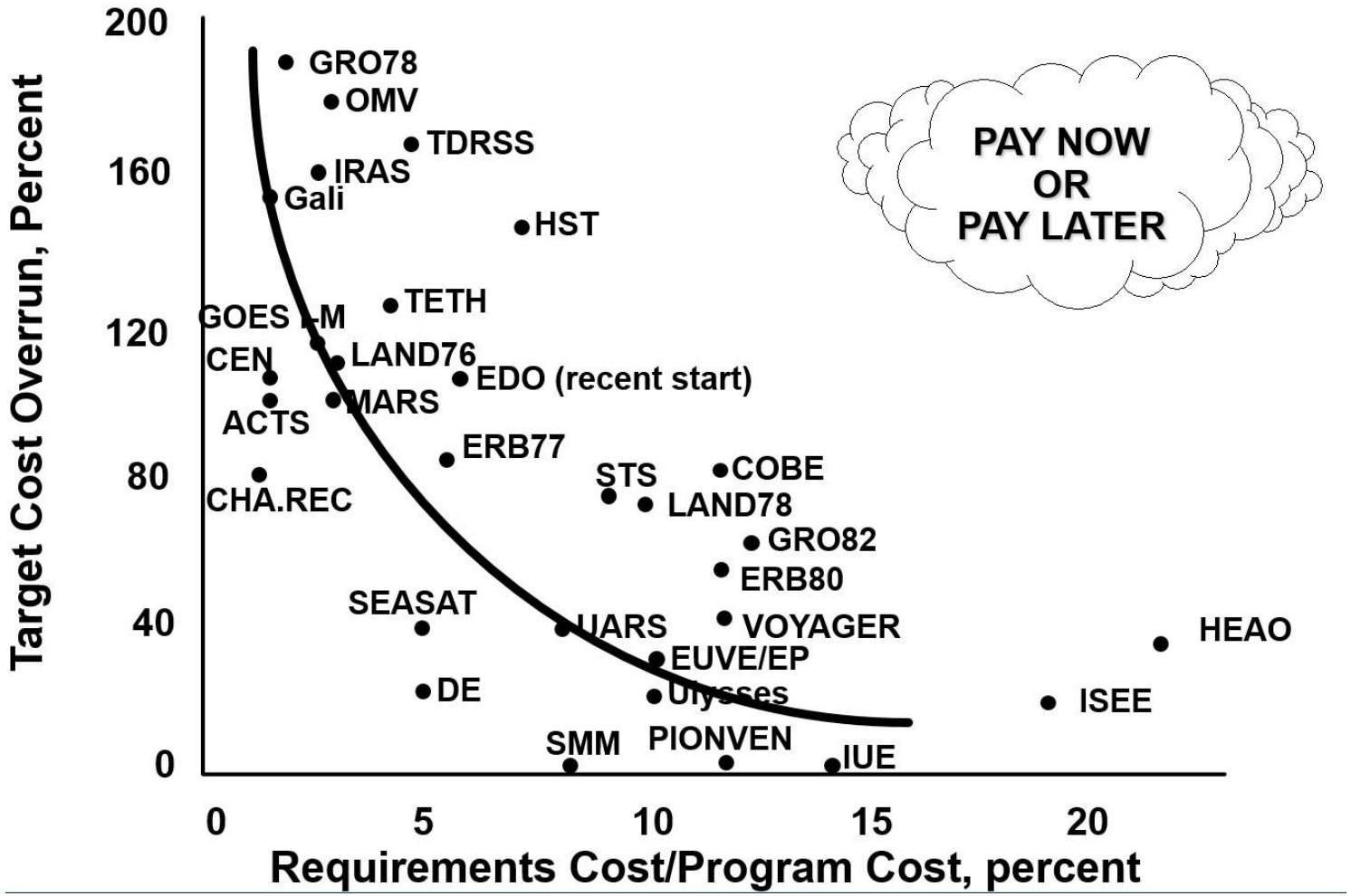
***The objective of systems engineering is to see** to it that the system is designed, built, and operated so **that it accomplishes its purpose in the most cost-effective way possible**, considering performance, cost, schedule, and risk*.

Systems Engineering Competencies*	
Competency Area: **1.0 Concepts and Architecture**	**Competency Area:** **6.0 NASA Internal and External Environments**
1.1 Mission Needs Statement	6.1 Agency Structure, Mission, and Internal Goals
1.2 System Environments	6.2 NASA PM/SE Procedures and Guidelines
1.3 Trade Studies	6.3 External Relationships
1.4 System Architecture	
Competency Area: **2.0 System Design**	**Competency Area:** **7.0 Human Capital Management**
2.1 Stakeholder Expectation Definition & Management	7.1 Technical Staffing and Performance
2.2 Technical Requirements Definition	7.2 Team Dynamics and Management
2.3 Logical Decomposition	
2.4 Design Solution Definition	
Competency Area: **3.0 Production, Product Transition, Operations**	**Competency Area:** **8.0 Security, Safety and Mission Assurance**
3.1 Product Implementation	8.1 Security
3.2 Product Integration	8.2 Safety and Mission Assurance
3.3 Product Verification	
3.4 Product Validation	
3.5 Product Transition	
3.6 Operations	
Competency Area: **4.0 Technical Management**	**Competency Area:** **9.0 Professional and Leadership Development**
4.1 Technical Planning	9.1 Mentoring and Coaching
4.2 Requirements Management	9.2 Communication
4.3 Interface Management	9.3 Leadership
4.4 Technical Risk Management	
4.5 Configuration Management	
4.6 Technical Data Management	
4.7 Technical Assessment	
4.8 Technical Decision Analysis	
Competency Area: **5.0 Project Management and Control**	**Competency Area:** **10.0 Knowledge Management**
5.1 Acquisition Strategies and Procurement	10.1 Knowledge Capture and Transfer
5.2 Resource Management	
5.3 Contract Management	
5.4 Systems Engineering Management	

Benefit of SE



Effect of Requirements Definition Investment on Program Costs

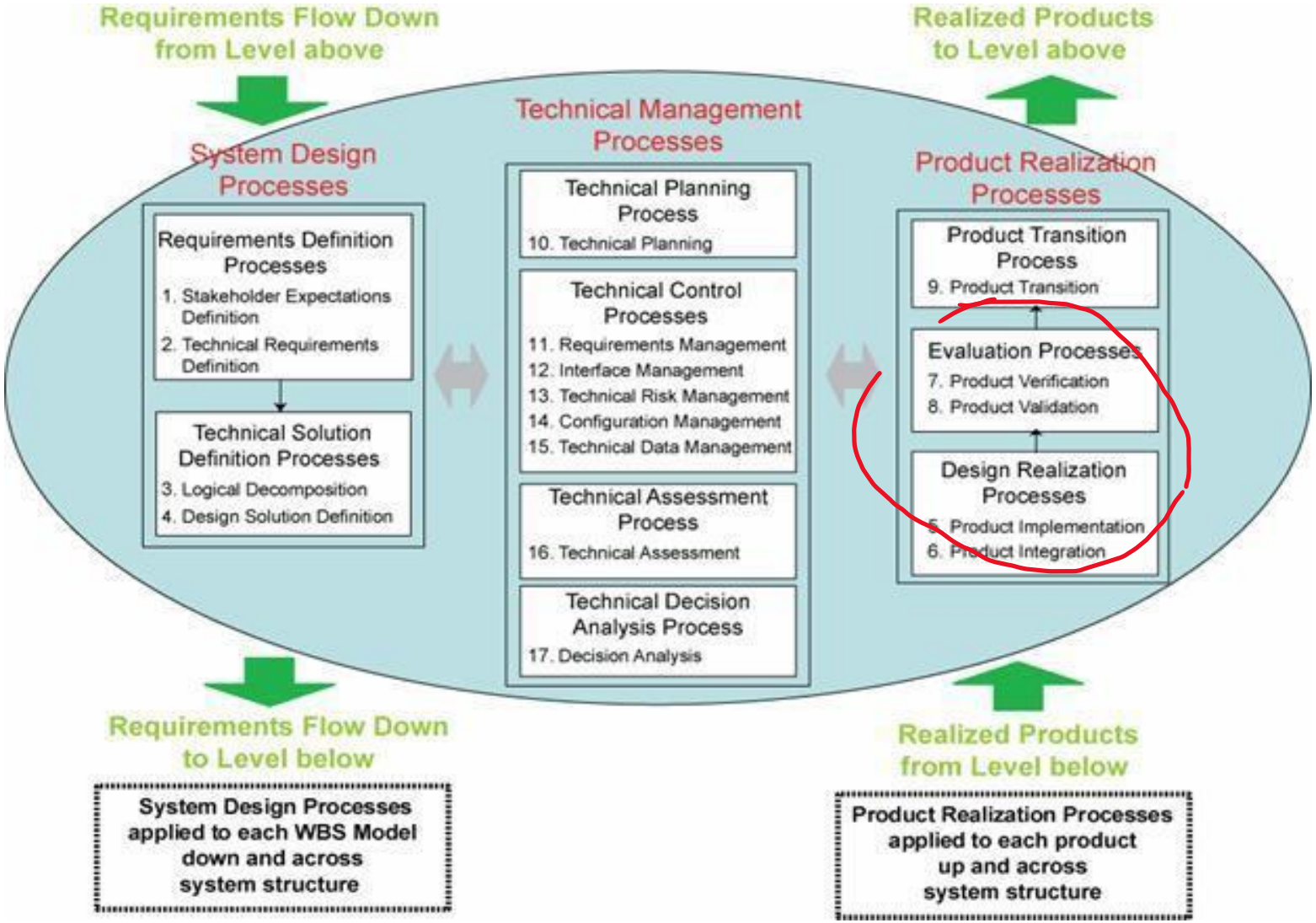


MUST BALANCE

Risk (R)! Performance (P)! Cost (C)!

C*R = P

1. Reduce C at constant R = P drops
2. Reduce R with constant C = P drops
3. Reduce P at constant C = Risk drops
4. Reduce P at constant R = Cost drops
5. Reduce C at constant P = Risk increase
6. Reduce R at constant P = Cost increase
7. Etc.


Requirements Flow Down from Level above
Realized Products to Level above
System Design Processes
Requirements Definition Processes
1. Stakeholder Expectations Definition
2. Technical Requirements Definition
Technical Solution Definition Processes
3. Logical Decomposition
4. Design Solution Definition
Technical Management Processes
Technical Planning Process
10. Technical Planning
Technical Control Processes
11. Requirements Management
12. Interface Management
13. Technical Risk Management
14. Configuration Management
15. Technical Data Management
Technical Assessment Process
16. Technical Assessment
Technical Decision Analysis Process
17. Decision Analysis
Product Realization Processes
Product Transition Process
9. Product Transition
Evaluation Processes
7. Product Verification
8. Product Validation
Design Realization Processes
5. Product Implementation
6. Product Integration
Requirements Flow Down to Level below
Realized Products from Level below
System Design Processes applied to each WBS Model down and across system structure
Product Realization Processes applied to each product up and across system structure


NASA/SP-2007-6105
Rev1
NASA
Systems Engineering
Handbook

This handbook consists of six core chapters:

(1) Systems engineering fundamentals discussion

(2) the NASA program/project life cycles

(3) systems engineering processes to get from a concept to a design

(4) systems engineering processes to get from a design to a final product

(5) crosscutting management processes in systems engineering

(6) special topics relative to systems engineering

How do MFPT efforts relate to Failure Prevention?

Sensors

- Sensors are used for monitoring and can be used to determine Health and Status of a particular component
- From Prognostics/Health Management (PHM), Sensors can be developed to watch for a particular failure mode
- Sensors feed the data analysis/management people
- Any other ideas from the audience that pertain to sensors and failure prevention?

Data analysis and management (DAM)

- Through DAM failures can be captured and analyzed
- New data analysis techniques can be developed to analyze data and glean out when a particular failure occurs
- New data management techniques can be developed to handle the enormous amounts of data taken in this day and age.
- DAM work feeds into Signal Processing.
- Any other ideas from the audience that pertain to DAM and failure prevention?

Signal Processing

- Signal processing take input from DAM and tries to make sense of it.
- The processing will massage the data into something that can be used to determine how the system/component of interest is operating
- This information is passed on to the Diagnostics people
- Any other ideas from the audience that pertain to Signal processing and failure prevention?

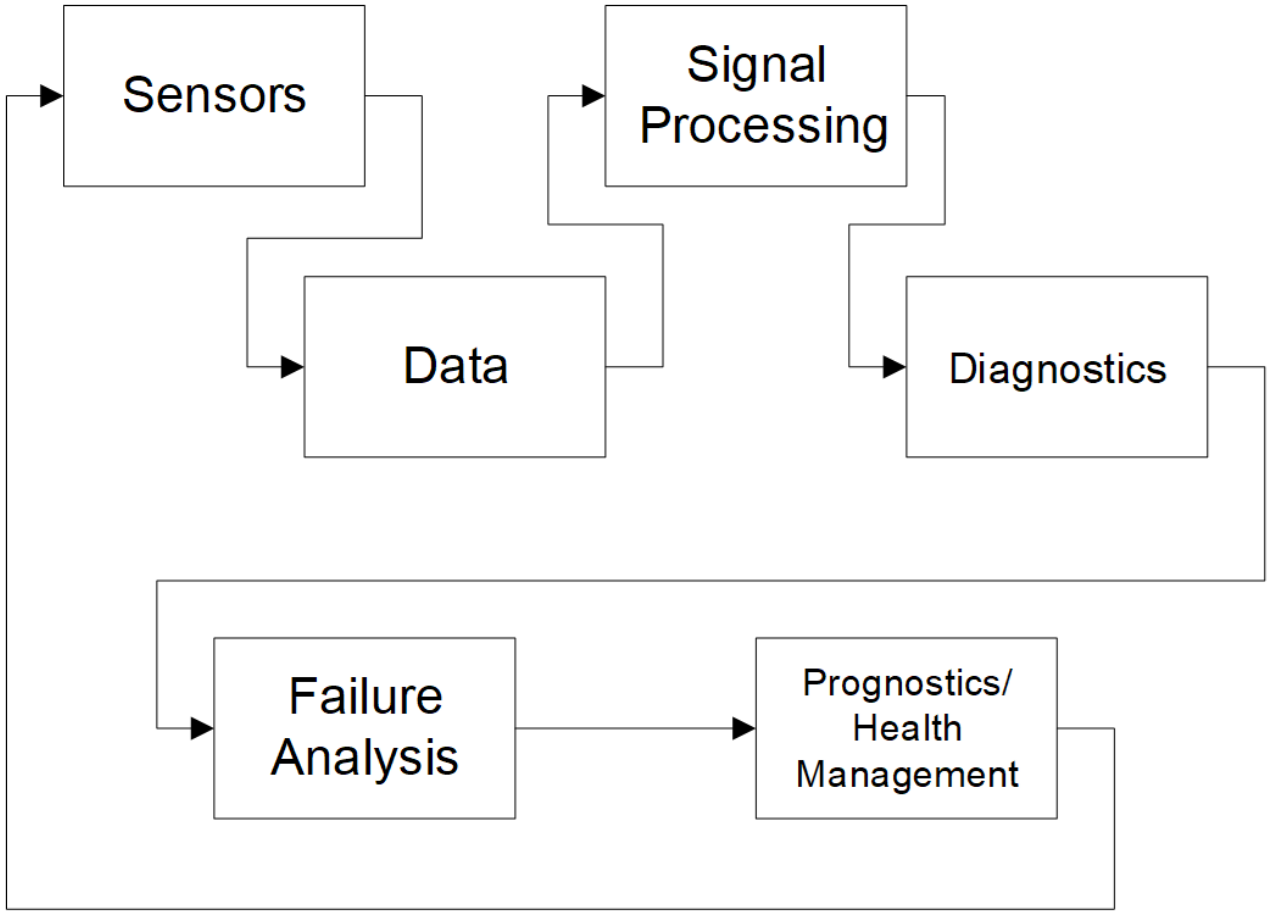
Failure Analysis (FA)

- The FA takes the information gathered by the previous groups to obtain the physical and failure information of components and subsystems.
- The FA is used by the PHM group for data modeling and analysis
- Any other ideas from the audience that pertain to FA is used for failure prevention?

Prognostics and Health Management (PHM)

- PHM permits the evaluation of a system's reliability in its actual life-cycle conditions.
- Used predict the future degradation or damage and the Remaining Useful Life (RUL) of an asset or part, based on the measured data
- PHM information is used to develop sensors to keep an eye on
- Any other ideas from the audience that pertain to PHM is used for failure prevention?

Systems Engineering and MFPT



Design Reviews and Failure Prevention

Leading up to Preliminary Design Review

- To determine the feasibility and desirability of a suggested new major system and establish an initial baseline compatible with strategic plans.
- Develop final mission concept, system-level requirements, and needed system structure technology developments.
- Mature requirements for all products in the developing product tree, develop ConOps, preliminary designs, and perform feasibility analysis of the verification and validation concepts to ensure the designs will likely be able to meet their requirements.

Most “key” valuable lessons

- Techniques on calling, holding, and archiving meetings/action items
- Human interface, stakeholder education for synthesis of requirements document (design by requirements is bad)
- Functional Analysis (gives insight, interfaces, WBS, PBS based on product architecture)
- Clarity (no vague requirements wording)
- Plan to iterate
- Diplomacy
- One shall per requirement
- Verify – feasible and affordable
- Validate – use it

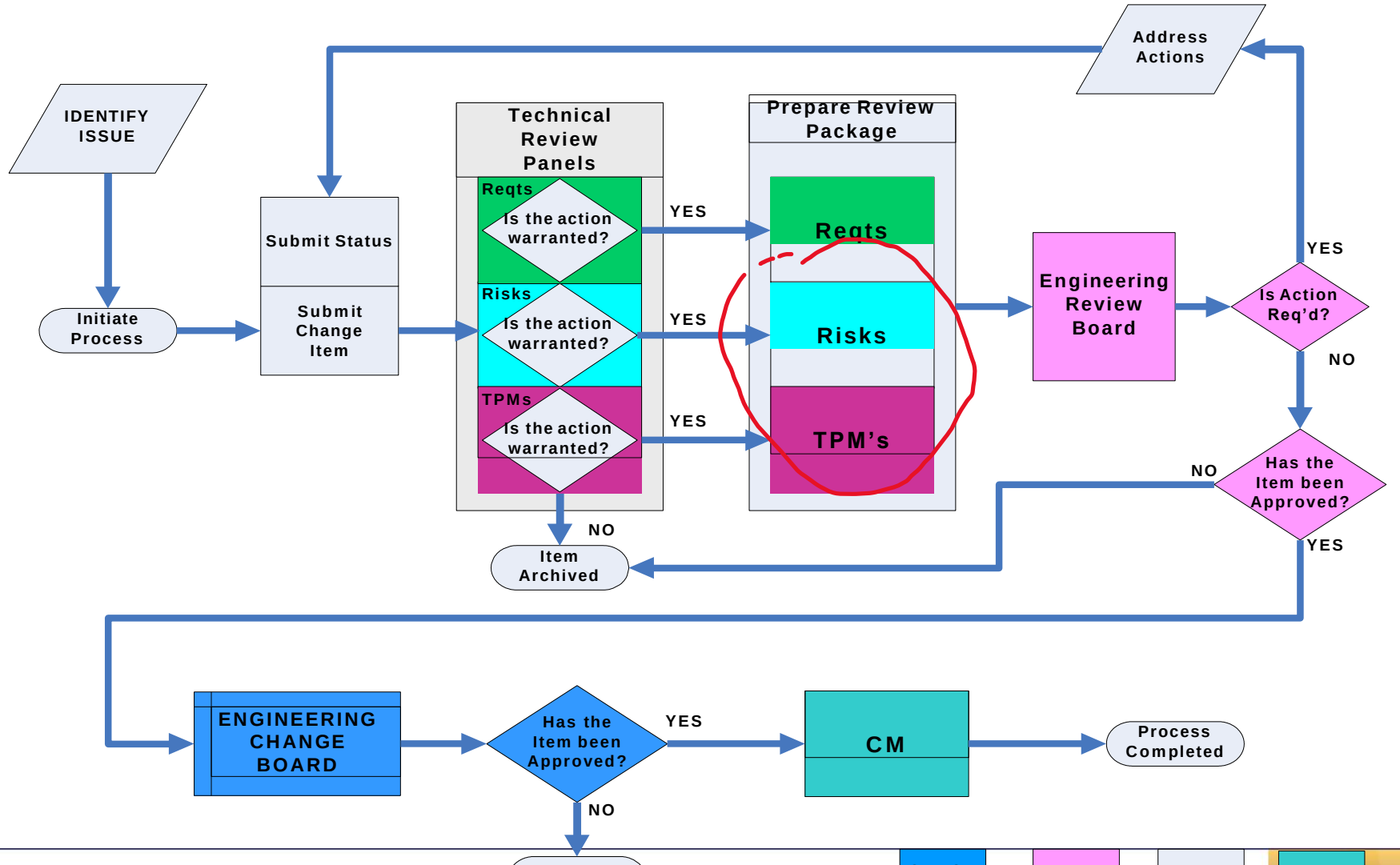
Output of PDR

End products in the form of mockups, trade study results, specification and interface documents, and Prototypes.

How to get to PDR

- Main Goal and Objective
- Functional Mission and Concept of Operations
- Develop High Level Requirements
- Identify Key Driving Requirements
- Define Verification Methods
- Identify Design Solutions
- Perform Trade Studies (Identify Stakeholders)
- Develop a Work Break Down Structure (Product Based)
- Cost and Schedule
- Risk Management and Mitigation
- Technical Performance Measures
- Configuration Management

Business Rhythm



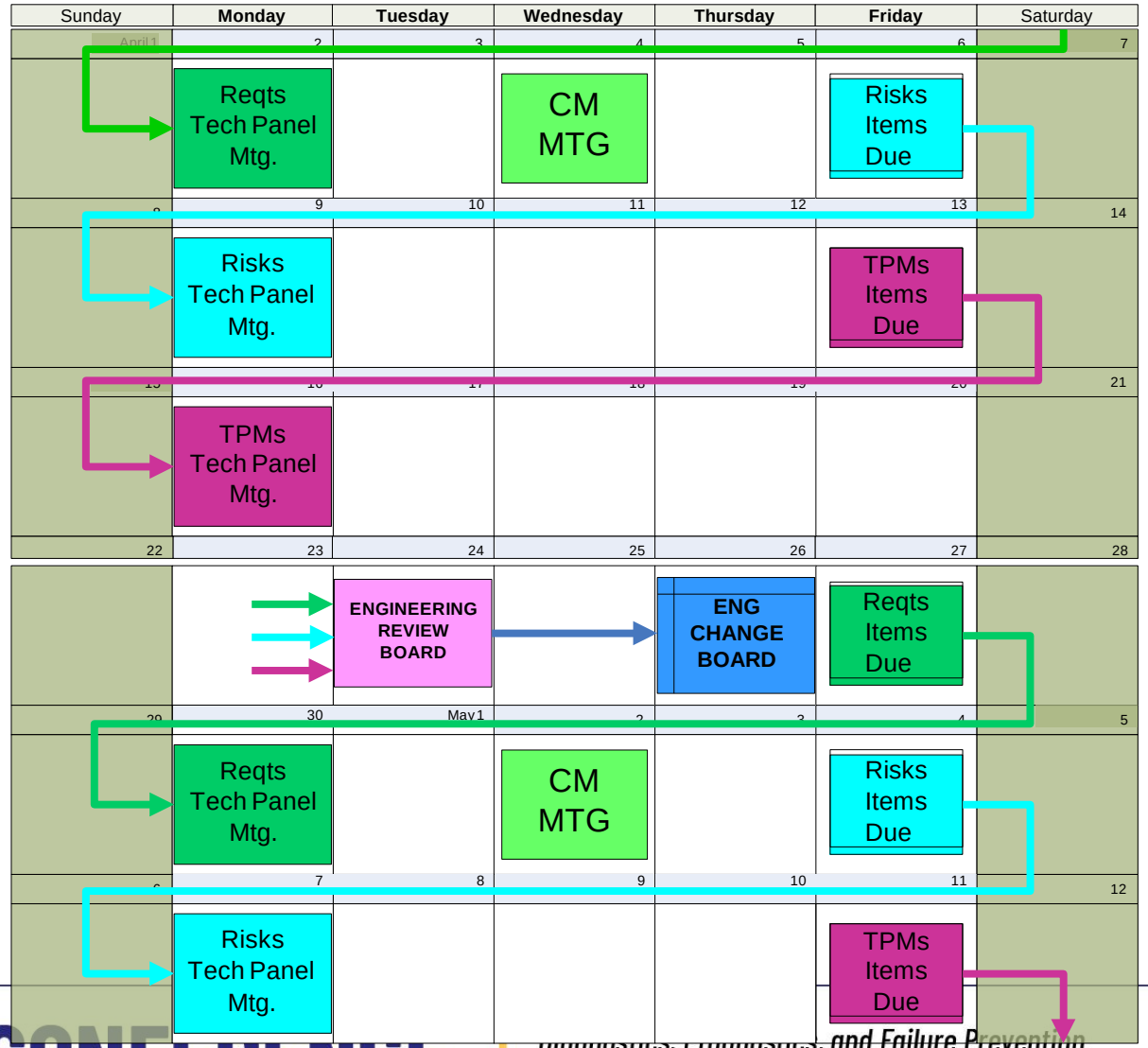
REVIEW CYCLE

WEEK1

WEEK2

WEEK3

WEEK4



System Design Processes

1 Stakeholder Expectations Definition

2Technical Requirements Definition

3 Logical Decomposition

4 Design Solution Definition

Stakeholder Expectations

- Understand User Requirements
- High Level Specifications
- Lessons Learned

Understand User Requirements

- Need?
- User vision?
- Cost?
- Risk?
- Educate diplomatically

Requirements Definition

- Tools for Discovery
  - Con Ops
  - Functional Analysis
  - Logical Decomposition

High Level Specifications

- Functional Characteristics
- Thresholds/uncertainty
- Operational Goal
- Key Performance Parameters (KPPs)

KPPs

- Most essential (speed, accuracy. . .)
- Need a threshold (minimum value)
- Operational Goal metrics
- Document in High Level Program Requirements

Types of Requirements

- Functional – what does it do?
- Operational – how is it operated?
- Constraints/Ground Rules – restrictions on development, operation, support
- Performance – How does it perform?
- Process – Prevailing guidelines and procedures the system is designed in.

Requirements vs. Specifications

- Requirement = states a problem
- Specification = is a solution
- Can be one in the same. For example:
  - Logistics
  - Materials Processes
  - Reliability
  - Availability
  - Interchangeability
  - Other –ilities
  - Interfaces
  - Workmanship (some kind of metric)
  - Physical Properties

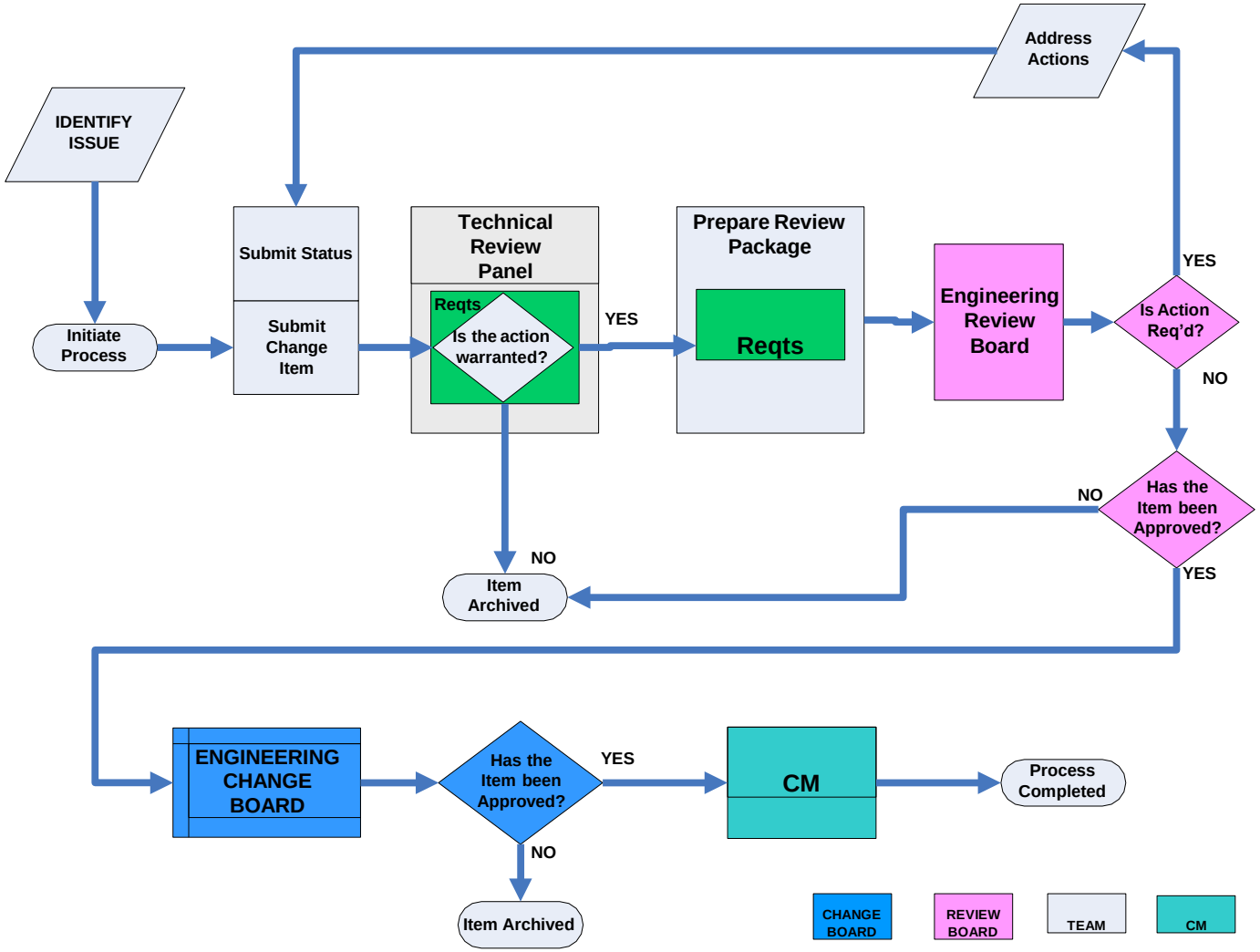
Deriving Requirements Lessons Learned

- Achievable
- Verifiable (VCRM!!)
- Crystal clear
- Completeness
- Appropriate level
- Reflects need not solution (no design solution at high level)

Deriving Requirements Lessons Learned

- One “shall” per requirement
- One requirement at a time.
- Use simplest language possible
- Plan to iterate
- “Will” is statement of intent but not binding.
- “must” shall not be used

Requirements Review Process



Requirements Traceability

High Level Requirements	Design Solution	sub system detail
DR28 All critical dimensions shall be field verified prior to finalization of design.	DR28.1 AAPL historical field implementation methodology shall be used.	DR28.1.1 Actual Field implementation
Rationale: Quality	V27.2 Analysis: Report: AAPL DART Fuel Tank Implementation	DR10.1.1 NNC12BA01B, GESS-3 Task 483 DART/AAPL Facility Integration Fuel System Engineering Report
		DR5.2.1 NNC12BA01B, GESS-3 Task 484 DART/AAPL Facility Integration DART test stand Engineering Report
		DR27.2.1 Field Implementation following Report specifications in AAPL DART Fuel Tank Implementation

Verification and Validation

The purpose of the V&V Plan is to identify the activities (right way) that will establish compliance with the requirements (verification) and to establish that the system will meet the customers' expectations (the right thing) (validation)

Verification

- A Verification Matrix (VM) is generated to show the requirement traceability and closure methodology.

Verification Definitions

- Demonstration: Showing the use of an end product achieves the individual specified requirement. It is generally a basic confirmation of performance capability, differentiated from testing by the lack of detailed data gathering. Demonstrations can involve the use of physical models or mock-ups; for example, a demonstration could be the actual operation of the end product by highly-qualified personnel who perform a one-time event that demonstrates a capability to operate at extreme limits of system performance, an operation not normally expected from a representative operation of the product.

Verification Definitions

- Inspection: The visual examination of a realized end product or drawing. Inspection is generally used to verify physical design features or specific manufacturer identification. For example, if there is a requirement that the safety arming pin has a red flag with the words “Remove Before Flight” stenciled on the flag in black letters, a visual inspection of the arming pin flag can be used to determine if this requirement was met.

- Analysis: The use of mathematical modeling and analytical techniques to predict the suitability of a design to stakeholder expectations based on calculated data or data derived from lower system structure end product verifications. Analysis is generally used when a prototype; engineering model; or fabricated, assembled, and integrated product is not available. Analysis includes the use of modeling and simulation as analytical tools. A model is a mathematical representation of reality. A simulation is the manipulation of a model. Analysis can include verification by similarity of a heritage product.

Verification Definitions

- Test: The use of an end product to obtain detailed data to verify performance, or provide sufficient information to verify performance through further analysis. Testing can be conducted on final end products, breadboards, brass boards or prototypes. Testing produces data at discrete points for each specified requirement under controlled conditions and is the most resource-intensive verification technique. As the saying goes, *"Test as you fly, and fly as you test."* Testing can also be done in facilities that simulate flight conditions. Also done to verify and validate CFD and other flow simulation modeling software development.

APPENDIX B: VERIFICATION CROSS REFERENCE

Table B1: Verification Cross Reference Matrix (VCRM)

Require. No.	Requirement Text	Verif. Method	Verification Text
SS14	The System shall be delivered with the necessary alignment tools provided and a procedural document for set up and alignment	I	Inspect deliverables list
SS15	The System shall have protective dust covers for any new mirrors that are specified	I	Inspect deliverables list
SS16	Existing mirror protective covers shall be tested for fit and can be modified to fit new structure if used in the new system.	D	Demonstrate capability at end use
SS17	The System shall include a light shutter on the output of the light source.	D	Demonstrate capability at end use
SS18	The System shall have remote operation capability.	I	Inspection of drawings

Validation Testing

a NASA and Boeing test team subjected a test version of the Space Launch System (SLS) liquid hydrogen tank to a series of 37 tests that simulate liftoff and flight stresses.

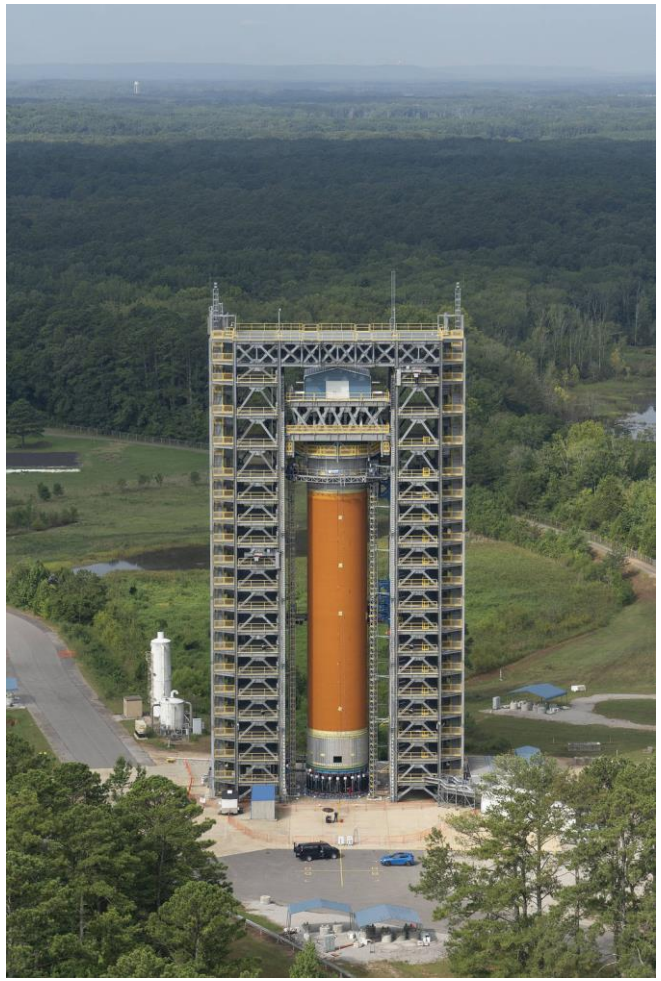


Image credit NASA/MSFC

Need guideline when NOT to use Agile Development
Don’t use it when consequences of failure outweigh the benefits

Design Solutions and Trade Studies

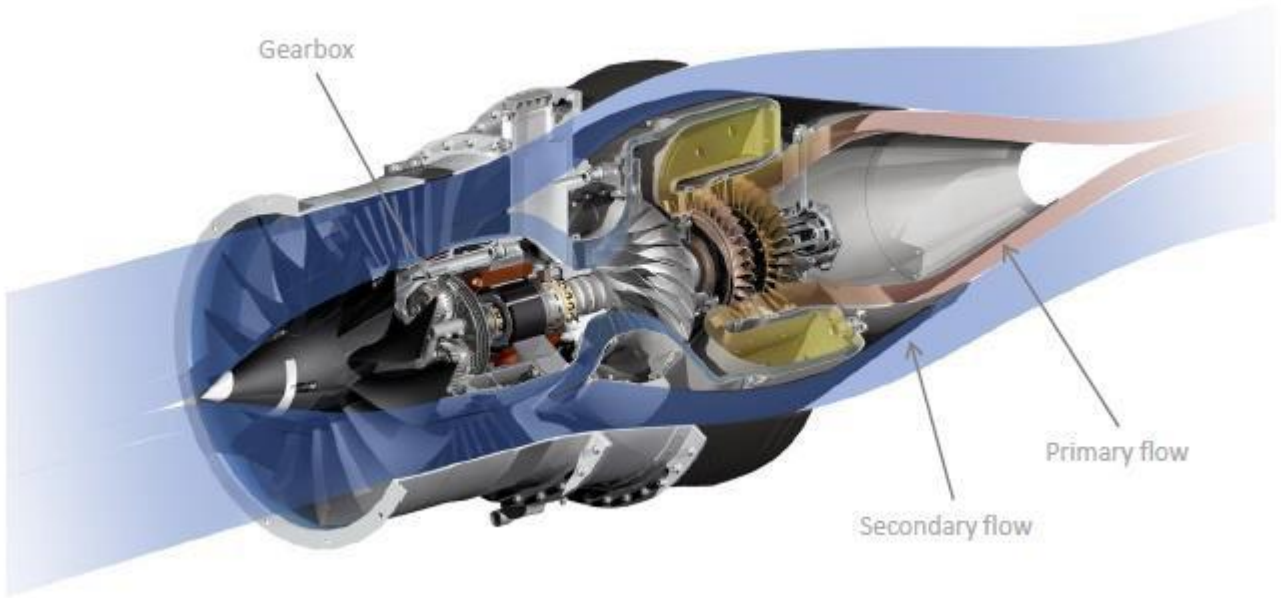
Trade Studies and the Decision Analysis Process

- Used to:
  - Evaluate technical issues and alternatives
  - Evaluate uncertainties in decision making support
- Used throughout:
  - System design
  - Technical management
  - Product realization

Basic Principles

1. Define the Objective (requirements analysis)
2. Identify alternatives (concept exploration)
3. Compare the alternatives (definition)
4. Sensitivity analysis (validation)

Risk Management



Risk Management

Top PDR Identified Risks

1. Life Cycle Fatigue failure
2. Fire in the engine
3. Overheating of electronics
4. Fuel System leak
5. Over-speed hardware failure
6. Data compromised by blast shield
7. Single engine/controls/parts supplier
8. Hardware damage during relocation
9. Heavy Maintenance technical support
10. Damage of Critical or long lead item

Risk Management

Top PDR Identified Risks

1. Life Cycle Fatigue failure (analysis complete)
2. Fire in the engine (accepted by project)
3. Overheating of electronics (monitor temperature)
4. Fuel System leak (Dikes, procedure, welded, visual)
5. Over-speed hardware failure (multiple speed control, shield)
6. Data compromised by blast shield (not in use during research)
7. Single engine/controls/parts supplier (live with it)
8. Hardware damage during relocation (inspection)
9. Heavy Maintenance technical support (maintenance contract)
10. Damage of Critical or long lead item (limited to engine components)

Risk Management

Newly Identified Risks

11. Redesigned Engine does not pass testing

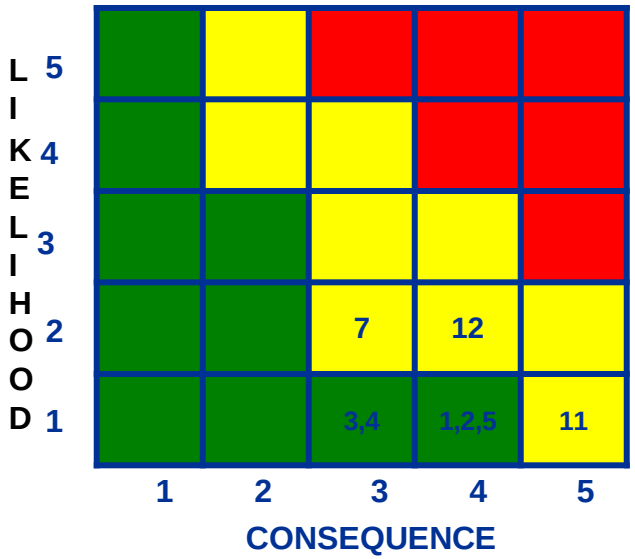
- Unmodified engine has been tested and met vendor historical standards
- Redesigned/modified engine will be tested 22-March-2017

12. Labor force not sufficient to complete the tasks

- Will communicate need to project and management regularly

DART Top Risk List

May 12, 2016



Legend

- Decreasing (Improving)
- Increasing (Worsening)
- 9 Unchanged
- $ Cost Threat (Level 1, 2, 3)

Rank	Trend	Title	Owning Team	LIKE	Consequence			
					SAFE	PERF	SCH	COST
	9			3	0	0	3	0
CANDIDATE RISKS								
~~1~~	↓	~~1- High Cycle Fatigue~~	~~Des.~~	~~2~~	~~4~~	~~3~~	~~4~~	~~4~~
~~3~~	↓	~~2- Fire in engine~~	~~Des.~~	~~1~~	~~3~~	~~3~~	~~4~~	~~4~~
~~4~~	↓	~~3- Overheating of electronics~~	~~Des.~~	~~1~~	~~3~~	~~1~~	~~1~~	~~3~~
~~5~~	↓	~~4-Fuel system leak~~	~~Res.~~	~~1~~	~~3~~	~~0~~	~~1~~	~~1~~
~~2~~	↓	~~5-Rotating hardware failure containment~~	~~Des.~~	~~1~~	~~4~~	~~0~~	~~3~~	~~3~~
3	9	7- supplier	Des.	2	0	3	3	3
1	9	11 – modified engine doesn't pass test	Des.	1	0	5	5	5
2	9	12 = labor force not available	Prog.	2	0	0	4	3
ASSOCIATED RISKS								
	9							
	9							
	9							

Conclusions

1. Using Systems Engineering processes ensures project success
2. With Robust Verification and Validation processes in place, you can:
   - Plan for initial success with minimal failures along the way
   - use agile development to iterate often and — where engineers confirm a minimally viable design and then develop a minimally viable product very quickly.
3. Agile development can be used on smaller projects but depends on the cost and schedule constraints.
4. Agile development introduces RISK due to quick turnaround mentality and must be used wisely

References/Acknowledgements

1. National Institute of Aerospace – Systems Engineering: Chapter 2
2. Wikipedia – Systems Engineering
3. NASA Systems Engineering Handbook NASA/SP-2007-6105 Rev 1
4. Systems Engineering Fundamentals – Space Mission Excellence Program 2008
5. INCOSE Systems Engineering Handbook
6. Systems Engineering Awareness, J. Lucero, MFPT 2017 May 16, 2017
7. The Systems Engineering Method, J. Lucero MFPT2015
8. A Functional Analysis of the Society for Machinery Failure Prevention Technology, J Lucero 2018
9. https://www.nasa.gov/feature/glenn/2023/nasas-modern-history-makers-david-avanesian

Questions?

- Presenter Contact Information: John.M.Lucero 216 433 2684
- MFPT Discussion Forum: https://www.linkedin.com/groups/8920840/