CPSTRIDE: A Threat Modeling Framework for Cyber-Physical Systems

Abstract. Cyber-physical systems are vulnerable to attacks on physical and cyber-physical processes and devices alike; comprehensive defense requires models that account for them. We present the CPSTRIDE framework, an extension of the classic STRIDE model that incorporates a novel Cyber-Physical Flow Diagram as well as Security Property and Threat definitions. We demonstrate CPSTRIDE's utility by modeling threats beyond STRIDE's capabilities in an additive manufacturing context.

Keywords: Cyber-Physical Systems · Additive Manufacturing · Threat Modeling · STRIDE · Critical Infrastructure · LLM-assisted

1 Introduction

Cyber-physical systems (CPS) use sensors, actuators, and computation to monitor, control, and interact with physical processes. CPS are exemplified by embedded devices such as medical implants, home appliances, mobile delivery robots, self-driving cars, and environmental control systems, as well as large infrastructures such as electrical grids, refineries, and traffic control systems. Consequently, CPS are the foundation of automation and efficiency control in critical sectors such as transportation, health care, manufacturing, and energy networks.

CPS are also integral to distributed, adaptive, and data-driven decision-making, operations, and control in Industry 4.0 [13]. Of particular importance are Additive Manufacturing (AM) technologies, capable of fabricating physical objects from digital models [3]. AM systems are quintessential examples of CPS; highly connected and automated, they blur the line between digital and physical to produce objects impossible to create via legacy manufacturing methods.

Automation and connectivity give AM and CPS many advantages over legacy systems, but expose new attack paths that compromise safety-critical systems. Small CPS face security challenges related to cyber-physical interactions, processes, and operations, and large-scale CPS pose additional security concerns due to complexity. In light of potentially catastrophic consequences for compromising equipment, services, and human safety, designing these systems for security, adaptability, and resilience is imperative [5].

Traditional cyber-threat modeling frameworks (e.g., STRIDE, Cyber Kill Chain, MITRE ATT&CK) are used widely in the design and analysis of information and communications technologies (ICT) such as computers, software applications, and the Internet. As designed, however, these solutions lack the physical dimensionality and expressiveness required to fully model security for CPS [10]. Our research fills this gap with CPSTRIDE, a purpose-built framework for CPS threat modeling that extends the STRIDE framework. This work comprises primary research contributions:

1. We present CPSTRIDE, a threat modeling framework that extends STRIDE with updated security properties and threats for CPS.
2. We describe the Cyber-Physical Flow Diagram (CPFD) that augments the Data Flow Diagram paradigm to capture cyber-physical elements and threats and distinguish between cyber-physical processes and enablers.
3. We demonstrate CPSTRIDE's utility and advantages over the conventional STRIDE approach via side-by-side modeling and threat identification on an additive manufacturing system.

The remainder of the paper is organized as follows: Section 2 covers background information and previous work related to CPS and AM threats and threat modeling. Section 3 details the CPSTRIDE threat modeling framework and CPFD. Section 4 performs side-by-side CPSTRIDE and STRIDE threat modeling of an additive manufacturing system. Section 5 compares and discusses the results. Section 6 suggests future directions and offers concluding remarks.

2 Background / Previous Work

2.1 Cyber-Physical System Threat Modeling

A substantial body of research is directed at re-purposing existing ICT threat modeling frameworks for use in CPS; one popular choice is Microsoft's STRIDE framework [14]. The model's iterative four-step work cycle entails creating a Data Flow Diagram (DFD) for the system being modeled, identifying threats to DFD elements, investigating vulnerabilities for threats, and planning mitigations for vulnerabilities. DFDs use a set of five symbols that represent different types of software-relevant objects [8]. To our knowledge, there is currently no widely accepted standard for representing physical components with STRIDE.

Yampolskiy et al. [18] extend STRIDE for application to uncrewed aerial systems (UAS), one type of CPS. They note STRIDE's insufficiency for differentiating CPS-relevant interactions, e.g., cyber vs. physical communications, and formulate an extended DFD or "xDFD" that enables modeling of "physical components, communication media, optional data flows, and physical signal" using four additional DFD elements. They address several threat modeling challenges in CPS, but do not expand STRIDE security property and threat definitions.

Khan et al. [10] apply STRIDE to analysis of a synchronous island microgrid electrical system, demonstrating the method's expertise-informed brainstorming to identify cyber-attacks. They discuss the DFD's shortcomings for representing physical and cyber-physical elements and processes in electric power systems, but opt to exclude physical components not susceptible to cyber attacks.

2.2 Additive Manufacturing Threat Modeling

AM systems produce physical objects directly from physical feedstock using digital design models, and are quintessential examples of CPS. Though implementation details between systems vary, all AM follows the characteristic process chain illustrated by the green entities and flows in Figure 1.

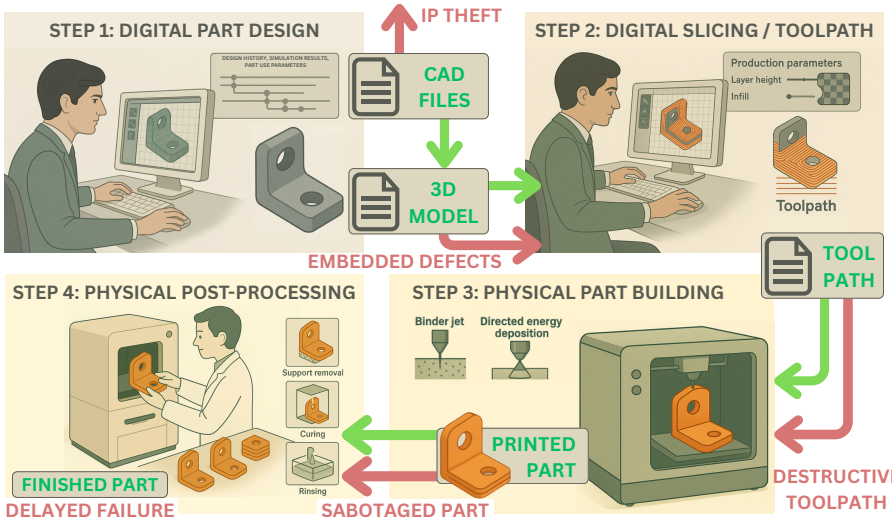


Fig. 1. The AM process chain, with benign and malicious cyber-physical flows

Using computer aided design (CAD) software, AM parts are digitally modeled and optimized through iterative simulation and analysis; the resulting CAD files include the part's 3-D model, design history, and simulated performance information (if applicable). The 3-D model is then *sliced* into layers and a *toolpath* is generated that contains a set of machine instructions for physically building each part layer. This toolpath is then given to an AM machine, which executes each line of instructions to mechanically deposit and/or join feedstock one layer or small amount at a time. Once the toolpath file has been executed completely, the physical part may finally undergo post-processing, quality control testing, warehousing, shipping, and other product life cycle phases.

The AM process chain enables digital designs to be rapidly transformed into physical objects, with the unintended side effect of also allowing cyber-attacks to be rapidly translated into physical harms. AM systems are susceptible to regular cyber-security flaws as well as to unique attack vectors [4,6,7,12,19], some of which are illustrated in Figure 1. Sturm et al. identify four main opportunities for cyber-attacks to cross into the physical world: the CAD file, 3D model, toolpath file, and the physical machine. However, all AM machinery may permit the physical manifestation of a large number of cyber-attack vectors [16].

CAD files are the most information-dense digital artifacts produced by the AM process chain, containing a part's geometric data, design history, simulated performance data, use parameters, and more, making them attractive targets for intellectual property (IP) theft and ransomware. Sabotage at this early stage can propagate data integrity and availability failures through the entire process chain [16]. 3-D model tampering can produce physical objects with hidden defects that are difficult or impossible to detect, causing unpredictable and dangerous failure

during use, as found by Belikovetsky [4]. Toolpath files are vectors for sabotaging manufactured objects, allowing theft of IP in the form of operational and manufacturing parameters, and can be modified to result in incorrect machine movement, dimension scaling, heating, feedrates, and other actions resulting in production defects and/or catastrophic equipment damage [19].

Supply chain attacks, as Yampolskiy et al. report, are difficult to defend against due to the sprawling ecosystem of third-party providers in AM systems [19]. Malware embedded in AM software, hardware, and firmware components could grant adversaries access to IP and even real-time operational control. Other attacks targeting mechanical AM system components actuators, and feedstocks can result in material composition, size, or form factor inconsistency. Gupta et al. examine supply chain vulnerabilities where material composition, purity, and microstructure might be attacked [7]. Side channels for AM system attack include acoustic, magnetic, and thermal emanations that allow the recreation or replication of AM parts without direct access to files. This type of technical data theft can be accomplished via smartphones and inexpensive surveillance equipment [1,2,9]. In addition, 3-D model files can carry hidden malicious payloads via steganographic embedding [17].

The unique nature of the digital-model-to-physical-object AM process chain requires a comprehensive cyber-physical threat framework that is rich enough to capture system and process detail, and abstract enough to describe diverse types of CPS. Next, we describe our approach to creating such a framework.

3 CPSTRIDE Framework Specification

We choose the mature and widely-used STRIDE model as a foundation due to its balance between specificity and generality for modeling cyber threats. While too data-centric and narrow for full description of CPS, we expand its coverage by examining its structure from first principles, starting with its four-step workflow:

1. Create a DFD model of the system.
2. Identify STRIDE threats, either per-element or per-interaction.
3. Investigate vulnerabilities to identified threats.
4. Plan mitigations for identified vulnerabilities.

Our changes to the STRIDE framework involve only the first two steps of the process; Steps 3 and 4 are not considered in our CPSTRIDE framework specification here, nor are they applied during side-by-side threat modeling of the AM system with both frameworks in Section 4. We begin with Step 1 by defining an expanded Cyber-Physical Flow Diagram (CPFD). For Step 2, we specify the CPS Security Properties and Threats required for threat identification.

3.1 CPFD: Cyber-Physical Flow Diagram

Drawing from Khan and Yampolskiy [10,18], and considering Shostack's [15] guidance to keep models "...aggressively simple to prioritize easy learning and use over expressiveness," we borrow five visual notation rules from DFDs:

1. All lines are solid, except for trust boundaries, which are dashed or dotted.[1]
2. CPFDS can use color for additional information, but must not require it.
3. All elements should have a label.
4. Context diagram(s) for complex systems are optional.
5. Must, must not, should, should not are used per IETF norms.

Each existing DFD element has a name, a definition, an abbreviation, and a graphical symbol. Our process for developing the CPFD is to consider whether the *core meaning* of each existing DFD element definition can be expanded to include important physical and cyber-physical analogs in a CPS context. If so, we rename, redefine, and/or re-abbreviate the existing DFD element to include this context, and we retain its graphical symbol. Otherwise, we create a new element in the CPFD and strive for aggressive simplicity, à la Shostack [15]. Our resulting CPFD specification is found in Figure 2.

For example, the DFD *Interactor (I)* element (sometimes referred to as External Entity – EE – as in [10]) represents a person, code or website that interacts with the software system but is outside its control. The core meaning, "beyond system scope," can be expanded to include CPS analogs such as physical raw material sources, gas or electric mains, cyber-physical supply chain providers, autonomous service robots, etc. We redefine a CPFD Interactor as "an entity that exchanges data, energy, or material with the CPS but remains outside its design scope and/or control boundary," specify its cyber, physical, and cyber-physical abbreviations, and keep the graphical symbol (see Figure 2). Similarly we redefine the DFD *Trust Boundary* as "a virtual and/or physical zone of privileged access" and give it CPS abbreviation versions.

The DFD *Data Store (DS)* element represents data at rest (e.g., files, databases, registry keys) in software systems. This can be expanded to include CPS analogs at rest such as physical and cyber-physical materials, objects, and keys at rest. We wish to differentiate between the entity being stored and the storage medium as well as represent hierarchical or nested cyber-physical stores (e.g. digital files on a physical hard drive). Thus, we simplify the CPFD element name to *Store* and define it as "data, energy, or material at rest, distinct from its storage medium or container, with nesting allowed." Abbreviations and graphical symbol changes can be found in Figure 2. We add a new element to the CPFD for physical and cyber-physical storage media and containers: *Device (D)*.

Similarly, the *Data Flow (DF)* element represents data in motion (e.g., communication patterns and function calls); this can be expanded to include CPS analogs such as material flows, but we agree with Yampolskiy et al. [18] that CPS flow-enabling paths and media such as gas pipes, transmission lines, and radio frequency (RF) spectrum deserve first-class representation. We simplify the CPFD element name to *Flow*, define it as "data, energy, or material in motion, distinct from its enabling path, channel or medium," modify its abbreviations and keep the graphical symbol, and add a new CPFD element to represent Flow enablers: *Link*.

[1] We extend the use of dashed lines for the two new CPFD elements: Links and Devices; see Figure 2.

Cyber-physical Flow Diagram (CPFD)

Cyber indicates information, data, or signal; *physical* indicates material, energy, or force; *cyber-physical* indicates the integration or combination of the two. Each CPFD element is categorized as either cyber, physical, or cyber-physical depending on whether the element can reasonably be considered vulnerable to cyber and/or physical threats.

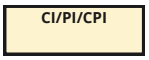
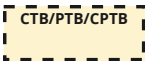
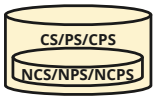
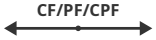
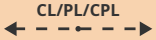
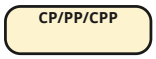
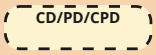
Element name, abbreviation, and description	**Graphical Symbol**	**Examples** **C:** *Cyber* **P:** *Physical* **CP:** *Cyber-physical*
Interactor (I) An entity that exchanges data, energy, or material with the CPS but remains outside its design scope and/or control boundary.		**CI**: External APIs, the Internet and other networks. **PI**: Raw material sources; water, gas or electric mains. **CPI**: Humans (e.g., employees, contractors), external orgs (e.g., supply chain providers, partners, customers), technological entities (e.g., autonomous delivery and service robots).
Trust Boundary (TB) A virtual and/or physical zone of privileged access.		**CTB**: Password-protected systems, encrypted files, or trusted computing environments. **PTB**: Physically secured areas with controlled access, locked rooms, fenced perimeters, analog safes, motor housings, machine casings. **CPTB**: Secured areas with both physical barriers (locks, fences) and cyber controls (authentication, surveillance monitoring).
Store (S) Data, energy, or material at rest, distinct from its storage medium or container. Nesting is allowed.		**CS**: Files, databases, registry keys. **PS**: Raw materials, simple manufactured objects, physical keys. **CPS**: Smart materials, physical key cards, 3D-printed objects. *Note: The 3D-printed object's transformation from cyber to physical makes it vulnerable to time-dependent cyber-physical threats.*
Flow (F) Data, energy, or material in motion, distinct from its enabling path, channel or medium.		**CF**: Function calls, network communications, data transfers. **PF**: Material flows, energy transfers, mechanical forces. **CPF**: Sensor data streams, HVAC / IoT communications, transport of smart materials or devices, cyber-physical process I/Os.
Link (L) - New for CPFD A logical and/or physical path, channel, or medium that connects and enables Flows between CPFD elements.		**CL**: File formats / schema, data structures; communication ports, channels, & protocols. **PL**: Geographic routes, power lines, fluid pipes. **CPL**: RF spectrum, air (visible light / IR / acoustic transmission).
Process (P) Activity that transforms inputs into outputs.		**CP**: Only digital inputs and outputs, e.g. **any running code**. **PP:** Only physical inputs and outputs, e.g. manual manufacturing, simple raw material mixing / refining. **CPP**: Cyber-physical inputs and/or outputs, e.g. OT processes, smart manufacturing, automated logistics, robotic assembly, adaptive environmental control, etc.
Device (D) - New for CPFD An instantiation of computational capability and/or physical functionality for Processes and Stores; a virtually- and/or physically-embodied enabler of Processes and/or Storage in a cyber-physical system.		**CD**: Abstracted virtual / digital resources, e.g. virtual sensors and machines, Docker containers, digital twins, cloud compute instances, remote database servers, content delivery networks (CDN), cloud storage instances, distributed blockchain ledgers. **PD**: Mechanical actuators, manual valves, analog gauges, hydraulic motors, physical key storage lockboxes, material storage tanks, pressure vessels, chemical reagent containers. **CPD**: Embedded systems, smart thermostats, autonomous vehicles, IoT-enabled medical implants, OT actuators, desktop computers, 3D printers, smart inventory management systems, RFID-enabled storage cabinets, IoT-connected storage tanks with sensors.

Fig. 2. CPSTRIDE Cyber-physical Flow Diagram Specification

The DFD *Process (P)* element represents "any running code." This definition can be expanded to include analogous CPS processes, but we wish to distinguish between cyber-physical processes (e.g., manufacturing, refining, automated logistics) and the entities that enable them (e.g., manufacturing and refining equipment, logistic robots). We define the CPFD Process element as "activity that transforms inputs into outputs," modify its abbreviations and keep the graphical symbol, and choose to represent Process enablers with the new CPFD Device element. The new CPFD *Link* and *Device* elements represent the paths and media that enable Flows and the entities that enable Stores and Processes, respectively. Their definitions, abbreviations, and graphical symbols can be found in Figure 2; visually, these elements combine existing graphical conventions of Trust Boundaries, Flows, and Processes.

3.2 Security Properties and Threats

Our next task is to expand the STRIDE framework's Security Properties and corresponding Threats as needed to include CPS contexts; most of these need only minor modifications, which can be found in Figures 3 and 4. However, we find that Authentication, Confidentiality, and Information Disclosure are too narrowly data-centric for CPS, and require more substantial redefinition.

CPSTRIDE Cyber-Physical Security Properties

Highlighted rows contain new CPSTRIDE Security Properties.

Property	Definition
Authenticity (*previously Authentication*)	System elements (such as users, processes, devices, materials, and energy sources) are genuine and can be verified as what they claim to be. Authenticity replaces and includes the traditional *Authentication* security property for data systems while extending to the verification of physical components, materials, and energy signatures in cyber-physical contexts.
Integrity	System elements (such as data, software, firmware, hardware, materials, and energy parameters) remain unaltered and uncorrupted by unauthorized means throughout their lifecycle. This preserves the traditional data Integrity concept while expanding to include physical properties such as material composition, structural integrity, and energy calibration.
Non-Repudiation	Actions performed within the system cannot be denied by their initiator, through providing sufficient evidence of activities across cyber and physical domains. This extends beyond digital audit trails to include physical evidence trails, sensor data, surveillance records, and material verification techniques that establish accountability.
Containment (*previously Confidentiality*)	System elements (such as data, energy, and material resources) remain within their authorized boundaries and are accessible only to entities with appropriate privileges. Containment replaces and includes the traditional data *Confidentiality* security property, and more broadly represents the prevention of unauthorized cyber-physical extraction, leakage, or diversion.
Availability / Reliability	System functions, services, and resources are accessible and operational when needed, at expected performance levels. This maintains the traditional concept of digital Availability while extending to the physical reliability of components, consistent energy supply, material accessibility, and operational continuity across the cyber-physical spectrum.
Authorization	Specific entities are explicitly granted or denied permission to access, control, or modify certain system elements. This extends traditional digital access controls to include physical access rights, operational authority over equipment, material handling permissions, and energy distribution controls throughout the cyber-physical system.

Fig. 3. CPSTRIDE Security Properties Specification

The Authentication security property deals with the identification of users and software agents; we wish to expand the core meaning to include CPS analogs such as physical or cyber-physical parts or materials assumed to have come from a third-party supply chain provider. We define a new property – *Authenticity* – that includes the authentication of data entities as well as physical entities. Similarly, the Confidentiality property and corresponding Information Disclosure threat are too data-centric. The core meaning involves "(limiting) unauthorized access of valuable system elements and resources." These can be expanded to CPS analogs, such as the extraction or diversion of physical resources by unauthorized recipients, so we define a new security property and corresponding threat – *Containment* and *Interception* – that deal with (limiting) unauthorized interception of cyber-physical entities, including data (see Figures 3 and 4).

3.3 Susceptibility Matrix

Next, we consider that the STRIDE model conventionally assumes certain types of DFD elements to be immune to specific threats; for example, DFD Data Stores and Data Flows are considered immune to Spoofing; Interactors are assumed immune to Tampering; Information Disclosure; and Denial of Service threats; and Process elements are uniquely susceptible to Elevation of Privilege (see Figure 5). In the context of secure software development these assumptions may be reasonable. However, CPSTRIDE's inclusion of physical dimensions and novel attack vectors motivates their reexamination. In addition, we argue that although Interactors are outside of system scope and/or control, the exercise of considering the effects of attacks on Interactors can still inform system hardening. The same argument holds for all other CPFD elements and threat categories. Accordingly, we broaden the assumed susceptibility of all CPFD elements to all threat categories, and leave narrowing the matrix to future work.

4 AM Threat Modeling: CPSTRIDE vs. STRIDE

To show the advantages of CPSTRIDE over STRIDE, we perform the first two steps of the threat modeling process side-by-side. Since the third and fourth steps for both frameworks are identical, we leave them as a future exercise. The CPS to be modeled is an advanced additive manufacturing facility providing critical parts for downstream customers. The hardware setup consists of a commercial-grade bound metal deposition (BMD)-type 3D printer, a debinder, and a sintering furnace, as well as a workstation and a network router/switch.

4.1 Modeling the AM System

First we perform the CPSTRIDE version of Step 1, modeling the AM system with a CPFD (Figure 6). Each of the AM machines is modeled as a cyber-physical Device (CPD1-5). The router is connected via Cat5 ethernet cable to the other Devices, as well as to an enterprise network with Internet access. The networks

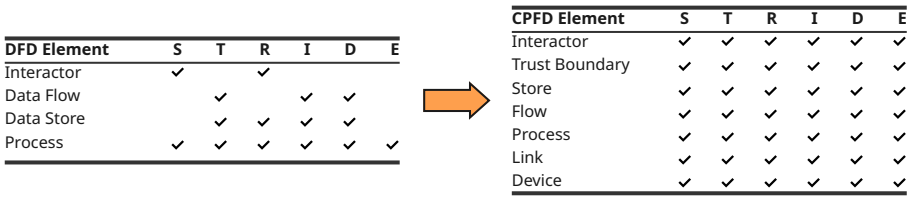
CPSTRIDE Cyber-Physical Threats

Each Threat potentially violates a corresponding Security Property. In the Examples column, *Cyber* indicates threats to information, data, control signal, etc.; *Physical* indicates threats to material, energy, force, etc.; *Cyber-physical* indicates the integration or combination of the two. Highlighted rows contain new CPSTRIDE Threats.

Threat	Definition	Examples **C:** *Cyber* **P:** *Physical* **CP:** *Cyber-physical*
Spoofing	Falsification of identity, source, or authenticity of system elements, including users, processes, signals, or physical/cyber-physical stores, undermining trust mechanisms and authentication controls within the CPS. *Violates Authenticity.*	**C:** Phishing, smishing, social engineering, malicious broadcast of trusted WiFi network SSID, typosquatting, deepfaking. **P:** Faking physical credentials, passing off counterfeit parts and materials as genuine, forging signatures on physical documents. **CP:** Broadcasting fake GPS to misguide autonomous vehicles or drones, injection of counterfeit OT sensor readings.
Tampering	Unauthorized modification, corruption, or alteration of legitimate cyber-physical entities including data, structures, energy flows, material compositions, or control signals, that compromises system integrity. *Violates Integrity.*	**C:** Modifying control logic in industrial automation software. **P:** Physically adjusting valve settings or equipment calibration screws. **CP:** Altering sensor readings through electromagnetic interference, causing the system to respond to fabricated conditions.
Repudiation	Denial of responsibility for actions within the system, either through passive rejection of accountability or active measures to destroy, corrupt, or disable auditing mechanisms or evidence trails that would establish proof of activities, legitimate or malicious. *Violates Non-repudiation.*	**C:** Disabling logging mechanisms to hide evidence of digital access. **P:** Destroying physical access records or tampering with surveillance footage. **CP:** Cross-domain log corruption.
Interception *(previously Information Disclosure)*	Unauthorized acquisition or monitoring of system resources, including data, energy flows, or physical materials, violating containment. Interception replaces and includes the traditional Information Disclosure threat, and *Violates Containment.*	**C:** Capturing sensitive control data through network sniffing. **P:** Physically extracting / diverting material from manufacturing processes. **CP:** Harvesting energy from wireless power transmission systems through unauthorized coupling.
Denial of Service	Impairment or prevention of system availability through any means that renders services, functions, or resources inaccessible or unreliable for legitimate users. *Violates Availability / Reliability.*	**C:** Network flooding, resource exhaustion, communication jamming. **P:** Blockage of moving parts; permanent damage by physical destruction, component sabotage, or irreversible physical alterations; energy disruption through power supply manipulation or battery depletion; environmental manipulation to introduce adverse conditions. **CP:** Creating electromagnetic interference to disrupt wireless communications and/or electronic sensors, physical obstruction of sensors/actuators.
Elevation of Privilege	Exploitation of system vulnerabilities to gain unauthorized higher-level access rights beyond assigned permissions. *Violates Authorization.*	**C:** Traditional privilege elevation cyber-techniques such as exploiting software vulnerabilities to gain administrative access to control systems. **P:** Obtaining master keys or accessing restricted physical areas without authorization. **CP:** Using physical access to maintenance ports to install privileged software that bypasses normal authorization controls.

Fig. 4. CPSTRIDE Threats Specification

Fig. 5. Assumed susceptibility for DFD and CPFD elements.



DFD Element	S	T	R	I	D	E
Interactor	✓		✓			
Data Flow		✓		✓	✓	
Data Store		✓	✓	✓	✓	
Process	✓	✓	✓	✓	✓	✓

CPFD Element	S	T	R	I	D	E
Interactor	✓	✓	✓	✓	✓	✓
Trust Boundary	✓	✓	✓	✓	✓	✓
Store	✓	✓	✓	✓	✓	✓
Flow	✓	✓	✓	✓	✓	✓
Process	✓	✓	✓	✓	✓	✓
Link	✓	✓	✓	✓	✓	✓
Device	✓	✓	✓	✓	✓	✓

are modeled as cyber-Interactors (CI1, CI2) and each physical connection is modeled as a cyber-physical Link (CPL1-6). Four cyber-physical Interactors are modeled: an internal designer/engineer, an operator/controller, an external material supply chain provider, and a critical downstream manufacturer (CPI1-4).

The AM process chain is broken into nine steps. Digital process chain steps from CAD design to toolpath transmission are represented by cyber-Processes (CP2-6) connected by cyber and cyber-physical Flows (CPF1, CPF2, CF1-10), while physical part production is represented by cyber-physical Processes (CPP1-4) with cyber (toolpath) and cyber-physical (material cartridge, physical part, operator input) input Flows (CF11, CPF3-12, CPF15).

Part CAD files are modeled as nested cyber-stores (CS2, NCS2.1-2.5) located on the workstation, and the AM part material cartridge is modeled as a cyber-physical store (CPS1). The physical stages of manufactured part production are modeled as four separate cyber-physical stores (CPS2-CPS5). Other modeled entities include material transport to and from the external downstream manufacturer and supply chain provider (cyber-physical Flows CPF13-14), both of which cross the primary AM Facility Cyber-Physical Trust Boundary (CPTB1); the operator/controller's quality control inspection of the AM part in the final production step (physical flow PF1); the transmission of design requirements and production parameters from the enterprise network to the human Interactors and the CAD files (cyber Flows CF12-14); and the emanation of RF and acoustic energy from the 3-D printer during operation (cyber-physical Link CPL7).

Next we perform the STRIDE version of Step 1, modeling the AM system with a DFD (Figure 7). The AM facility is modeled as a Trust Boundary (TB1), with the Internet, human designer/engineer and operator/controller, router/switch and enterprise modeled as Interactors (I1-5). The AM process chain is modeled as 9 separate Processes (P1-9) with 20 Data Flows (DF1-20). CAD files are modeled as individual Data Stores (DS1-5), and the transmission of design requirements and production parameters from the enterprise network to the humans and router are modeled by Data Flows (DF14, DF21-22), but omitted for the CAD files to avoid cluttering the diagram. Physical entities are not modeled, nor are entities which only interact with the system physically; this includes several Links, Stores, and Devices modeled in the CPFD, as well as the supply chain and downstream manufacturing Interactors.

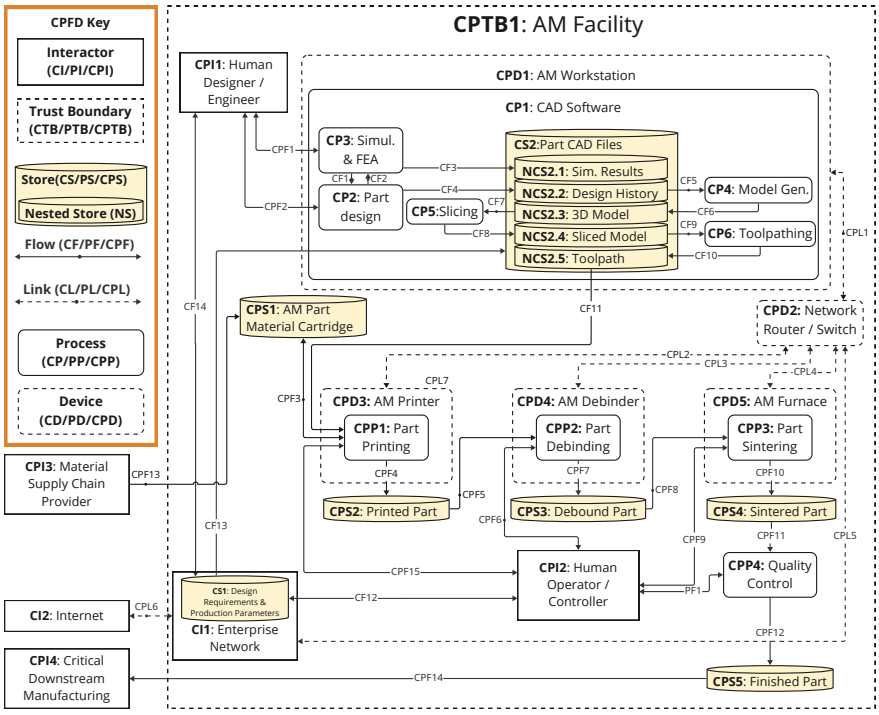


Fig. 6. Cyber-Physical Flow Diagram (CPFD) for additive manufacturing facility.

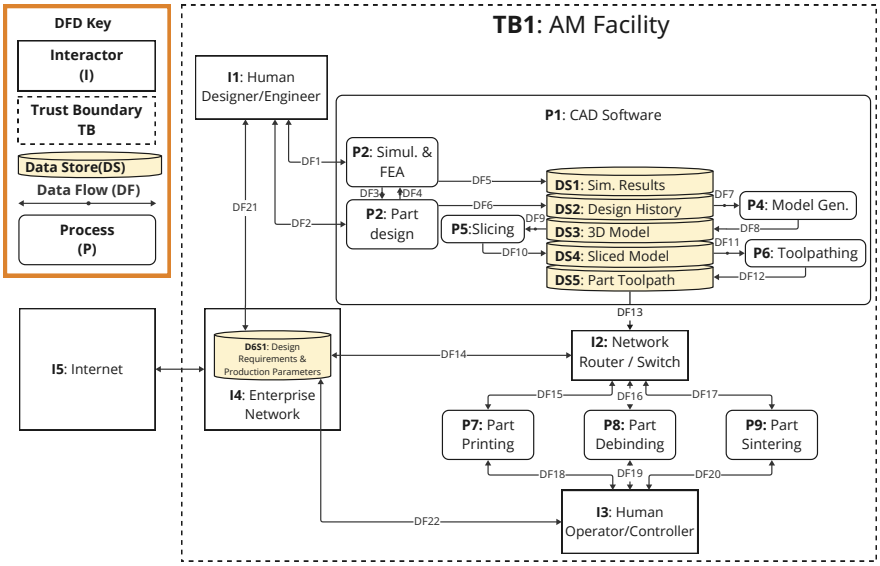


Fig. 7. Data Flow Diagram (DFD) for additive manufacturing facility.

4.2 AM Threat Identification

Next, we perform threat identification in both frameworks. This entails considering how the threat categories apply to elements from the flow diagrams in Step 1. For instance, to identify threats against the STRIDE representation of the 3-D Model (DS3) element in the DFD, we consult the susceptibility matrix (Figure 5) and find that STRIDE Data Stores are susceptible to Tampering, Repudiation, Information Disclosure, and Denial of Service. We then consider how each applies to the 3-D Model; Tampering with the 3-D Model could alter the design of the part; a Repudiation threat might modify parts of the 3-D Model's history; an Information Disclosure threat might represent theft of IP in the 3-D Model or leaking it to the public; a Denial of Service threat could represent ransomware or deletion of the 3-D Model. Each relevant threat category is used as a brainstorming prompt that helps the threat modeler generate examples of threats to each flow diagram element modeled in the system. This process repeats until all susceptibilities to threat have been considered for all elements.

This approach generates rich, comprehensive lists of threats to the system, but suffers from at least three problems. First, it is time consuming; the larger and more complex the system flow diagram is, the more threats there are to identify. Second, it relies on expert knowledge; cyber-security professionals can consult online repositories such as MITRE ATT&CK and CVE to help identify likely cyber threats, but must also be well acquainted with the architecture and function of their system. Since there are no global, standardized, and regularly updated cyber-physical threat databases mirroring CVE for CPS, threat modelers have to rely even more on their expert knowledge of these systems.

The third problem with Step 2 of STRIDE/CPSTRIDE is ambiguity. What does it mean to ask how a threat category applies to an element? Are we asking whether the element is the subject of a threat, i.e., performing the threat action? Are we asking whether the element is the object (target/victim) of the threat? Or perhaps we are considering whether an element is an instrument (used as a means to threaten another target) of a threat, or something else altogether.

Fortunately, the first two drawbacks can be partially alleviated through the use of automation. In response to the third, we adopt a posture of systematically considering each threat category / element combination from all three of the perspectives mentioned above (subject, object, and instrument). The automation employed for our differential analysis of STRIDE and CPSTRIDE is Anthropic's Claude 3.7 Sonnet large language model (LLM) assistant.

4.3 LLM Assisted Threat Modeling

We metaprompt the LLM to serve as a subject matter expert in threat modeling, providing it with specifications for the CPSTRIDE and STRIDE models [8,11]; the full metaprompt and conversation can be found in the project repository.

As the LLM serves as a subject matter expert, we assume the following:

– Given sufficient time, a knowledgeable human professional could complete full threat identification for both STRIDE and CPSTRIDE.

– Due to the additional CPSTRIDE elements, effects, and interactions, there would be many more threats identified by the CPSTRIDE process.
– STRIDE could not capture threats missed by CPSTRIDE if both threat identification processes were performed with identical rigor.

Accordingly, we pursue a first-order approximation of these results by instructing the LLM to identify all elements in the AM-CPFD for which no corresponding AM-DFD element exists, and then to create a CPSTRIDE threat identification matrix for the AM-CPFD using only these elements – the goal being to expose threats considered by the CPSTRIDE process that STRIDE could not.

The full conversation with the LLM is found at the repository link at the end of the article. We direct the LLM to focus on physical and cyber-physical threats for the processes identified, rather than purely cyber threats that STRIDE would identify. We also instruct it to consider each threat category / element combination in terms of subject, object, and instrument contexts. We instruct the LLM to identify realistic threats only, that filling each cell is not necessary, and that it should work through the matrix systematically, if needed, completing a small number of rows at a time and awaiting prompting to continue building the matrix. Finally, we give the LLM permission to group elements with similar or identical threats to reduce redundancy in the matrix, and give formatting instructions.

[[**THE RESULTS OF THE LLM-ASSISTED THREAT MODELING EXERCISE CAN BE FOUND IN THE FULL CPSTRIDE PAPER**]]

Competing Interests. The authors have no competing interests to declare that are relevant to the content of this article.

Repository. An anonymized repository for CPSTRIDE that includes figures, tables, and LLM prompts and conversations can be found online at the following address: https://anonymous.4open.science/r/CPSTRIDE-5D65

References

1. Al Faruque, M., Chhetri, S.R., Canedo, A., Wan, J.: Acoustic Side-Channel Attacks on Additive Manufacturing Systems. In: 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS). pp. 1–10 (Apr 2016). https://doi.org/10.1109/ICCPS.2016.7479068
2. Al Faruque, M., Chhetri, S.R., Faezi, S., Canedo, A.: Forensics of Thermal Side-Channel in Additive Manufacturing Systems. Technical Report 16-01, University of California, Irvine; Siemens Corporation, Center for Embedded and Cyber-Physical Systems (Jan 2016)
3. Beaman, J.J., Bourell, D.L., Seepersad, C.C., Kovar, D.: Additive Manufacturing Review: Early Past to Current Practice. Journal of Manufacturing Science and Engineering **142**(11), 110812 (Nov 2020). https://doi.org/10.1115/1.4048193

4. Belikovetsky, S., Yampolskiy, M., Toh, J., Gatlin, J., Elovici, Y.: dr0wned – Cyber-Physical Attack with Additive Manufacturing. In: 11th USENIX Workshop on Offensive Technologies. p. 16. USENIX (2017)
5. Duo, W., Zhou, M., Abusorrah, A.: A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica **9**(5), 784–800 (May 2022). https://doi.org/10.1109/JAS.2022.105548
6. Graves, L., King, W., Carrion, P., Shao, S., Shamsaei, N., Yampolskiy, M.: Sabotaging metal additive manufacturing: Powder delivery system manipulation and material-dependent effects. Additive Manufacturing **46**, 102029 (Oct 2021). https://doi.org/10.1016/j.addma.2021.102029
7. Gupta, N., Tiwari, A., Bukkapatnam, S.T.S., Karri, R.: Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks. IEEE Access **8**, 47322–47333 (2020). https://doi.org/10.1109/ACCESS.2020.2978815
8. Hernan, S., Lambert, S., Ostwald, T., Shostack, A.: Uncover Security Design Flaws Using The STRIDE Approach. Microsoft MSDN Magazine (Nov 2006), https://learn.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach
9. Hojjati, A., Adhikari, A., Struckmann, K., Chou, E., Tho Nguyen, T.N., Madan, K., Winslett, M.S., Gunter, C.A., King, W.P.: Leave Your Phone at the Door: Side Channels that Reveal Factory Floor Secrets. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 883–894. ACM, Vienna Austria (Oct 2016). https://doi.org/10.1145/2976749.2978323
10. Khan, R., McLaughlin, K., Laverty, D., Sezer, S.: STRIDE-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). pp. 1–6 (Sep 2017). https://doi.org/10.1109/ISGTEurope.2017.8260283
11. Kohnfelder, Loren, Garg, Praerit: The-Threats-To-Our-Products (Apr 1999), https://shostack.org/files/microsoft/The-Threats-To-Our-Products.docx
12. McCormack, M., Chandrasekaran, S., Liu, G., Yu, T., DeVincent Wolf, S., Sekar, V.: Security Analysis of Networked 3D Printers. In: 2020 IEEE Security and Privacy Workshops (SPW). pp. 118–125 (May 2020). https://doi.org/10.1109/SPW50608.2020.00035
13. Rahman, H., Shafae, M.: Cyber-Physical Security Vulnerabilities Identification and Classification in Smart Manufacturing: A Defense-in-Depth Driven Framework and Taxonomy (2024), https://arxiv.org/abs/2501.09023
14. Saßnick, O., Rosenstatter, T., Schäfer, C., Huber, S.: STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review. In: 2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS). pp. 1–8 (May 2024). https://doi.org/10.1109/ICPS59941.2024.10639949, iSSN: 2769-3899
15. Shostack, A.: adamshostack/DFD3 (Apr 2025), https://github.com/adamshostack/DFD3, original-date: 2017-11-05T21:20:58Z
16. Sturm, L.D., Williams, C.B., Camelio, J.A., White, J., Parker, R.: Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects. Journal of Manufacturing Systems **44**, 154–164 (Jul 2017). https://doi.org/10.1016/j.jmsy.2017.05.007
17. Yampolskiy, M., Graves, L., Gatlin, J., Skjellum, A., Yung, M.: What Did You Add to My Additive Manufacturing Data?: Steganographic Attacks on 3D Printing Files. In: 24th International Symposium on Research in Attacks, Intrusions and Defenses. pp. 266–281. ACM, San Sebastian Spain (Oct 2021). https://doi.org/10.1145/3471621.3471843

18. Yampolskiy, M., Horvath, P., Koutsoukos, X.D., Xue, Y., Sztipanovits, J.: Systematic analysis of cyber-attacks on CPS-evaluating applicability of DFD-based approach. In: 2012 5th International Symposium on Resilient Control Systems. pp. 55–62 (Aug 2012). https://doi.org/10.1109/ISRCS.2012.6309293
19. Yampolskiy, M., King, W.E., Gatlin, J., Belikovetsky, S., Brown, A., Skjellum, A., Elovici, Y.: Security of additive manufacturing: Attack taxonomy and survey. Additive Manufacturing **21**, 431–457 (May 2018). https://doi.org/10.1016/j.addma.2018.03.015