MITRE

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

Dayton, OH

MP250155

Embedded Systems Threat Matrix™

Authors:

Mario Zuniga
Matt Janson
Adam Bairos
Jon Salisbury
George Roelke
Deihim Hashemi
Peter Malinovsky
Mike Kaun

August 2025

This page intentionally left blank

Executive Summary

Embedded systems, crucial to critical infrastructure and various technologies, face increasingly sophisticated cyber threats, demanding proactive security measures. The MITRE-developed Embedded Systems Threat Matrix (ESTM) provides a purpose-built framework to address these vulnerabilities by offering a structured approach to analyzing and understanding potential adversarial behaviors targeting these systems. Inspired by the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, the ESTM categorizes adversarial tactics and techniques specific to embedded systems, enabling organizations to analyze threats, conduct realistic assessments, and develop comprehensive defense strategies. The ESTM has proven valuable in various applications, including cyber threat modeling and attack path analysis, and its alignment with established cybersecurity frameworks ensures seamless integration with existing security practices.

Acknowledgments

The authors thank Bob Heinemann, Steve Luke, Roger Beard, Chris Sielski, Ben Janis, Kyle Skey, Cedric Carter Jr., Joe Morrissey, Stephen J. Dillon, Peter Malinovsky, Adam Hahn, Mike Kaun, Rich Kutter, Harrell Van Norman, Kevin Payne, Mike Crouse, and Chris Bottomley for their invaluable contributions to the development and shaping of the Embedded Systems Threat Matrix.

Table of Contents

List of Figures

1 Introduction

Embedded systems, integral to everything from aircraft avionics to critical infrastructure, are increasingly susceptible to sophisticated cyber threats.[1] These threats demand proactive mitigation strategies to ensure the resilience and survivability of these essential systems. This paper introduces the MITRE ESTM, a purpose-built framework designed to describe adversary behaviors against embedded systems.

The ESTM's genesis can be traced back to a recognized gap in existing cybersecurity frameworks. As shown in Figure 1, while frameworks like the MITRE ATT&CK provide valuable insights, they lack the dedicated focus needed to fully capture the vulnerabilities specific to embedded systems. This gap was highlighted in previous analyses, including the Platform Independent Vectors of Techniques (PIVOT) concept paper, which called for a dedicated framework to comprehensively model potential adversarial behaviors targeting embedded systems within a systems-of-system environment.[2]

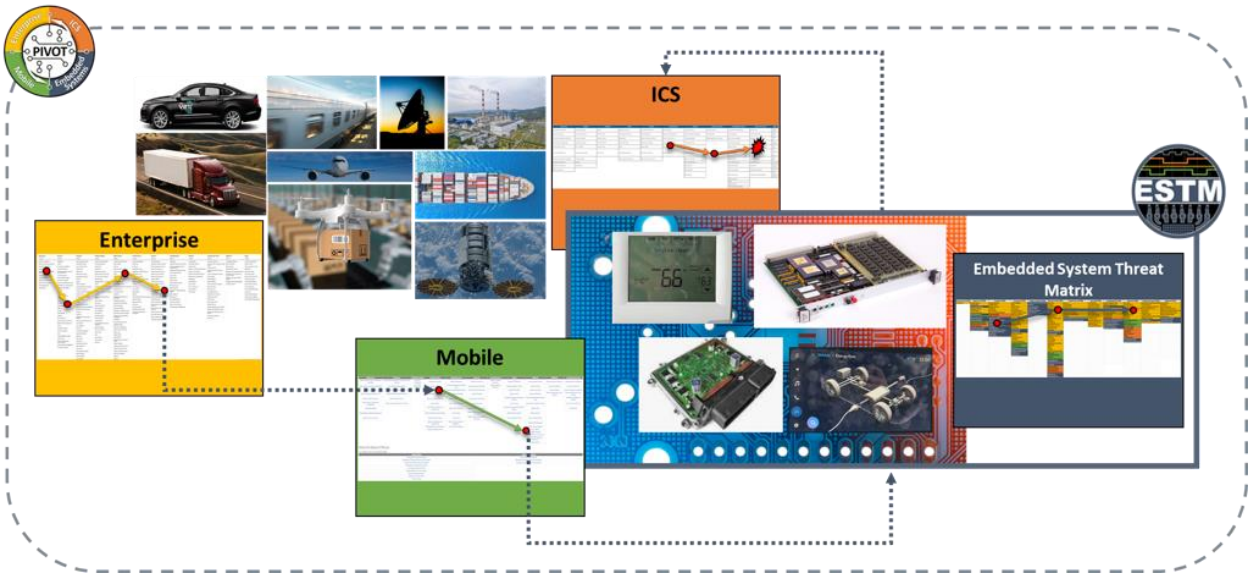


Figure 1 - Embedded Systems Threat Matrix within the PIVOT Concept

The ESTM directly addresses this need by providing a structured approach to understand and analyze threats to the diverse architectures, software, protocols, and components found within embedded systems. While conceptually aligned with ATT&CK and designed for seamless integration, the ESTM stands as a distinct and independent tool. This paper delves into the development of the ESTM, its structure, key distinctions from existing frameworks, and its diverse applications for strengthening the security posture of embedded systems.

[1] For the purposes of the ESTM, MITRE adopts the definition provided by the National Science Foundation's Center for Embedded Systems: An embedded system is an application-specific computing system found inside products such as home appliances, mobile handheld personal systems (e.g., cellphones, health monitors, assistive devices, cameras, electronic games), instrumentation, automobiles, aircraft, missiles, satellites, and nuclear power plants.

[2] MITRE Product 220278 Platform Independent Vectors of Techniques - An Approach to Systems of Systems Attack Path Analysis, May 2022, https://apps.dtic.mil/sti/trecms/pdf/AD1180518.pdf

This page intentionally left blank

2 Background

The development of ESTM originated from a critical need to enhance cybersecurity for embedded systems across various sectors. In 2020, efforts to create a framework specifically tailored for vulnerability assessments of complex systems with embedded technologies highlighted a significant gap in existing resources, especially for avionics environments. While existing frameworks provided valuable insights, they lacked the nuanced understanding required to address the unique vulnerabilities inherent in embedded systems.

ESTM has undergone significant development since its initial iteration, which focused on capturing potential adversarial behaviors and techniques within embedded environments. Through extensive collaboration with mission partners, MITRE has matured the framework into its current form, ESTM 3.0.[3] This iteration prioritizes three key areas of improvement. First, it emphasizes system-agnostic tactics and techniques, ensuring the framework's applicability across diverse domains, including public, commercial, and specialized sectors. Second, ESTM 3.0 aligns its structure with Structured Threat Information Expression 2.1, promoting interoperability and enabling machine-readable threat intelligence. Finally, the framework focuses on developing and validating attack patterns specific to embedded systems, providing defenders with actionable insights to strengthen their security posture.

[3] The ESTM 3.0 framework, https://estm.mitre.org/

This page intentionally left blank

3 Technical Approach

ESTM leverages the robust structure of MITRE ATT&CK while adapting its focus to the distinct challenges of embedded system security. This involved a rigorous, multi-step approach. We began by analyzing ATT&CK's Enterprise, Mobile, and Industrial Control Systems (ICS) matrices to identify tactics and techniques relevant to embedded environments.[4] This involved merging the matrices and meticulously evaluating each entry for its applicability to embedded systems. Techniques deemed relevant were consolidated into the initial ESTM framework. This consolidated set formed the foundation for further development.

Mirroring the structure of MITRE ATT&CK, the ESTM utilizes "Tactics" to categorize similar techniques based on the adversary's objective. This aligns with the principle that understanding the "why" behind an attack—the adversary's tactical goal—is crucial for effective defense. ESTM currently incorporates the following Tactics:[5]

1. **Reconnaissance (ETAC012):** A Cyber Embedded Tactic in which the adversary is actively or passively gathering information that can be used to support targeting a specific embedded system or component.

2. **Initial Access (ETAC001)**: A Cyber Embedded Tactic in which the adversary is trying to gain access to an embedded system or component.

3. **Execution (ETAC002)**: A Cyber Embedded Tactic in which the adversary is trying to run malicious code on an embedded system or component.
4. **Persistence (ETAC003)**: A Cyber Embedded Tactic in which the adversary is trying to maintain their foothold on an embedded system or component.

5. **Privilege Execution (ETAC004)**: A Cyber Embedded Tactic in which the adversary is trying to gain higher-level permissions on an embedded system or component.

6. **Defense Evasion (ETAC005)**: A Cyber Embedded Tactic in which the adversary is trying to avoid being detected on an embedded system or component.

7. **Credential Access (ETAC006)**: A Cyber Embedded Tactic in which the adversary is trying to steal credentials for an embedded system or component.

8. **Discovery (ETAC007)**: A Cyber Embedded Tactic in which the adversary is trying to map out a system's embedded system or component environment.

9. **Lateral Movement (ETAC008)**: A Cyber Embedded Tactic in which the adversary is trying to move through an environment via embedded systems or components.

10. **Collection (ETAC009)**: A Cyber Embedded Tactic in which the adversary is trying to gather data of interest for embedded systems or components.

[4] The ESTM 1.0 gap analysis was based on MITRE ATT&CK version 8.2, October 2021-April 2021

[5] Naming convention for Tactics: Embedded Tactic (ETAC)

11. **Command and Control (ETAC010)**: A Cyber Embedded Tactic in which the adversary is trying to command and control a compromised system via embedded systems or components.

12. **Exfiltration (ETAC011)**: A Cyber Embedded Tactic in which the adversary is trying to steal data via an embedded system or component.

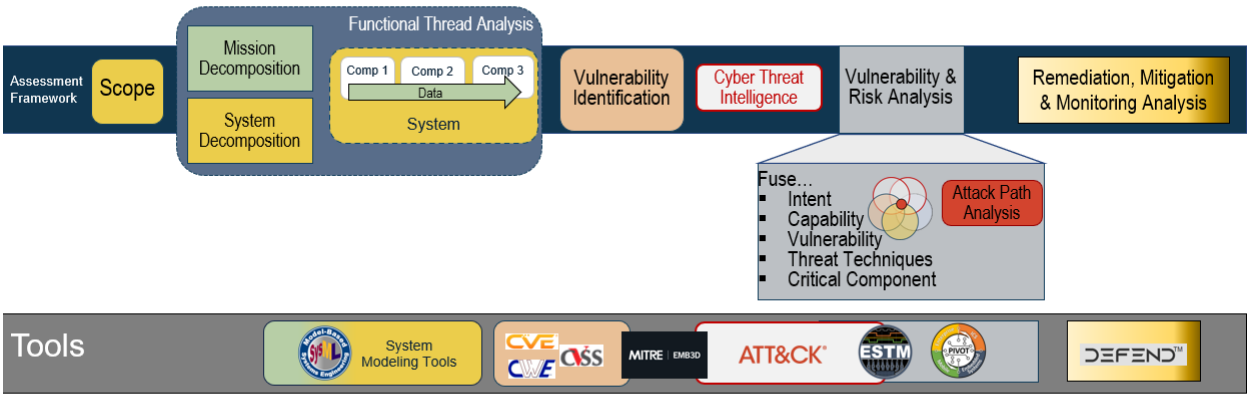
13. **Impact (ETAC013):** A Cyber Embedded Tactic in which the adversary is trying to manipulate, interrupt, or destroy your systems and data.

While drawing inspiration from the MITRE ATT&CK framework, the ESTM includes behaviors not yet widely observed against real systems, including known exploitable weaknesses, proofs-of-concept, and theoretical techniques. This forward-looking approach helps organizations anticipate and prepare for future threats. The ESTM's standardized terminology and framework break down communication barriers between researchers, vendors, and security teams, enabling a more unified approach to embedded system security. Although the ESTM doesn't currently offer specific mitigation guidance, it provides a common language and framework for cybersecurity professionals to analyze attacks, understand potential vulnerabilities, and collaborate on more effective defense strategies.

The ESTM works in conjunction with MITRE's EMB3D™ Threat Model to provide comprehensive embedded system security. EMB3D provides a knowledge base of device properties, cyber threats, and mitigations intended to help system developers, asset operators, and researchers improve the security of embedded device hardware and software.[6] It supports the goal of "secure-by-design" system development. ESTM adds value to EMB3D by providing further information on threats, specifically regarding adversarial behavior and methods for executing cyber-attacks within system-of-system environments using PIVOT.

For example, EMB3D identifies side-channel threats like power consumption analysis (TID-101) and cache timing analysis (TID-103). ESTM complements this by providing specific attack techniques, such as the "Side-Channel Attack" technique (EST000067) under the "Privilege Escalation" tactic (ETAC004). This ESTM technique details how vulnerabilities like Spectre and Meltdown, which exploit cache timing, can be leveraged by adversaries to gain elevated privileges through the cyber-attack life cycle, directly illustrating how the EMB3D side-channel threats can be exploited in practice. By combining EMB3D's threat modeling with ESTM's attack techniques, organizations gain a comprehensive understanding of embedded system vulnerabilities, enabling them to strengthen their security posture across the entire system life cycle, from design and development to deployment and operation. Figure 2 shows a generic cyber assessment process and how the various cyber analysis tools and knowledge bases fit into the process.

[6] The EMB3D™ Threat Model for Embedded Devices, https://emb3d.mitre.org



This image depicts an integrated approach to cyber risk assessment, showcasing the relationship between various cyber analysis tools and knowledge bases. While not all-inclusive, it provides a representative overview of a tailored cyber assessment framework based on MITRE's Universal Cyber Assessment Framework.

Figure 2 - Leveraging Cyber Analysis Tools for Cyber Risk Assessments

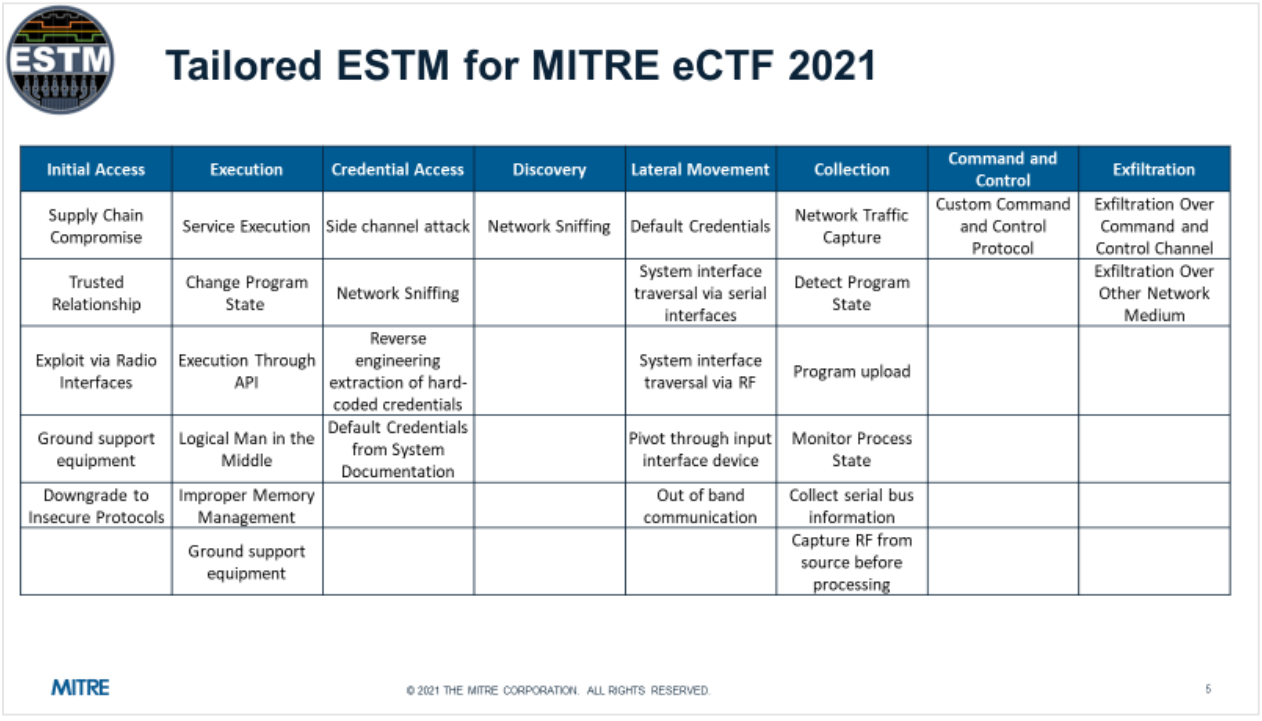
To further bridge the gap between device-level threat modeling and adversarial behavior, MITRE is actively mapping EMB3D Threat IDs to corresponding ESTM Tactics and Techniques. This is an ongoing effort that highlights the synergistic potential of the two frameworks. A comprehensive mapping will be released at a future date. As both the EMB3D framework and the ESTM continue to mature and expand, a more comprehensive and iterative analysis will be necessary to fully capture the complex interplay between device vulnerabilities and potential attack vectors. This continued mapping will provide defenders with an increasingly detailed and actionable understanding of the embedded system threat landscape, enabling more effective risk mitigation and proactive security measures.

This page intentionally left blank

4 Use Cases

The ESTM provides a versatile framework for analyzing and strengthening the security of embedded systems across numerous sectors, especially critical infrastructure. It's particularly valuable for tasks like attack path analysis and security exercises, helping secure vital systems in areas like transportation (including air, space, maritime, autonomous, and ground vehicles), energy, healthcare, industrial control, and robot systems. By offering a structured knowledge base of potential tactics and techniques targeting embedded systems, ESTM empowers organizations to proactively identify vulnerabilities, develop more effective defenses against increasingly sophisticated cyber threats, and practice their response to possible attack vectors.

Its alignment with established cyber threat frameworks, such as the commonly used cyber-attack life cycle,[7] Lockheed Martin's Cyber Kill Chain®[8], The Aerospace Corporation's Space Attack Research and Tactic Analysis (SPARTA) threat matrix[9] ensures seamless integration with existing security practices. This interoperability has been demonstrated through the ESTM's successful application in real-world exercises, including embedded capture the flag (eCTF) challenges, addressing various stages of the cyber-attack life cycle. The ESTM's practical value was showcased at a major eCTF competition in 2021, focused on unmanned aerial vehicle (UAV) security. During this event, a tailored version of the framework, as seen in Figure 3, provided participants with a common language and framework to describe their attack and defense strategies.



Initial Access	Execution	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Supply Chain Compromise	Service Execution	Side channel attack	Network Sniffing	Default Credentials	Network Traffic Capture	Custom Command and Control Protocol	Exfiltration Over Command and Control Channel
Trusted Relationship	Change Program State	Network Sniffing		System interface traversal via serial interfaces	Detect Program State		Exfiltration Over Other Network Medium
Exploit via Radio Interfaces	Execution Through API	Reverse engineering extraction of hard-coded credentials		System interface traversal via RF	Program upload		
Ground support equipment	Logical Man in the Middle	Default Credentials from System Documentation		Pivot through input interface device	Monitor Process State		
Downgrade to Insecure Protocols	Improper Memory Management			Out of band communication	Collect serial bus information		
	Ground support equipment				Capture RF from source before processing		

Figure 3 - Tailored ESTM for MITRE eCTF 2021

[7] MITRE Technical Report 130432 Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment, November 2013, https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

[8] Lockheed Martin's Cyber Kill-Chain, https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[9] The Aerospace Corporation's Space Attack Research and Tactic Analysis, https://aerospace.org/sparta

Furthermore, MITRE created a PIVOT storyboard to show the cyber-attack surface and associated adversarial behavior. Figure 3 represents an example vignette of an adversary gaining "Initial Access" through an enterprise environment onto a targeted UAV by *Exploiting via Radio Interface*. Once this foothold is established the adversary is able to "Execute" an *Improper Memory Management* attack technique to initiate "Lateral Movement" by a *Traversal via Serial Interface* on the bus to the processor. Once positioned on the processor, the adversary implements the last two steps of their attack by *Service Execution* on the processor to capture and then "Exfiltrate" data.

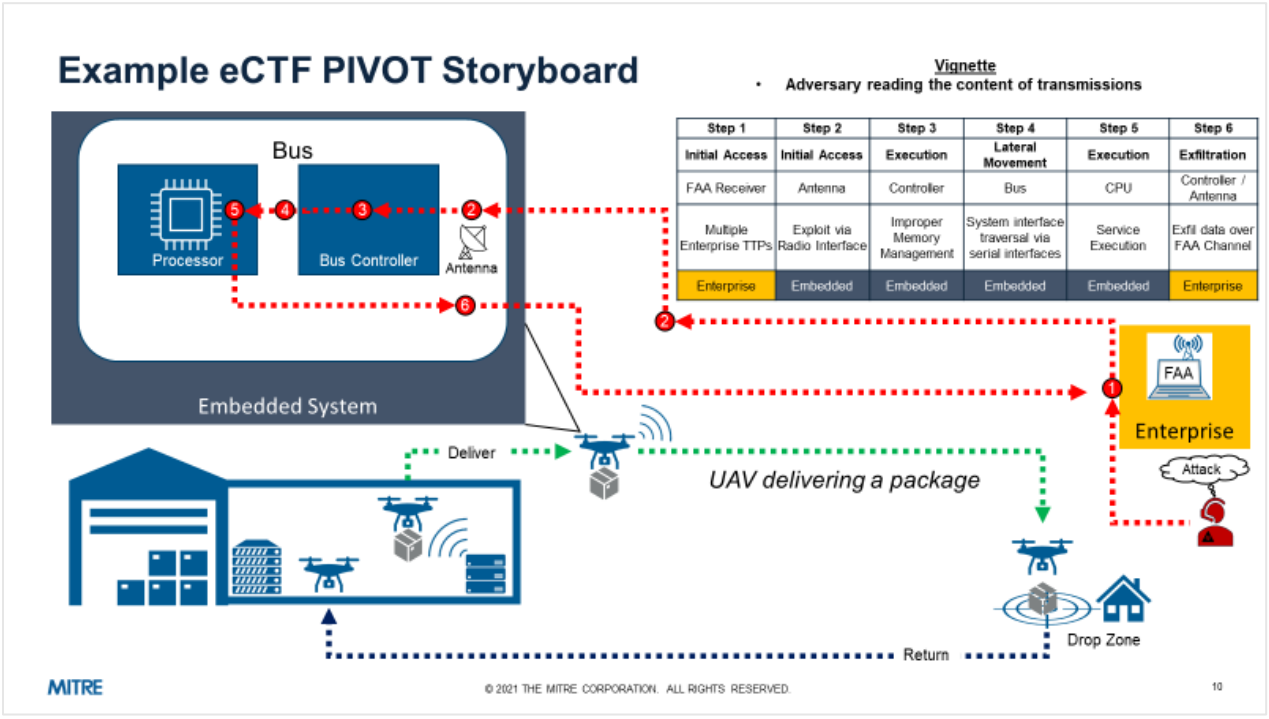


Figure 4 - MITRE eCTF 2021 PIVOT Storyboard

5 Conclusion

The ESTM addresses a critical need in the cybersecurity landscape by providing a dedicated cyber threat matrix for understanding threats to embedded systems. Derived from the robust structure of MITRE ATT&CK yet tailored to the unique characteristics of embedded environments, the ESTM offers a powerful toolset for defenders operating in this increasingly vital and vulnerable domain.

This paper has outlined the ESTM's development, driven by the recognition that existing frameworks lacked the nuanced understanding necessary to address the specific security challenges of embedded systems. The ESTM's value lies in its structured approach to modeling adversary behaviors, enabling realistic threat analyses and exercises, and facilitating comprehensive attack path analysis. Its alignment with established cyber threat frameworks ensures seamless integration with existing security practices, as demonstrated by its successful application in real-world scenarios like eCTF challenges and aviation system security.

The ESTM stands as a valuable resource for any organization seeking to proactively address the evolving threat landscape and bolster the security of their embedded systems. However, the framework's continued evolution relies on active collaboration and knowledge sharing within the cybersecurity community. MITRE encourages researchers, vendors, and practitioners to contribute their expertise and insights to further refine and expand the ESTM, ensuring its continued relevance and effectiveness in addressing the ever-evolving challenges of embedded system security. For those interested in learning more about the ESTM, contributing to its development, or exploring its applications, MITRE welcomes inquiries at estm@mitre.org.

This page intentionally left blank

6 Acronyms

ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge
ESTM	Embedded Systems Threat Matrix
E-CTF	Embedded Systems Capture-the-Flag
ICS	Industrial Control Systems
PIVOT	Platform Independent Vectors of Techniques
SPARTA	Space Attack Research and Tactic Analysis
UAV	Unmanned Aerial Vehicle