THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Failure as an Option: Mission Assurance and Systems Engineering

Timothy White

The Plan

Get your facts first, and then you can distort 'em as much as you please.

- Mark Twain

Discussion Points

- Mission Assurance and Systems Engineering: Better together?
- The breadth of the disciplines
- Standards and comparisons
- An example
- Research Question
- Tools
- Opportunity space
- Next Steps

Mission Assurance and Systems Engineering Alignment

Mission assurance (MA) is defined as the disciplined application of proven scientific, engineering, quality, and program management principles towards ***the goal of achieving mission success***. MA follows a general systems engineering (SE) framework and uses risk management (RM) and independent assessment as cornerstones throughout the program life cycle. (Guarro, Johnson-Roth, Tosney, 2012)

Systems Engineering is an interdisciplinary approach and means to ***enable the realization of successful systems***. It focuses on defining customer needs and required functionality early in the development cycle, documenting requirements, then proceeding with design synthesis and system validation while considering the complete problem:

Operations
Performance
Test
Manufacturing
Cost & Schedule
Training & Support
Disposal

Systems Engineering integrates all the disciplines and specialty groups into a team effort forming a structured development process that proceeds from concept to production to operation. Systems Engineering considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs. (INCOSE)

Comparison of Breadth

Element	Systems Engineering	Mission Assurance
Industry recognized functions	☑	☑
Employment opportunities	☑	☑
Technical Journals	☑	
Higher Education Programs	☑	
Professional Societies	☑	
Discipline Certification	☑	
Industry Conferences	☑	☑

Lower breadth, but are there opportunities?

ISO/IEC/IEEE 15288 Processes

6.1.1 Acquisition	6
6.1.2 Supply	6
6.2.1 Life Cycle Model management	8
6.2.2 Infrastructure management	5
6.2.3 Portfolio management	7
6.2.4 Human resource management	5
6.2.5 Quality management	6
6.2.6 Knowledge Management	7
6.3.1 Project planning	8
6.3.2 Project assessment and control	6
6.3.3 Decision management	8
6.3.4 Risk management	11
6.3.5 Configuration management	11
6.3.6 Information management	6
6.3.7 Measurement	8
6.3.8 Quality assurance	8
6.4.1 Business or mission analysis	6
6.4.2 Stakeholder needs and requirements definition	10
6.4.3 System requirements definition	12
6.4.4 Architecture definition	11
6.4.5 Design definition	9
6.4.6 System analysis	6
6.4.7 Implementation	7
6.4.8 Integration	8
6.4.9 Verification	9
6.4.10 Transition	5
6.4.11 Validation	11
6.4.12 Operation	7
6.4.13 Maintenance	9
6.4.14 Disposal	7

ISO/IEC/IEEE 15288 Processes

6.4.3 System requirements definition	12
6.3.4 Risk management	11
6.3.5 Configuration management	11
6.4.4 Architecture definition	11
6.4.11 Validation	11
6.4.2 Stakeholder needs and requirements definition	10
6.4.5 Design definition	9
6.4.9 Verification	9
6.4.13 Maintenance	9
6.2.1 Life Cycle Model management	8
6.3.1 Project planning	8
6.3.3 Decision management	8
6.3.7 Measurement	8
6.3.8 Quality assurance	8
6.4.8 Integration	8
6.2.3 Portfolio management	7
6.2.6 Knowledge Management	7
6.4.7 Implementation	7
6.4.12 Operation	7
6.4.14 Disposal	7
6.1.1 Acquisition	6
6.1.2 Supply	6
6.2.5 Quality management	6
6.3.2 Project assessment and control	6
6.3.6 Information management	6
6.4.1 Business or mission analysis	6
6.4.6 System analysis	6
6.2.2 Infrastructure management	5
6.2.4 Human resource management	5
6.4.10 Transition	5

Requirements
Technical Management
Design

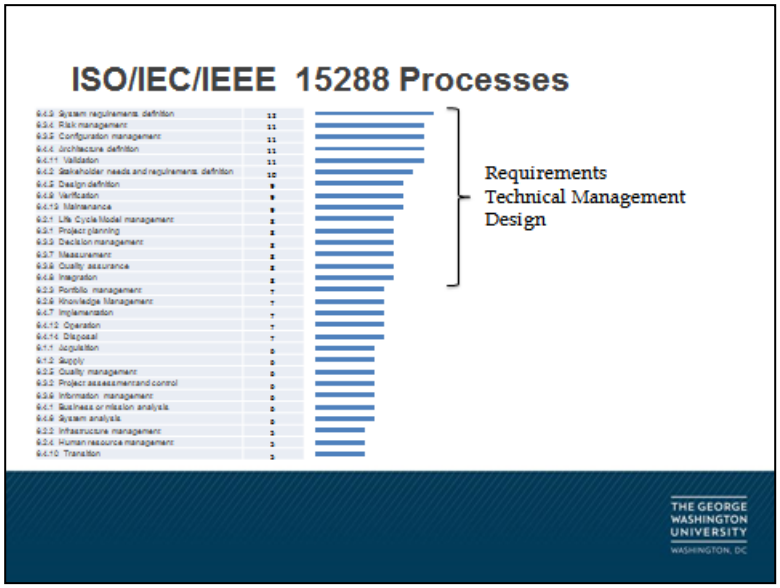
Mission Assurance Program Framework

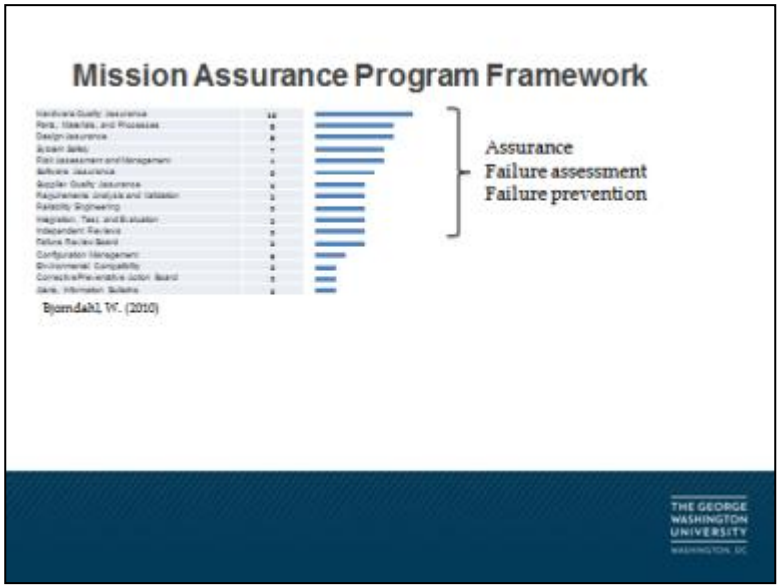
Hardware Quality Assurance	10
Parts, Materials, and Processes	8
Design Assurance	8
System Safety	7
Risk Assessment and Management	7
Software Assurance	6
Supplier Quality Assurance	5
Requirements Analysis and Validation	5
Reliability Engineering	5
Integration, Test, and Evaluation	5
Independent Reviews	5
Failure Review Board	5
Configuration Management	3
Environmental Compatibility	2
Corrective/Preventative Action Board	2
Alerts, Information Bulletins	2

Assurance
Failure assessment
Failure prevention

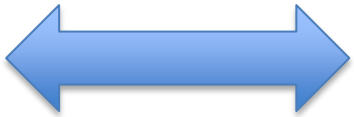
Bjorndahl, W. (2010)

Dichotomy of Focus



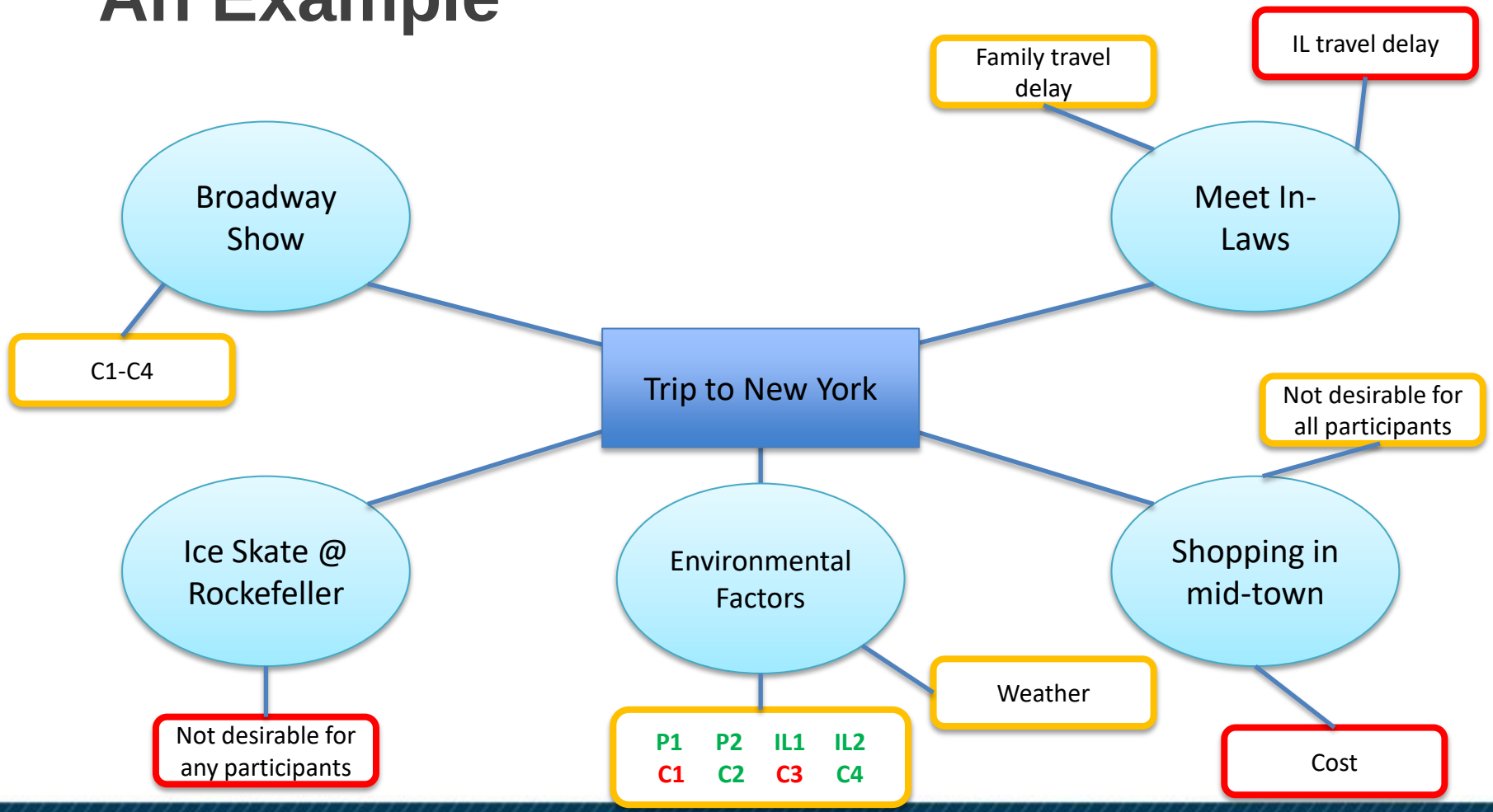


CREATIVE ACTIVITIES



FAILURE ACTIVITIES

An Example

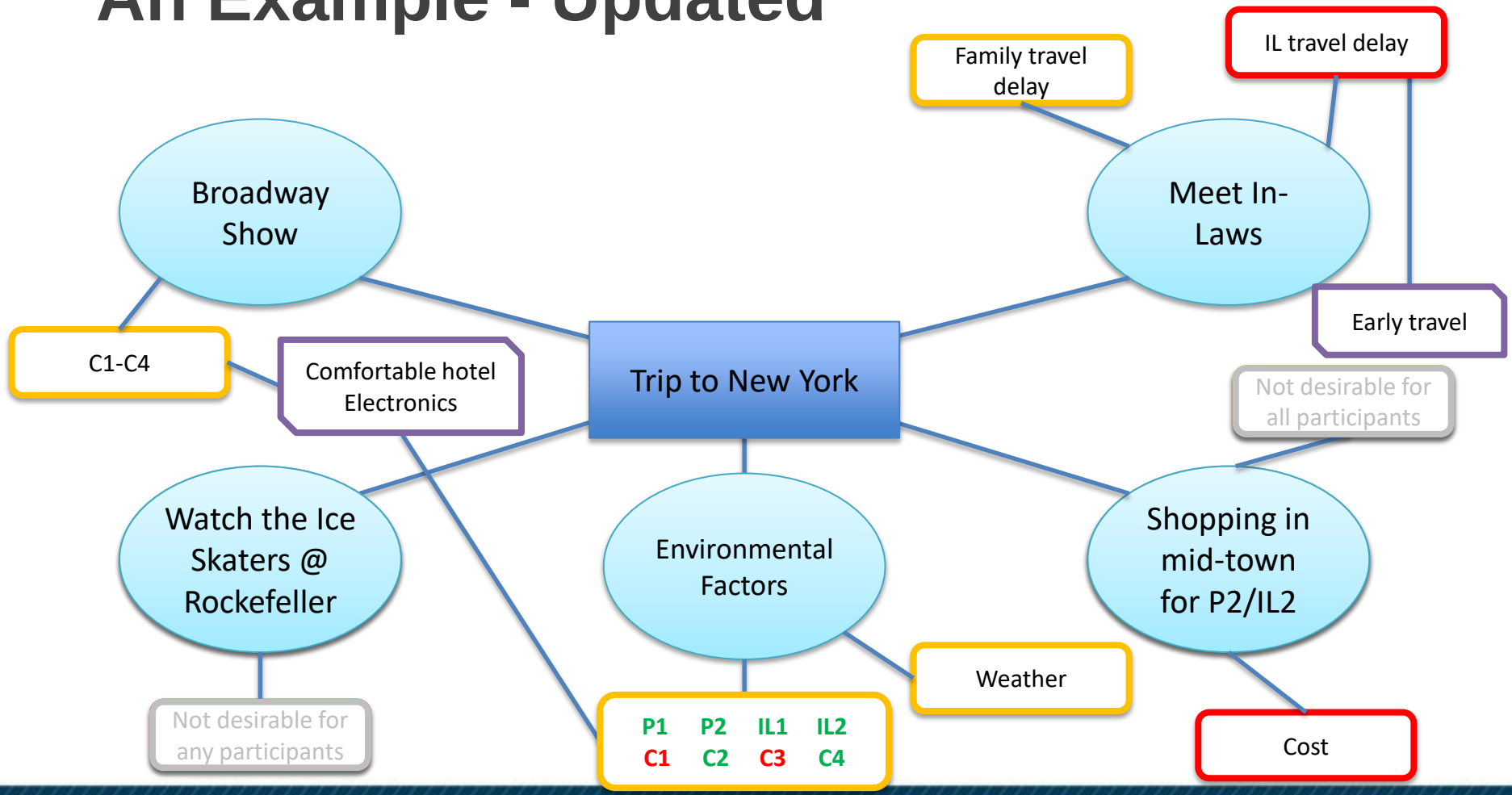


Objective

Requirement

Failure

An Example - Updated



Research Approach

Research Hypothesis:

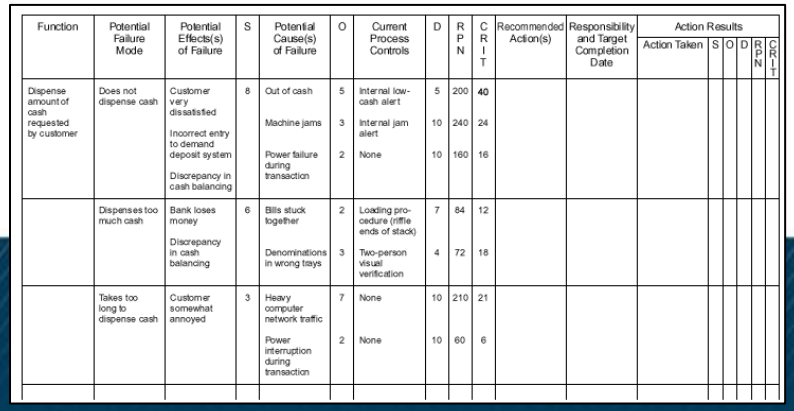
Applying anticipatory failure tools in the early requirements elicitation process yields a more complete and robust set of project requirements.

Research Questions:

- Where in the Systems Engineering process is failure typically considered?
- What tools currently exist?
- Are there opportunities to move these processes earlier?
- Are there tools that can be leveraged to improve results?

Failure Tools: FMEA

- Typically used to assess and prioritize risk
- Suggested usage in early design; typical usage is during component design or system operation
- Characteristics:
  - Identify failure modes
  - Identify failure effects
  - Assign severity, probability of occurrence, probability of detection
  - Calculate Risk Priority Number

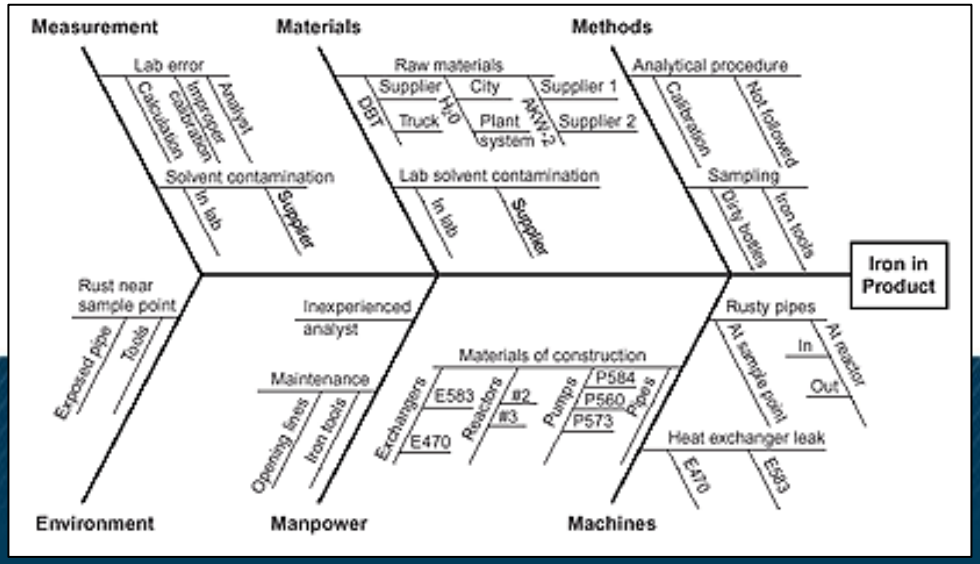


Function	Potential Failure Mode	Potential Effects(s) of Failure	S	Potential Cause(s) of Failure	O	Current Process Controls	D	RPN	CRIT	Recommended Action(s)	Responsibility and Target Completion Date	Action Results					
												Action Taken	S	O	D	RPN	CRIT
Dispense amount of cash requested by customer	Does not dispense cash	Customer very dissatisfied	8	Out of cash	5	Internal low-cash alert	5	200	40								
		Incorrect entry to demand deposit system		Machine jams	3	Internal jam alert	10	240	24								
		Discrepancy in cash balancing		Power failure during transaction	2	None	10	160	16								
	Dispenses too much cash	Bank loses money	6	Bills stuck together	2	Loading procedure (riffle ends of stack)	7	84	12								
		Discrepancy in cash balancing		Denominations in wrong trays	3	Two-person visual verification	4	72	18								
	Takes too long to dispense cash	Customer somewhat annoyed	3	Heavy computer network traffic	7	None	10	210	21								
				Power interruption during transaction	2	None	10	60	6								

Tague, N. (2005)

Failure Tools: Fishbone

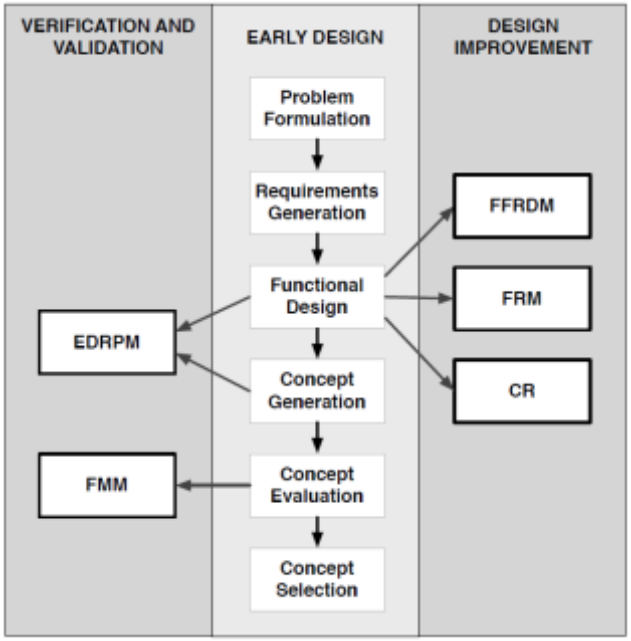
- Also called a ‘Cause and Effect Diagram’ or ‘Ishikawa’
- Used to diagnose causes of failure
- Can be particularly useful when group cannot close on a failure cause
- Failure evidence is recorded on the right; possible contributing factors are grouped and diagrammed hierarchically

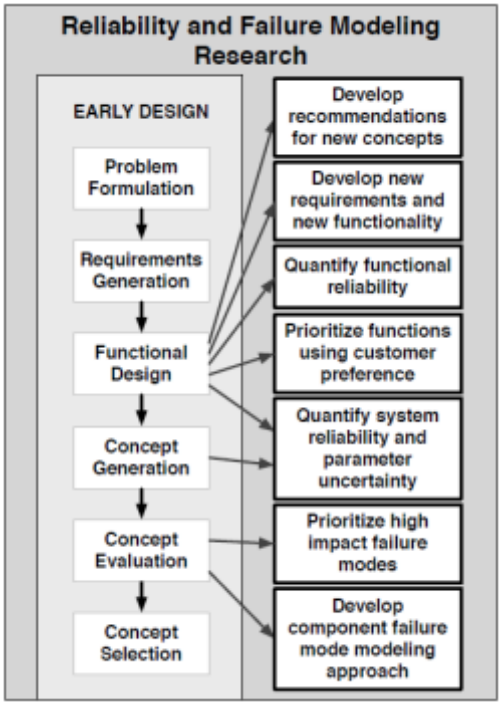


Tague, N. (2005)

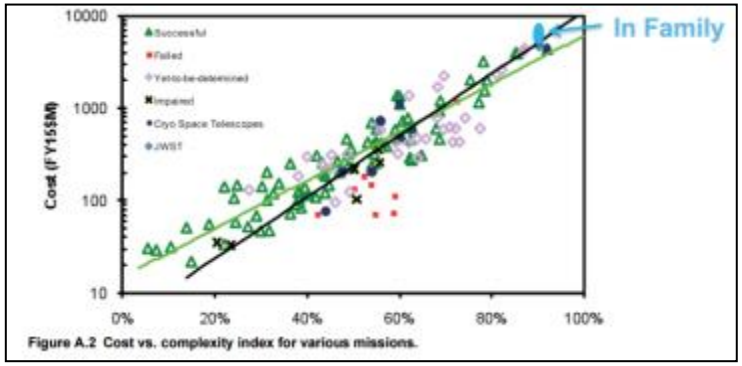
Prior Art

O'Halloran (2013) provides a framework to model reliability and failures early in the design process

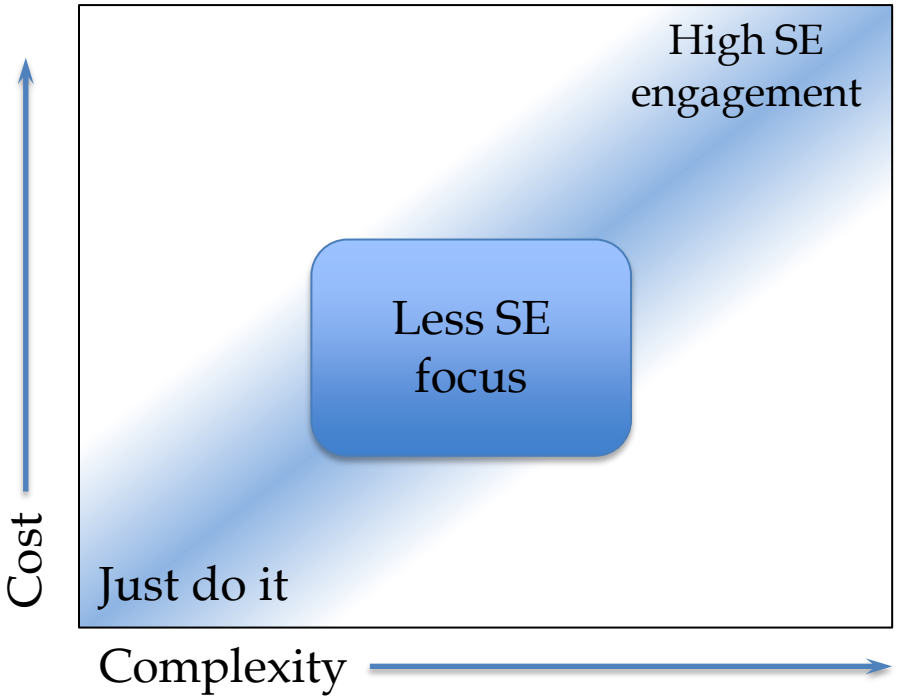




Opportunity Space



Ballhaus et al (2010)



"The function of systems engineering is to guide the engineering of complex systems" Kossiakoff (2003)

Research Objective: Further knowledge and advance SE capabilities

Next Steps

- Modified FMEA / Fault Tree approach to support requirement elicitation process
- Historical case studies
- Data collection / data identification
- Analysis
- Results publication

Contact Information

Timothy White

timothywhite@gwmail.gwu.edu

References

15288-2008 ISO. (2008). *Systems and software engineering – System life cycle processes.* IEEE / Institute of Electrical and Electronics Engineers Incorporated.

Ballhaus Jr, W., Casani, J., Dorman, S., Gallagher, D., Illingworth, G., Klineberg, J., Schurr, D. (2010) *James Webb Space Telescope (JWST) Independent Comprehensive Review Panel (ICRP).*

Bjorndahl, W. (2010) *Mission Assurance Program Framework*. Aerospace Report TOR-2010(8591)-18.

Guarro, S., Johnson-Roth, G., and Tosney, W. (Editors), (2012) *Mission Assurance Guide*. Aerospace Report TOR-2007(8546)-6018 REV B.

INCOSE *What is Systems Engineering?* Retrieved from http://www.incose.org/AboutSE/WhatIsSE

Kossiakoff, A., Sweet, W. (2003) *Systems Engineering Principles and Practice.* John Wiley and Sons, Hoboken, New Jersey

O'Halloran, B. (2013) *A Framework to Model Reliability and Failures in Complex Systems During the Early Engineering Design Process.* Retrieved from ProQuest Digital Dissertations. UMI Number: 3574327.

Tague, N. (2005) *The Quality Toolbox, Second Edition*. ASQ Quality Press.