# Securing Cyber-Physical Systems via Advanced Cyber Threat Intelligence Methods

Efrén López-Morales
Texas A&M University-Corpus Christi
Corpus Christi, Texas, USA
elopezmorales@islander.tamucc.edu

## Abstract

Many services that make our modern society work, such as communications and transportation, are only possible thanks to Cyber-Physical Systems (CPS). This makes CPS the target of cyberattacks that aim to disrupt our society. One tool that we can leverage to protect CPS is Cyber Threat Intelligence (CTI). CTI is threat information that helps us understand a threat actor's techniques. However, current CTI on CPS is limited as current methods cannot collect and analyze data on the latest cyberattacks against CPS. In this dissertation research description, we address this problem by developing three new methods that advance the state-of-the-art CTI of three different CPS: Industrial Control Systems (ICS), Satellites, and Connected Autonomous Vehicles (CAV). The first research project involves the development of a novel threat taxonomy for programmable logic controllers (PLCs), which are a key part of ICS. The second project is the development of a satellite honeypot to collect data on adversaries' techniques. The third and final project involves the development of a CAV sandbox that allows us to test cyberattacks on CAVs to collect raw threat intelligence.

Our preliminary results include a novel ICS threat matrix and a high-interaction satellite honeypot in the literature, which pushes the state of the art of CTI for CPS forward.

## CCS Concepts

• **Computer systems organization** → **Embedded software**; **Embedded and cyber-physical systems**.

## Keywords

Cyber-Physical Systems, Industrial Control Systems, Satellites, Connected Vehicles, Threat Intelligence, Cybersecurity

**ACM Reference Format:**
Efrén López-Morales. 2024. Securing Cyber-Physical Systems via Advanced Cyber Threat Intelligence Methods. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3658644.3690865


*CCS '24, October 14–18, 2024, Salt Lake City, UT, USA*

ACM ISBN 979-8-4007-0636-3/24/10
https://doi.org/10.1145/3658644.3690865

## 1 Introduction

Cyber-Physical Systems (CPS) underpin various critical infrastructures vital for society's well-being, including transportation, communications, and energy. CPS are systems that include physical and computational components to offer advanced levels of automation and connectivity [11]. CPS include Industrial Control Systems (ICS), Satellites, and Connected and Automated Vehicles (CAVs).

However, along with CPS' capabilities come cybersecurity risks, specifically, the risk of cyber threats and attacks that can compromise these systems' safety, reliability, and integrity. A successful cyberattack on a CPS endangers real-world assets such as nuclear facilities which might result in millions of dollars' worth of damage or, even worse, the loss of human life.

One key component of an effective cybersecurity strategy for CPS is cyber threat intelligence (CTI). CTI involves collecting, analyzing, and disseminating information about cyber threats and adversaries to inform defensive measures and decision-making [6]. By leveraging CTI, we can gain insights into adversary tactics specific to various computer systems, including CPS, enabling them to enhance their security by developing countermeasures.

However, current CTI for CPS methods are limited [4] and cannot provide the insights required to protect CPS. For example, although satellite security research is thriving [7, 10, 12], no satellite honeypot allows us to gather data on techniques targeting satellites.

To solve this problem, we have developed three new methods that advance the state of the art of CTI for CPS. First, we introduce a novel ICS threat taxonomy to categorize the latest techniques targeting ICS. Second, we develop the first satellite honeypot which allows to collect real-world data on adversaries' techniques targeting satellites. Third, we propose the first CAV cyberattack sandbox to simulate cyberattacks on multiple scenarios involving CAVs and collect data to develop countermeasures.

We do not have the final results as this dissertation is still in progress. Instead, we present preliminary results of the first and second methods. We reviewed the literature on PLC security, and based on this; we developed a novel ICS threat taxonomy called the ICS$^2$ Matrix, the most up-to-date ICS threat taxonomy [8]. We developed a high-interaction honeypot for the second method, the first satellite honeypot capable of realistically simulating an entire satellite mission. Finally, our third method is currently in the early stages of development.

## 2 Background

We now introduce relevant background topics to this work.

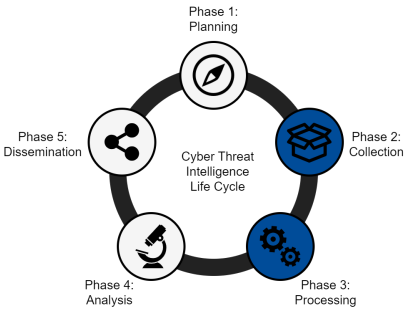


**Figure 1: Cyber Threat Intelligence Lifecycle [6]. Our work focuses on Phases 2 and 3 (blue).**

## 2.1 Cyber-Physical Systems

Cyber-Physical Systems (CPS) include physical and computational components that integrate physical and computing processes. CPS rely on sensors, e.g., temperature sensors and actuators that enable them to sense the physical world and control physical equipment, e.g., a water pump. CPS are very diverse, however, in this work we focus on ICS, satellites and CAVs discussed below.

**Industrial Control Systems.** ICS manage and controls critical utilities such as the power grid, and water treatment plants. ICS comprises multiple components, including sensors, actuators, and Programmable Logic Controllers (PLCs). PLCs control industrial processes such as the ones used in water treatment plants by running special programs known as control logic. Control logic reads inputs from sensors and outputs instructions to actuators based on the control logic and input data [3].

**Space Systems.** Satellites are complex CPS designed to withstand outer space conditions and tasked with specific missions. These missions include Earth's remote sensing and GPS location, among others. Satellite missions include two segments. The *ground segment* from which satellite operators control the satellite, and the *space segment* consists of the satellite itself [14]. Satellites' architecture includes software known as *flight software* (FS). Satellite FS manages the different satellite subsystems, e.g., power, and are typically written in low-level languages such as C. FS are important because they are vulnerable to common software attacks.

**Connected and Automated Vehicles (CAVs).** CAVs communicate with nearby vehicles and infrastructure to provide features such as vehicle automation to drive decision-making. CAVs use artificial intelligence or computer systems to drive themselves without human operators and are connected via Wi-Fi or another network to send and receive data from other CAVs, transportation infrastructure such as green lights and even pedestrians.

## 2.2 Cyber Threat Intelligence

CTI is the process of collecting, analyzing, and disseminating information about cyber threats and adversaries to inform defensive measures and decision-making [6]. CTI is produced during the CTI lifecycle, which includes five phases. 1) Requirement planning, 2) data collection, 3) information processing, 4) intelligence analysis, and 5) dissemination. The CTI lifycicle is depicted in Fig. 1.

Each of these stages leverages different methods to accomplish its objectives. For example, *data collection* involves identifying threat intelligence sources to start raw data collection. In this work we focus on *collection and processing phases*.

## 3 Problem Statement

In this dissertation, we develop new methods that advance the state of the art in CTI processing and collection phases for CPS as depicted in Fig. 1. Current methods for processing and collecting CTI for CPS are limited [4]. For example, there are honeypot implementations for other CPS such as ICS [9, 13]; however, there is no satellite honeypot that allows us to collect raw CTI data. Current processing and collecting methods are focused on commodity computers. However, these methods are not directly transferable to CPS as they have different architectures and purposes.

CTI is crucial for developing countermeasures and security strategies. Failing to develop effective CTI processing and collecting methods for CPS would result in poor CTI that would limit our capacity to develop effective countermeasures and security strategies.

To solve this research gap, this dissertation proposes the following three research projects:

(1) Developing a novel ICS threat taxonomy that categorizes the latet CTI data. This relates to Phase 3: Processing of the CTI lifestyle (Fig. 1).
(2) Developing a satellite honeypot that collects raw CTI data. This relates to Phase 2: Collection of the CTI lifecycle (Fig. 1).
(3) Developing the first CAV sanbox that allows us to simulate cyberattacks on CAVs to collect CTI of the simulated attacks. This relates to Phase 2: Collection of the CTI lifecycle (Fig. 1).

## 4 Methodology and Preliminary Results

We now describe the methodology and preliminary results for two of the three projects described above, the ICS threat taxonomy and the satellite honeypot. Due to space constraints and because it is early in development we do not describe the CAV sandbox.

## 4.1 Threat Taxonomy for ICS

**Methodology.** The methodology consists of two steps: 1) performing a systematization of knowledge and 2) developing a novel ICS threat taxonomy based on the results of step 1.

1) *Systematization of Knowledge.* To perform the knowledge systematization, we first performed a literature review. We review scientific literature to collect PLC attack and defense methods. As a result of the literature review, we collected 133 papers, the earliest from 2007 and the latest from 2023. Then we read and analyzed each paper to extract important security-relevant information such as attack vectors, PLC models and manufacturers, and PLC target components. We matched each attack and defense method to their corresponding technique, and mitigation category. We evaluate the data to produce the ICS threat taxonomy discussed next.

2) *Threat Taxonomy Development.* To better classify attack and defense methods for PLCs and ICS, we extended the MITRE ATT&CK for the ICS Matrix and the Hybrid ATT&CK Matrix [2] to create the ICS$^2$ Matrix. The taxonomy includes adversary tactics that describe "what" is the adversary's goal and attack techniques that describe

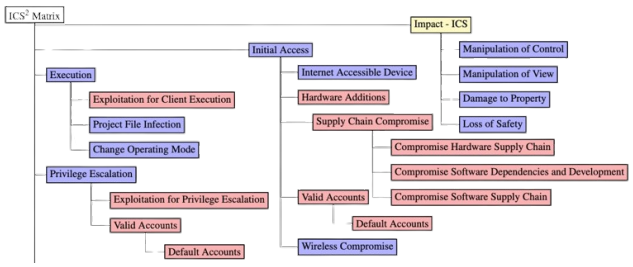


**Figure 2: Snippet of the ICS² Matrix which includes Tactics (yellow), techniques (blue), and procedures (red).**

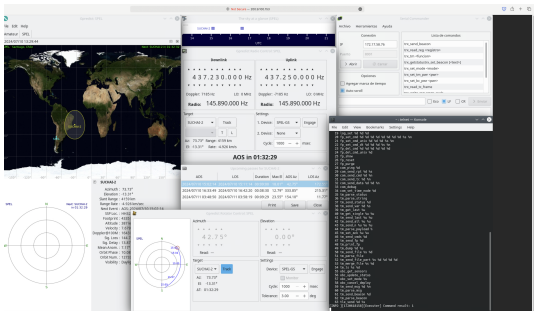

**Figure 3: Satellite honeypot ground software screenshot.**

"how" the adversary can complete their goal. Additionally, it includes mitigations that prevent a technique from being successfully executed. The ICS² Matrix incorporates the scientific knowledge by adding 6 new attack techniques and 5 new mitigation categories based on the literature reviewed.

**Results.** The ICS² Matrix, depicted in Fig. 2, is the most up-to-date ICS matrix in the literature. It incorporates tactics and techniques from 17 years of PLC security research. Our threat taxonomy is available on GitHub [8].

## 4.2 Satellite Honeypot

**Methodology.** The methodology for developing our satellite honeypot consists of two steps: 1) developing a space segment simulation to simulate a real satellite, and 2) developing a ground segment simulation to simulate a real satellite mission environment.

1) *Ground Segment Simulations.* The ground segment simulations (depicted in Fig. 3) mimic the software that satellite operators use to manage the satellite from Earth's surface. We leverage existing ground segment software such as Gpredict. Gpredict is a popular freeware GSCS that performs real-time satellite tracking and orbit prediction [5]. Gpredict can also interface with and control the radio system and antenna rotor during the satellite pass.

2) *Space Segment Simulations.* The space segment simulations mimic the spacecraft. We leverage an existing satellite flight software from a real satellite mission to achieve this. The satellite flight software manages all the satellite computer functions required for the mission operation, such as interacting with hardware peripherals, processing telecommands, and sending telemetry.

**Results.** We were able to develop a realistic satellite honeypot. To test our honeypot, we leverage the SPACE-SHIELD matrix [1], which provides a collection of adversary tactics and techniques for satellite systems. We compared the techniques the satellite honeypot supports against those documented in the SPACE-SHIELD matrix, and we found that our honeypot supports 86.8% of the feasible techniques. This means that our satellite honeypot provides advanced high-interaction opportunities to adversaries. Consequently, our honeypot can collect real-world CTI for satellites data.

## 5 Conclusion

In this dissertation research description, we explained three research projects designed to advance the state of the art of CTI for CPS. The first project resulted in a novel ICS threat taxonomy to appear at the 33rd USENIX Security Symposium [8]. The second project, a satellite honeypot, is currently under review, and our third project is in early development.

In conclusion, our research advances the state of the art of cyber threat intelligence for cyber-physical systems so that the security of critical infrastructures on which our society relies remains strong even as malicious actors continue to develop new, unknown techniques aimed at disrupting our well-being.

## Acknowledgments

I would like to thank my research advisor, Dr. Carlos Rubio-Medrano, for his support, guidance, and encouragement throughout this research. This work was partially supported by the Scholar Achievement in Graduate Education (SAGE) Fellowship from Texas A&M University-Corpus Christi.

## References

[1] European Space Agency. 2023. ESA SPACE-SHIELD. https://spaceshield.esa.int/#
[2] Otis Alexander. 2020. In Pursuit of a Gestalt Visualization: Merging MITRE ATT&CK® for Enterprise and ICS to Communicate. (Sept. 2020).
[3] William Bolton. 2015. *Programmable logic controllers.* Newnes.
[4] Sergio Caltagirone. 2018. Industrial Control Threat Intelligence. (2018).
[5] Alexandru Csete. 2023. Gpredict: Free, Real-Time Satellite Tracking and Orbit Prediction Software. https://oz9aec.dk/gpredict/
[6] Martin Dempsey. 2013. JP 2-0, Joint Intelligence. (Oct 2013).
[7] Tamara Gutierrez, Alexandre Bergel, Carlos E. Gonzalez, Camilo J. Rojas, and Marcos A. Diaz. 2021. Systematic Fuzz Testing Techniques on a Nanosatellite Flight Software for Agile Mission Development. *IEEE Access* (2021).
[8] Efrén López-Morales, Ulysse Planta, Carlos Rubio-Medrano, Ali Abbasi, and Alvaro A. Cardenas. 2024. SoK: Security of Programmable Logic Controllers. In *33rd USENIX Security Symposium (USENIX Security 24).* Philadelphia, PA.
[9] Efrén López-Morales, Carlos Rubio-Medrano, Adam Doupé, Yan Shoshitaishvili, Ruoyu Wang, Tiffany Bao, and Gail-Joon Ahn. 2020. HoneyPLC: A Next-Generation Honeypot for Industrial Control Systems. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, USA) *(CCS '20).* New York, NY, USA, 279–291.
[10] Gabriele Marra, Ulysse Planta, Philipp Wüstenberg, and Ali Abbasi. 2024. On the Feasibility of CubeSats Application Sandboxing for Space Missions. In *2nd Workshop on the Security of Space and Satellite Systems (SpaceSec).*
[11] National Institute of Standards and Technology. 2020. CSRC Topic: cyber-physical systems | CSRC. https://csrc.nist.gov/topics/applications/cyber-physical-systems
[12] Ulysse Planta, Julian Rederlechner, Gabriele Marra, and Ali Abbasi. 2024. Let Me Do It For You: On the Feasibility of Inter-Satellite Friendly Jamming. In *2024 Security for Space Systems (3S).* 1–6.
[13] Luis Salazar, Efren López-Morales, Juan Lozano, Carlos Rubio-Medrano, and Alvaro A Cardenas. 2024. ICSNet: A Hybrid-Interaction Honeynet for Industrial Control Systems. In *Proceedings of the 6th Workshop on CPS&IoT Security and Privacy* (Salt Lake City, UT, USA) *(CPSIoTSec '24).*
[14] Johannes Willbold, Moritz Schloegel, Manuel Vögele, Maximilian Gerhardt, Thorsten Holz, and Ali Abbasi. 2023. Space Odyssey: An Experimental Software Security Analysis of Satellites. In *2023 IEEE Symposium on Security and Privacy (SP).*