Mission Assurance for the Enterprise

Barbara Braun
The Aerospace Corporation

November 2023

Approved for Public Release. OTR202400097

Existing Cybersecurity Matrices

MITRE | ATT&CK

Matrices · Tactics · Techniques · Data Sources

layout: side · show sub-techniques · hide sub-te

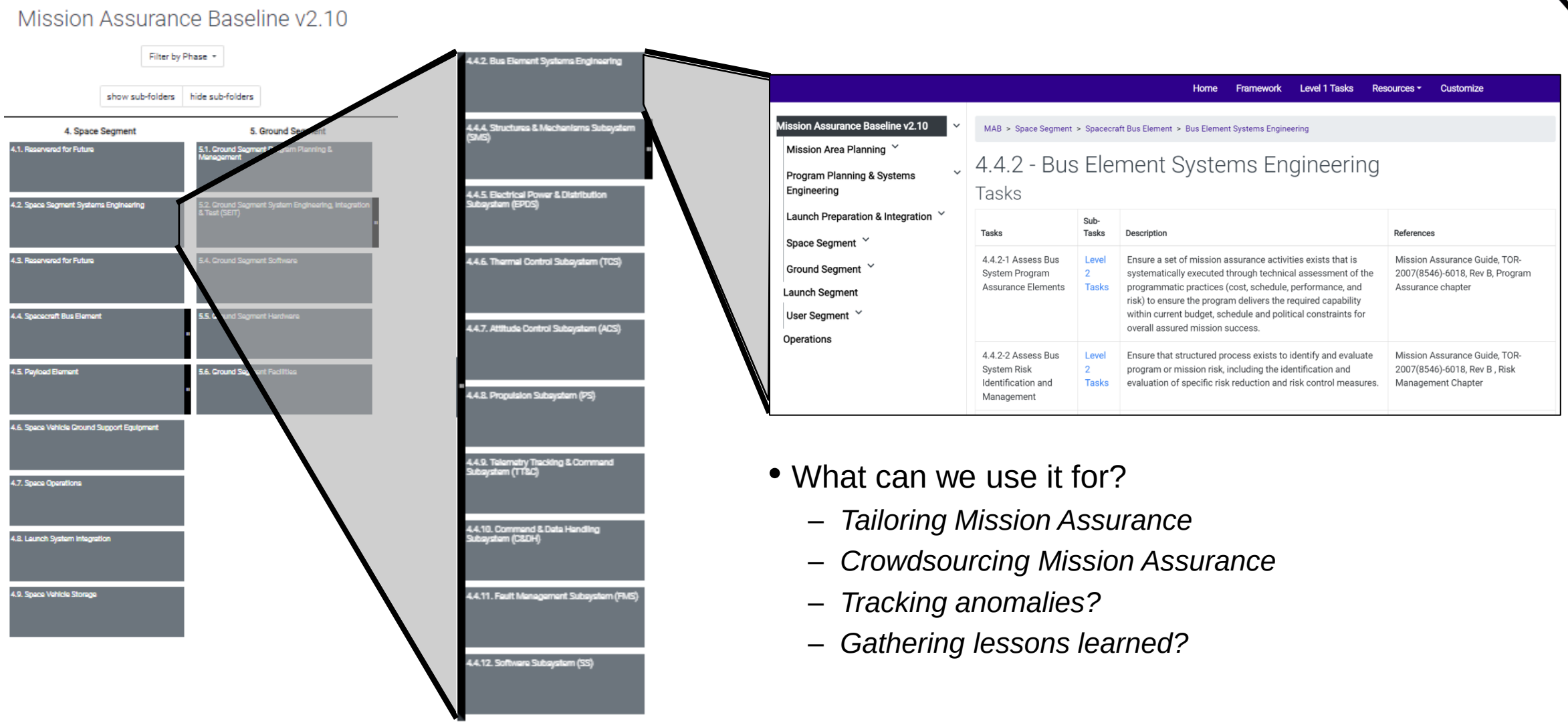
Reconnaissance (10 techniques)	Resource Development (8 techniques)	Initial Access (9 techniques)	Execution (14 techniques)	Persistence (19 techniques)	Privilege Escalation (13 techniques)	Defense Evasion (42 techniques)	Credential Access (17 techniques)
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain Compromise (3)	Native API	Create Account (3)	Escape to Host	Deploy Container	
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Scheduled Task/Job (5)	Create or Modify System Process (4)	Event Triggered Execution (16)	Direct Volume Access	
Search Open Websites/Domains (3)		Valid Accounts (4)	Serverless Execution	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Domain Policy Modification (2)	
Search Victim-Owned Websites			Shared Modules	External Remote Services	Hijack Execution Flow (12)	Execution Guardrails (1)	
			Software Deployment Tools	Hijack Execution Flow (12)	Process Injection (12)	Exploitation for Defense Evasion	
			System Services (2)	Implant Internal Image	Scheduled Task/Job (5)	File and Directory Permissions Modification (2)	
			User Execution (3)	Modify Authentication Process (8)	Valid Accounts (4)	Hide Artifacts (10)	
			Windows Management Instrumentation	Office Application Startup (6)		Hijack Execution Flow (12)	
				Pre-OS Boot (5)		Impair Defenses (10)	
				Scheduled Task/Job (5)		Indicator Removal (9)	
						Indirect Command Execution	
						Masquerading (8)	
						Modify Authentication Process (8)	
						Modify Cloud Compute Infrastructure (4)	

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

show sub-tec

Reconnaissance (9 techniques)	Resource Development (5 techniques)	Initial Access (12 techniques)	Execution (18 techniques)
Gather Spacecraft Design Information (9)	Acquire Infrastructure (4)	Compromise Supply Chain (3)	Replay (2)
Gather Spacecraft Descriptors (3)	Compromise Infrastructure (3)	Compromise Software Defined Radio (0)	Position, Navigation, and Timing (PNT) Geofencing (0)
Gather Spacecraft Communications Information (4)	Obtain Cyber Capabilities (2)	Crosslink via Compromised Neighbor (0)	Modify Authentication Process (0)
Gather Launch Information (1)	Obtain Non-Cyber Capabilities (4)	Secondary/Backup Communication Channel (2)	Compromise Boot Memory (0)
Eavesdropping (4)	Stage Capabilities (2)	Rendezvous & Proximity Operations (3)	Exploit Hardware/Firmware Corruption (2)
Gather FSW Development Information (2)		Compromise Hosted Payload (0)	Disable/Bypass Encryption (0)
Monitor for Safe-Mode Indicators (0)		Compromise Ground System (2)	Trigger Single Event Upset (0)
Gather Supply Chain Information (4)		Rogue External Entity (3)	Time Synchronized Execution (2)
Gather Mission Information (0)		Trusted Relationship (3)	Exploit Code Flaws (3)
		Exploit Reduced Protections During Safe-Mode (0)	Malicious Code (4)
		Auxiliary Device Compromise (0)	Exploit Reduced Protections During Safe-Mode (0)
		Assembly, Test, and Launch Operation Compromise (0)	Modify On-Board Values (13)
			Flooding (2)
			Jamming (3)
			Spoofing (5)
			Side-Channel Attack (0)
			Kinetic Physical Attack (2)
			Non-Kinetic Physical Attack (3)

Mission Assurance Baseline Matrix



- What can we use it for?
  - *Tailoring Mission Assurance*
  - *Crowdsourcing Mission Assurance*
  - *Tracking anomalies?*
  - *Gathering lessons learned?*

The System Engineering “V”

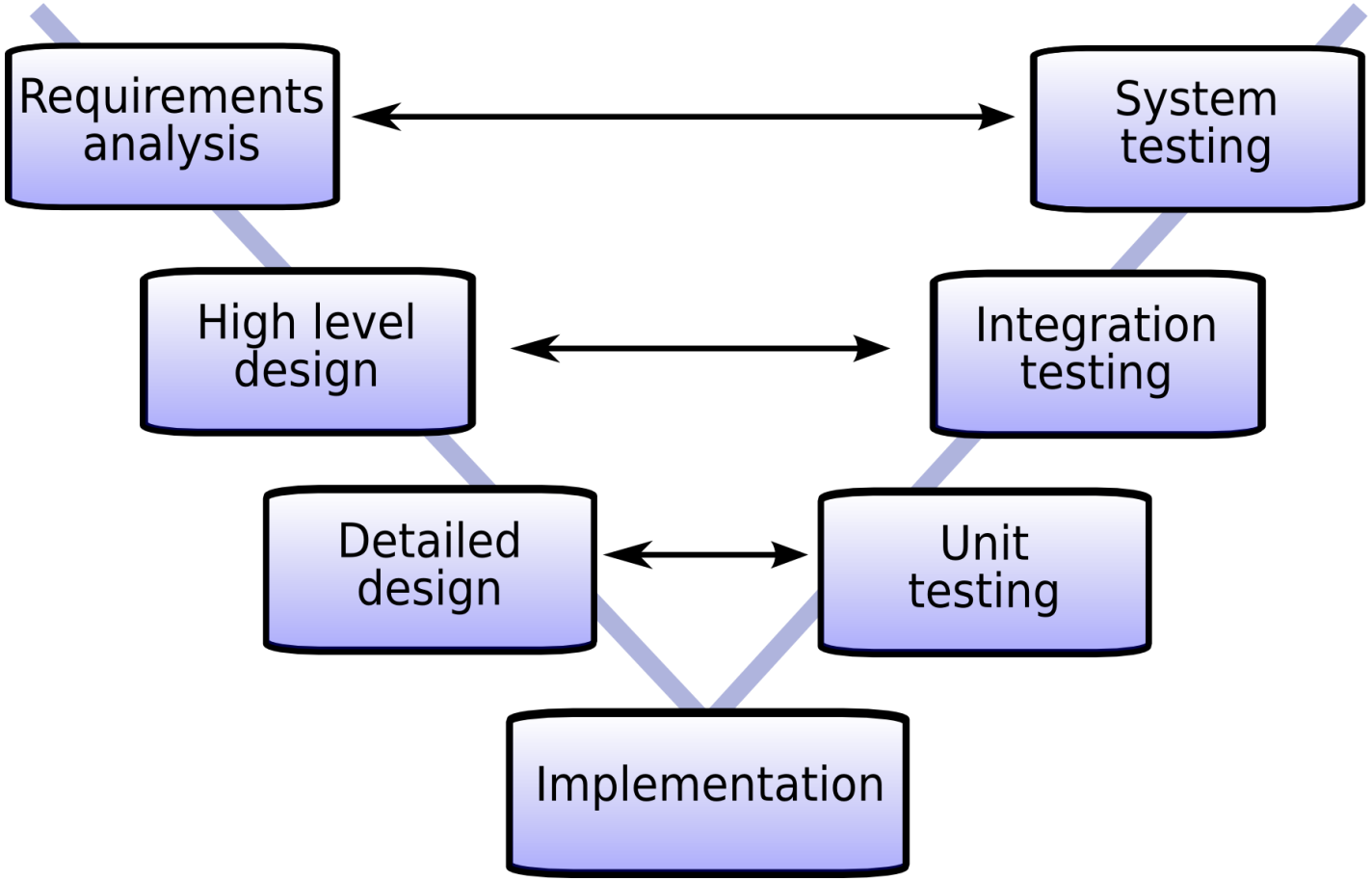


Image Credit: Herman Bruyninckx, used under Creative Commons Share-Alike 3.0

This is “Principled Design”

Mission Assurance is heavily involved in all sides!

Produces excellent widgets

But…

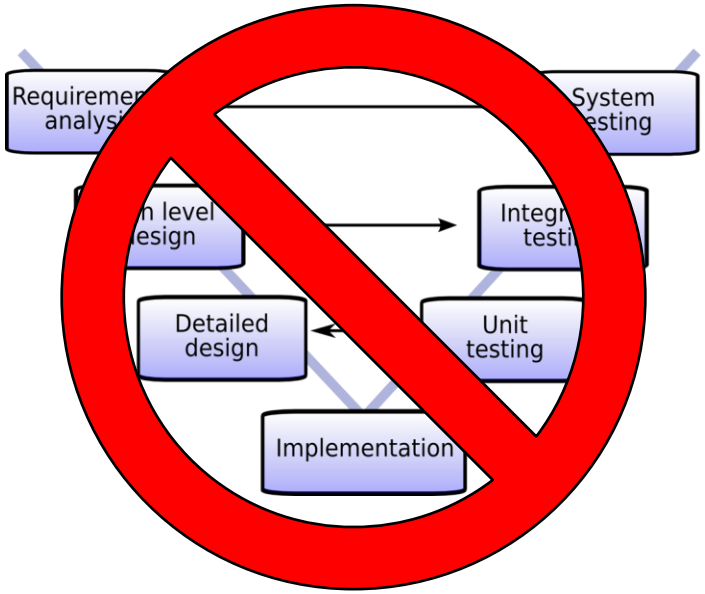
Consider the Internet…

…if it were a space acquisition program

- Possible Key Performance Parameters:
  - *The system shall support at least three billion unique users on a daily basis*
  - *The system shall support at least one billion unique content sites*
  - *The system shall support exchange of at least 200 million rich text messages every minute*
  - *The system shall allow users to access sites and content via any device that conforms to a few simple communication protocols*
  - *Users shall be able to use a protocol-conforming device to send 1MB of data via the system to any protocol-conforming device anywhere on earth in less than one second*
  - *The system shall allow for near-instantaneous search of all hosted content*
  - *The system shall support secure exchange of sensitive data*
  - *The system shall achieve 99.9 percent functional availability*

From Dr. Erin Ryan, "Designing for Principles"

- If these had been the KPPs, we could reasonably expect that this program would either:
  - *Not have delivered on even a small fraction of the performance requirements*
  - *Have been cancelled*
  - *Be the most expensive program in the history of civilization*



How Do We Design an Enterprise?

- Balance performance requirements with non-functional requirements such as:
  - *Independence (Each system function or functional requirement should be satisfied by an independent design parameter)*
  - *Integrability (Characterized by compatibility and interoperability)*
  - *Decentralization (Characterized by a decentralized distribution of control, information, resources, attributes, and properties within the system architecture)*
  - *Flexibility*
  - *Adaptability*
  - *Modifiability*
  - *Simplicity*
  - *Modularity*
  - *Scalability*
  - *Redundancy*

We need mission assurance processes that examine these factors!

List from Dr. Erin Ryan, "Designing for Principles" and Armin Schulz and Ernst Fricke, "Design for Changeability"

How Do We Assure an Enterprise?

- What might and Enterprise Mission Assurance Baseline look like?

- What other things should we measure?

9. Enterprise Segment

Scalability

- Ensure load testing is planned and applied
- Ensure scalability testing is planned and applied
- Evaluate if additional units can be manufactured quickly
- Evaluate vertical and horizontal scaling options
- …

Modifiability

- Ensure software changes can be accomplished easily
- Ensure sufficient hardware margin is available for upgrades
- Ensure standard ISAM registration decals are applied
- …

Modularity

- Evaluate conformance to interoperability standards
- Evaluate swapability of components
- Ensure mass model availability
- Ensure availability of a digital model
- …

List from Dr. Erin Ryan, "Designing for Principles" and Armin Schulz and Ernst Fricke, "Design for Changeability"

Parting Thoughts

- Leadership in Energy and Environmental Design (LEED)
  - Developed and administered by the U.S. Green Building Council
  - Similar models exist (e.g., “meaningful use” funding for healthcare)
- Allows for an incremental approach to the adoption of enterprise and interoperability requirements

LEED v4 for BD+C: New Construction and Major Renovation
Project Checklist

Y	?	N			
			Credit	Integrative Process	1
0	0	0	**Location and Transportation**		**16**
			Credit	LEED for Neighborhood Development Location	16
			Credit	Sensitive Land Protection	1
			Credit	High Priority Site	2
			Credit	Surrounding Density and Diverse Uses	5
			Credit	Access to Quality Transit	5
			Credit	Bicycle Facilities	1
			Credit	Reduced Parking Footprint	1
			Credit	Green Vehicles	1

Space System Enterprise Certification
Project Checklist

Y	?	N			
			Credit	Integrative Process	1
0	0	0	**Location and Transportation**		**31**
			Credit	Compatible with enterprise ground requirements	10
			Credit	Uses CCSDS compatible downlink	1
			Credit	Digital twin available	2
			Credit	Complies with SSC MOSA Standard v.1.1	5
			Credit	Incorporates standard hosted payload interface	5
			Credit	Incorporates digital engineering practices	1
			Credit	Compatible with NSSL Standard Service	1
			Credit	Incorporates standard crosslink	16

https://support.usgbc.org/hc/en-us/articles/4404406912403-What-is-LEED-certification

Parting Thoughts

- What About “Inverted V” Acquisitions?

- The “Inverted V” uses existing solutions to address needs at all levels
  - Allows for “flow up” of solutions into systems into architecture to improve the enterprise
- Off-the-shelf solutions
  - Obtain readily available, or easily modifiable, products or services
- Gaps are flowed back into either the regular or inverted “V”