EMBEDDED SYSTEM THREAT MATRIX

MITRE | ESTM™

Mario F. Zuniga
Capability Area Lead for Weapon System & Defensive Critical Infrastructure
Cyber Infrastructure Protection Innovation Center, MITRE Labs

MITRE

Today's Topics

What is the Embedded System Threat Matrix?

Challenges of Cybersecurity for Non-IT Systems

- Current Cybersecurity Paradigm
- Analyzing Cybersecurity Risk for Non-IT Systems

The History of ESTM

- Why ESTM Was Created

Leveraging ESTM

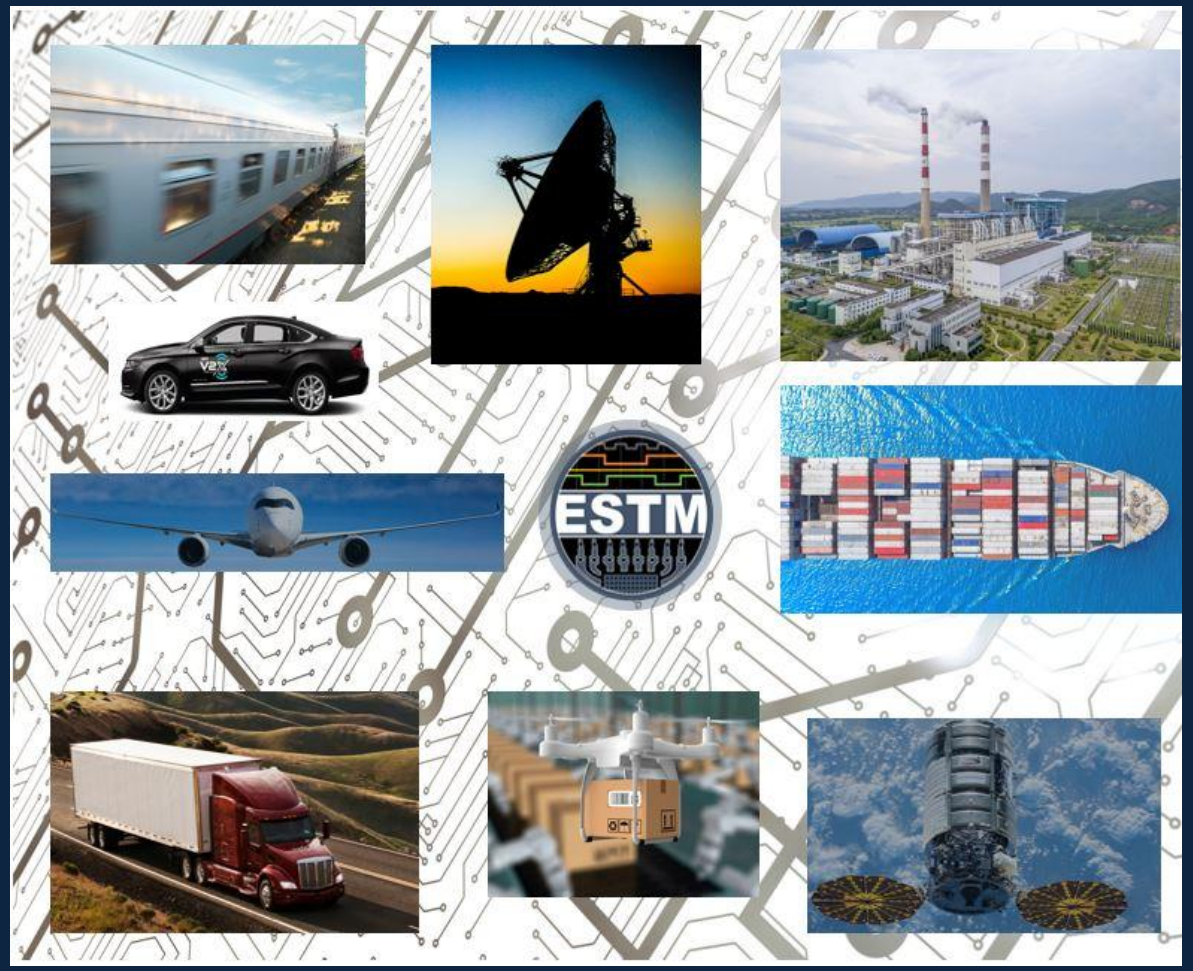
- Platform Independent Vectors of Techniques (PIVOT)
- PIVOT and ESTM Use Case
- The Fusion of Technology for Aviation
- Common Use Cases

ESTM Next Steps

MITRE

What is the Embedded System Threat Matrix?

- The MITRE-developed Embedded Systems Threat Matrix (ESTM™) is a purpose-built framework to address embedded system vulnerabilities
- Inspired by the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework
- Like ATT&CK, ESTM provides a structured approach categorizes adversarial tactics and techniques specific to embedded systems



MITRE

Sample ESTM Tactics and Techniques

ESTM Tactics

- Reconnaissance
- Initial Access
- Execution
- Persistence
- Privilege Execution
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

214 Techniques

Coloring coding represents which ATT&CK matrix a technique was derived from, such as "Drive-by compromise" is modeled after the Enterprise ATT&CK matrix, however the description has been modified to reflect an embedded environment.

	Enterprise	ICS	Mobile	Embedded Systems	
Reconnaissance	**Initial Access**	**Execution**	**Persistence**	**Privilege Escalation**	**Defense Evasion**
Active Scanning	Drive-By Compromise	Command-Line Interface	Account Manipulation	Privilege Escalation via Direct Connect System	Binary Padding
	Hardware Additions	Compiled HTML File	Bootkit	Hidden Menu	Code Signing
	Access via Removable Media	Graphical User Interface	Persistent Firmware	Reserve Software Options	Compile After Delivery
	Supply Chain Compromise	Scheduled Task	Create Account	Configuration Changes	Component Firmware
	Trusted Relationship	Service Execution	External Remote Services	Differential Software Loading	Evasive Connection Proxy
	Access via Valid Accounts	Execute via Trusted Developer Utilities	File System Permissions Weakness	Side Channel Attack	Deobfuscate Files or Information
	Exploit via Radio Interfaces	Change Operating Mode	Hidden Files and Directories	Fault Injection	Disabling Security Tools
	Install Insecure or Malicious Configuration	Execution Through API	Persistence Hooking		Execution Guardrails
	Maintenance or Debug Ports	Logical Man in the Middle	Hypervisor		Exploitation for Defense Evasion
	Authenticated Menu Bypass	Execute via Modified System Tasking	Kernel Modules and Extensions		File Deletion
	Masquerade as Legitimate Application	Improper Memory Management	Local Job Scheduling		Indicator Blocking
	Engineering Workstation Compromise	Execute via Direct Connect System	Modify Existing Service		Indicator Removal from Tools
	Internet Accessible Device	Positioning, Navigation and Timing (PNT) Geofencing	New Service		Indicator Removal on Host
	Access via Direct Connect System	Embedded System State	Path Interception		Install Root Certificate
	Downgrade to Insecure Protocols	Non-Self Originated Sensor Signal	Port Knocking - Serial Bus		Subsytem Masquerading
		Self-Originated Sensor Signal	Port Monitors - Serial Bus		Process Masquerading
		Hardware Trojan	Redundant Access Points		Bus Communication Masquerading
		Out-of-Band Transceiver Manipulation	Startup Items		Obfuscated Files or Information
			Evasive System Firmware		Port Knocking
			Time Providers		Process Hollowing
			Persistence via Valid Accounts		Process Injection
			Persistent OS Kernel or Boot Partition		Redundant Evasive Access Points
			Modify System Partition		Hidden Rootkit
			Modify Trusted Execution Environment		Scripting
			Modify NVRAM Code and Configuration		Timestomp
			Supply Chain and Third Party Library		Evade via Trusted Developer Utilities
			Embedded Software		Device Lockout
			Operational Data Files		Evade Analysis Environment
					Input Injection
					Evasive OS Kernel or Boot Partition
					Modify Underlying System
					Container Breakout
					Exploitation for Evasion
					Impersonate Master Device
					Spoof Reporting Message
					Evade via Operating Mode Changes
					Modify Checksums
					Evade Physical Detection

Sponsor: Cyber Resiliency Office for Weapon Systems (CROWS)
Dept. No.: N157
Contract No.: FA8702-24-C-0001
Project No.: 101716.25.306.4PA0

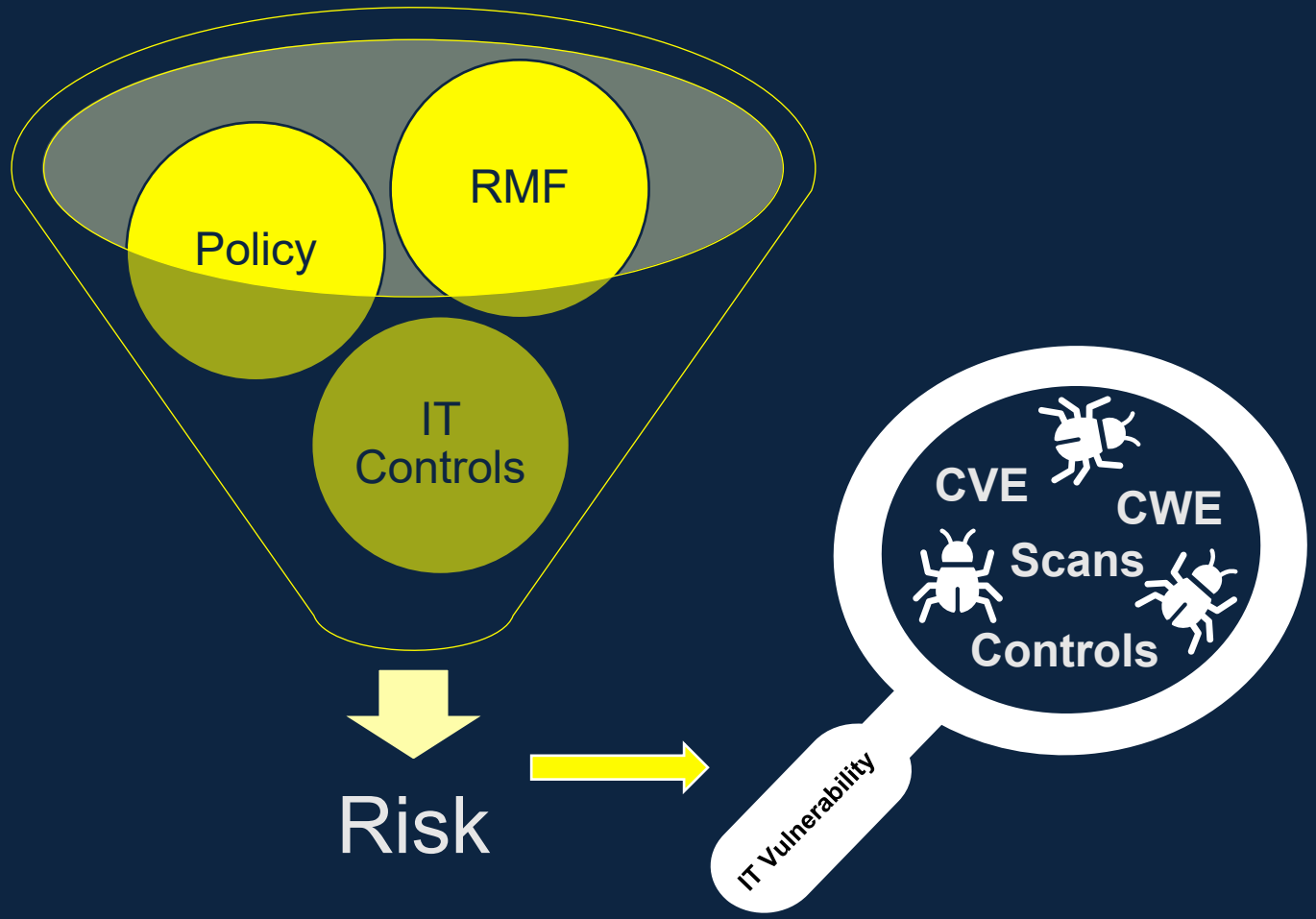
The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

DISTRIBUTION STATEMENT A Approved for public release: distribution is unlimited. Case 25-2080.

MP250526

MITRE

Challenge: Current Cybersecurity Paradigm



What we are missing…

- Serial Bus
- Real-Time Operating System
- Radio
- Program Logic Controller
- Cyber Physical

Challenge: Analyzing Cybersecurity Risk for Non-IT Systems

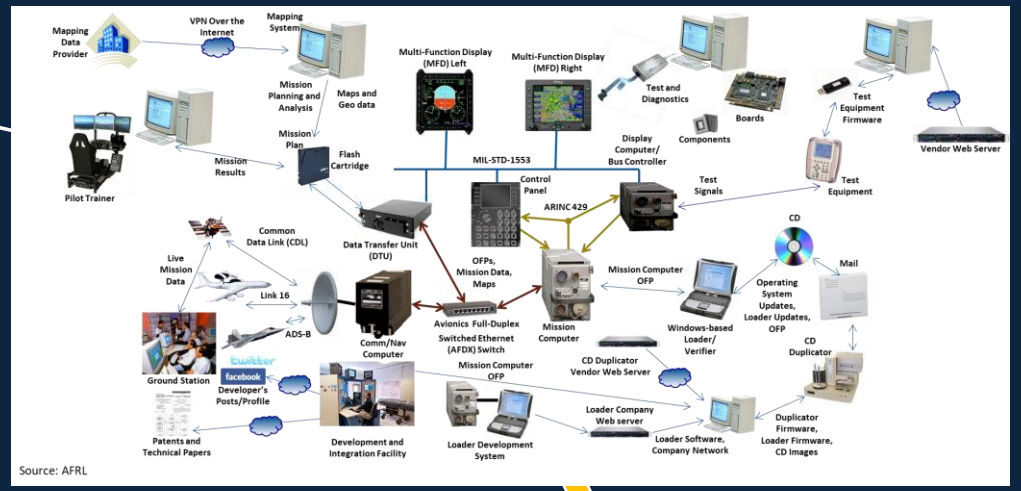
Not Standardized

IT Compliance Driven

Cybersecurity Risk Analysis

Silos of Excellence

Limited inclusion of Operational Technology (OT)



MITRE

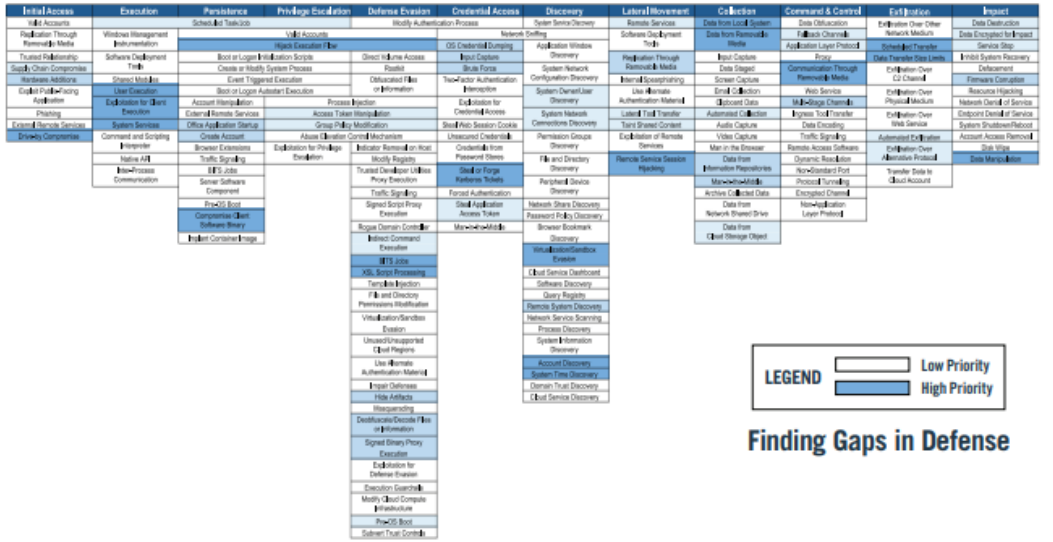
ATT&CK

ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques, developed by MITRE based on **real-world observations** of adversaries' operations.

The MITRE ATT&CK framework is increasingly being used by the community as a common way to **describe adversary behavior.**

Use ATT&CK to Build Your Defensive Platform

ATT&CK includes resources designed to help cyber defenders develop analytics that detect the techniques used by an adversary. Based on threat intelligence included in ATT&CK or provided by analysts, cyber defenders can create a comprehensive set of analytics to detect threats.



Use ATT&CK for Adversary Emulation and Red Teaming

The best defense is a well-tested defense. ATT&CK provides a common adversary behavior framework based on threat intelligence that red teams can use to emulate specific threats. This helps cyber defenders find gaps in visibility, defensive tools, and processes—and then fix them.

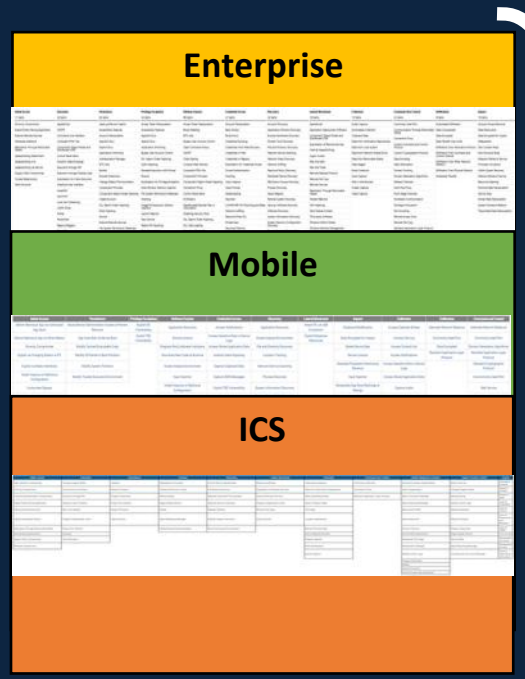
MITRE

Why ESTM Was Created

Build us ATT&CK for weapon systems*

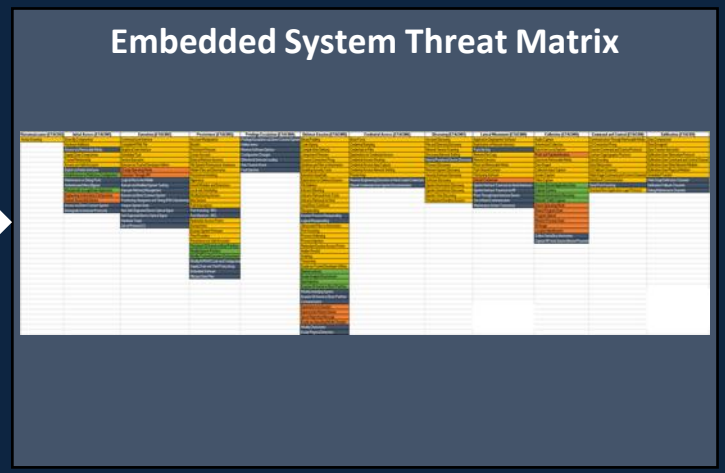
* There is no ATT&CK for weapon systems

ATT&CK gap analysis for embedded environments



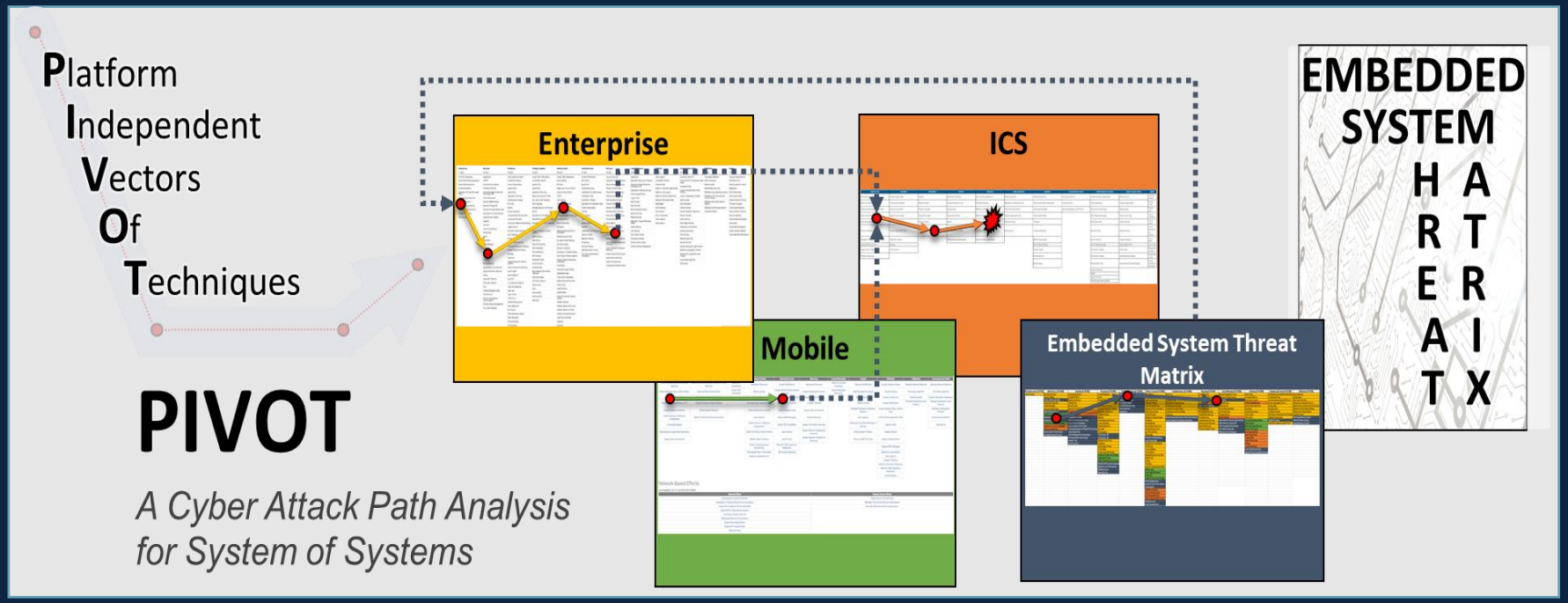
Filter for embedded

Umm...this is not a weapon system framework.



MITRE

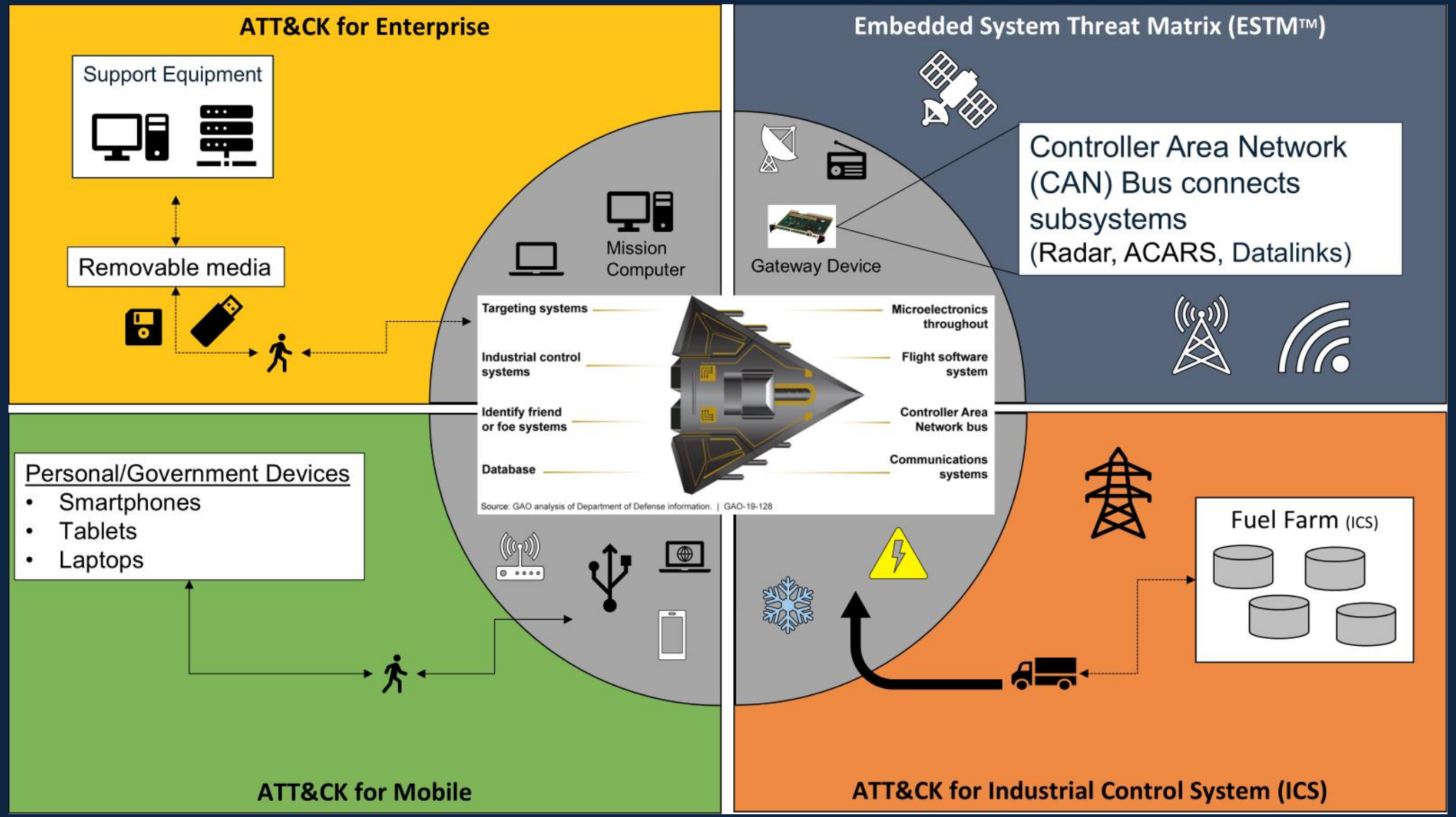
Platform Independent Vectors of Techniques (PIVOT™)



Attack path across a system-of-systems requires use of multiple threat matrices to observe how an adversary must conform their behavior to the environment they seek to effect.

MITRE

PIVOT Use Case



MITRE

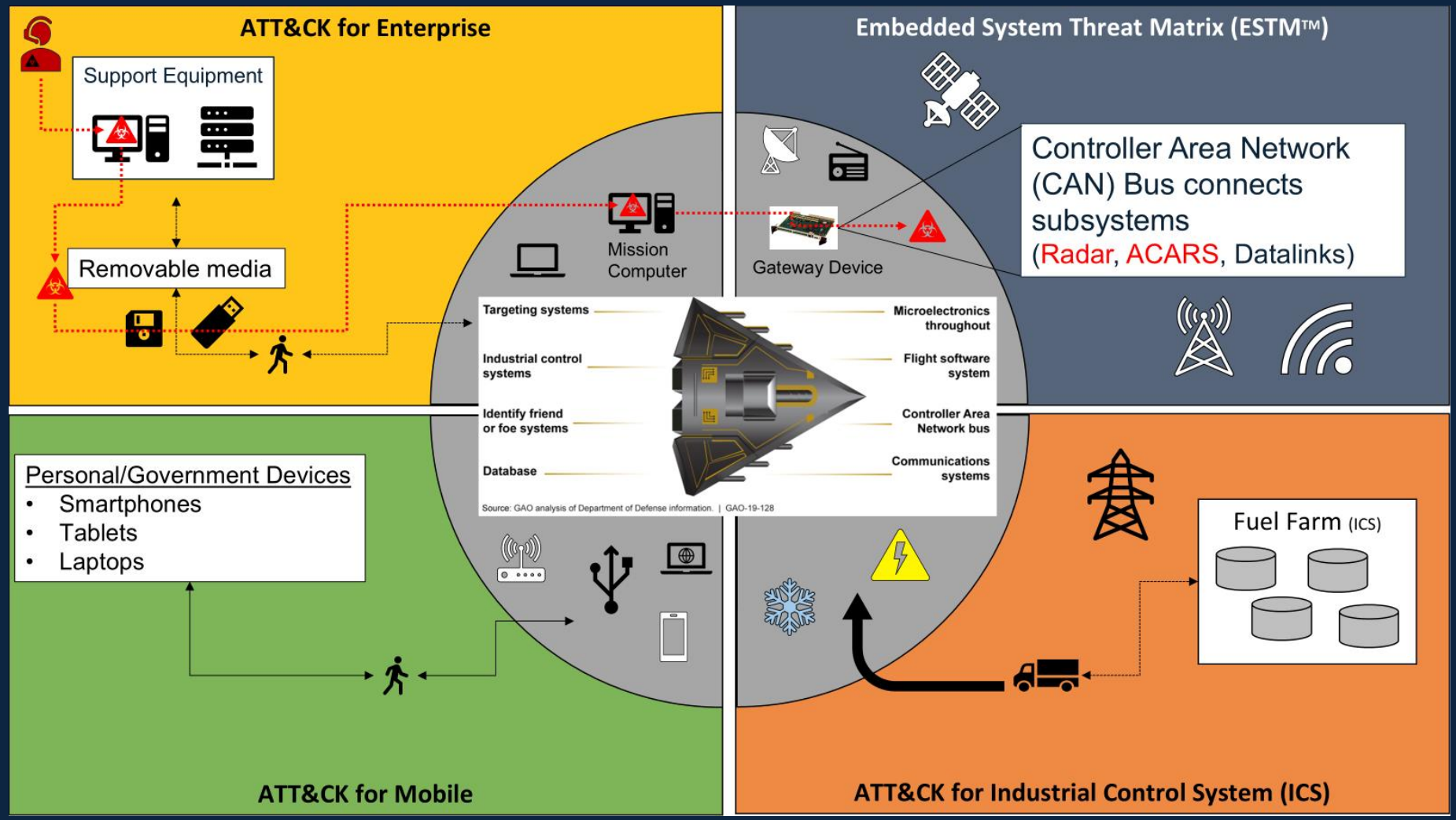
PIVOT & ESTM Notional Scenario

ATT&CK TTPs

T1195: Supply Chain Compromise

T1091: Replication Through Removable Media

T1570: Lateral Tool Transfer



ESTM TTPs

EST000140: System Interface Traversal via Serial Interface

EST000204: Impair Process via Modified System Tasking

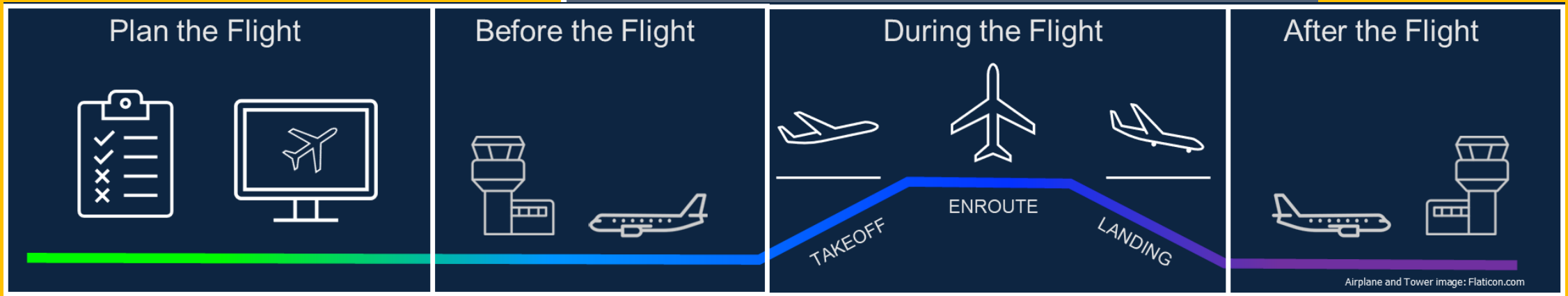
MITRE

The Fusion of Technology for Aviation

Embedded Systems



Radar and radio tower images: Wikipedia.com

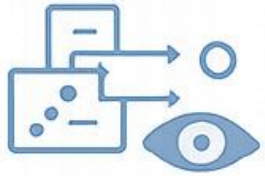


Information Technology

Critical Infrastructure

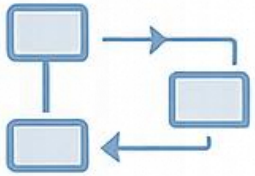
MITRE

Common Use Cases



Visualize Threats & Emulate Adversaries

Adversary behaviors against embedded & cyber physical systems



Analyze Attack Paths & Pivot Points

Initial access, trust boundaries, and system transitions

Assess Defensive Gaps

Unmonitored interfaces and implicit trust relationships

Develop Detection & Monitoring Analytics

Behavioral indicators and system telemetry

MITRE

ESTM Next Steps

Framework & Tool Integration

- Mitigations & Countermeasures
- Defense Gap Analysis

EMB3D™ D3FEND™

Operational & Real-World Use

Community & Innovation

- Collaborate & Share
- Expand Use Cases & Tooling
- Storyboard Creation

Industry & Academia Partners

- Create Secure Solutions

eCTF
EMBEDDED CAPTURE THE FLAG

MITRE

For more information email the ESTM team at: ESTM@mitre.org

Or

Visit https://estm.mitre.org/