CPSTRIDE: A Threat Modeling Framework for Cyber-Physical Systems

Dallas Elleman & John Hale

CRITIS 2025
Högskolan i Jönköping - 2025.10.22

Cyber Fellows

THE UNIVERSITY of TULSA

Agenda

1. Overview & Contributions
2. Background
   - ➢ Additive Manufacturing cyber-physical systems (CPS)
   - ➢ The STRIDE framework
3. CPSTRIDE Framework Specification
   - ➢ CPFD: Cyber-Physical Flow Diagram
   - ➢ CPSec Properties, Threats, & Susceptibility Matrix
4. LLM-assisted comparative threat modeling for additive manufacturing CPS
5. Discussion
   - ➢ Advantages, Limitations, and Challenges
   - ➢ Future Work
6. Conclusion

Overview

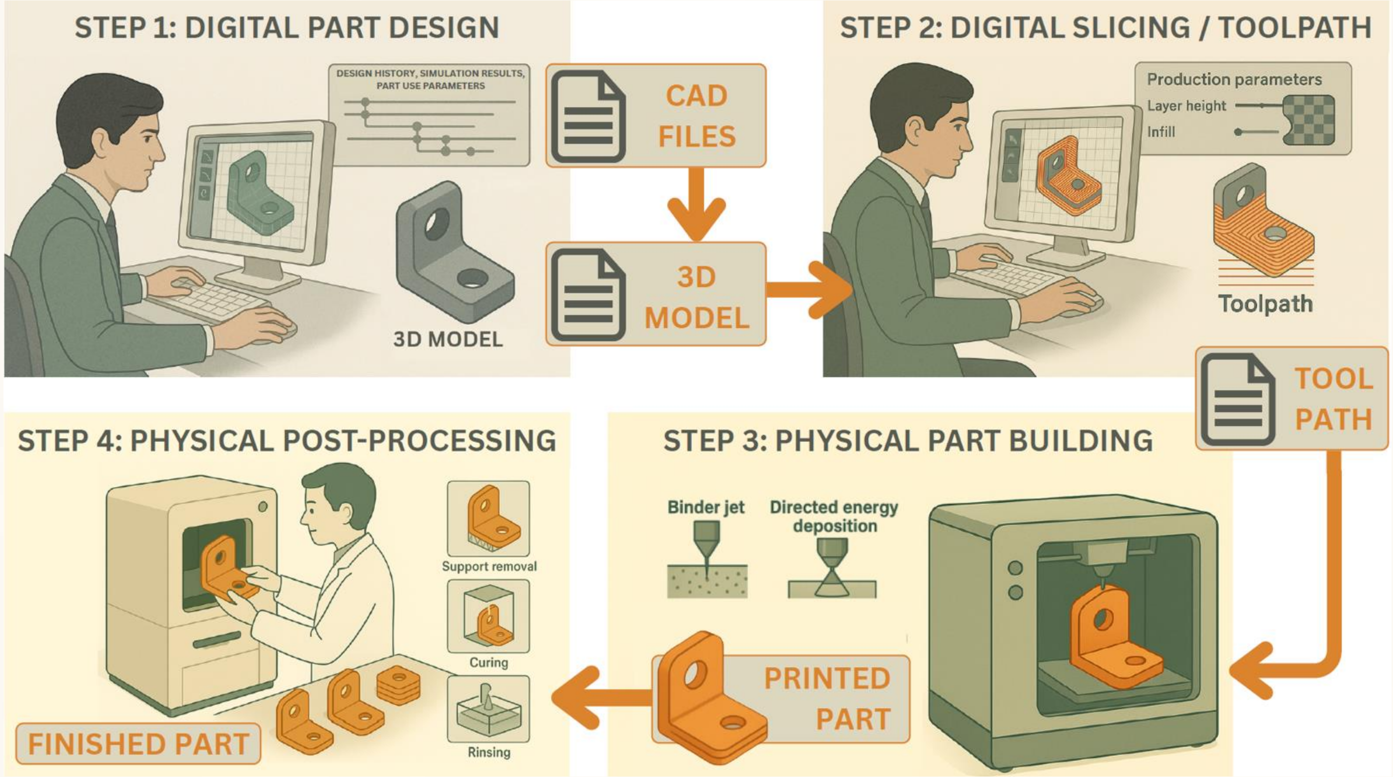
“Det finns inget dåligt väder, bara dåliga kläder."

“There are no bad cyber-physical threat models, only bad frameworks.”

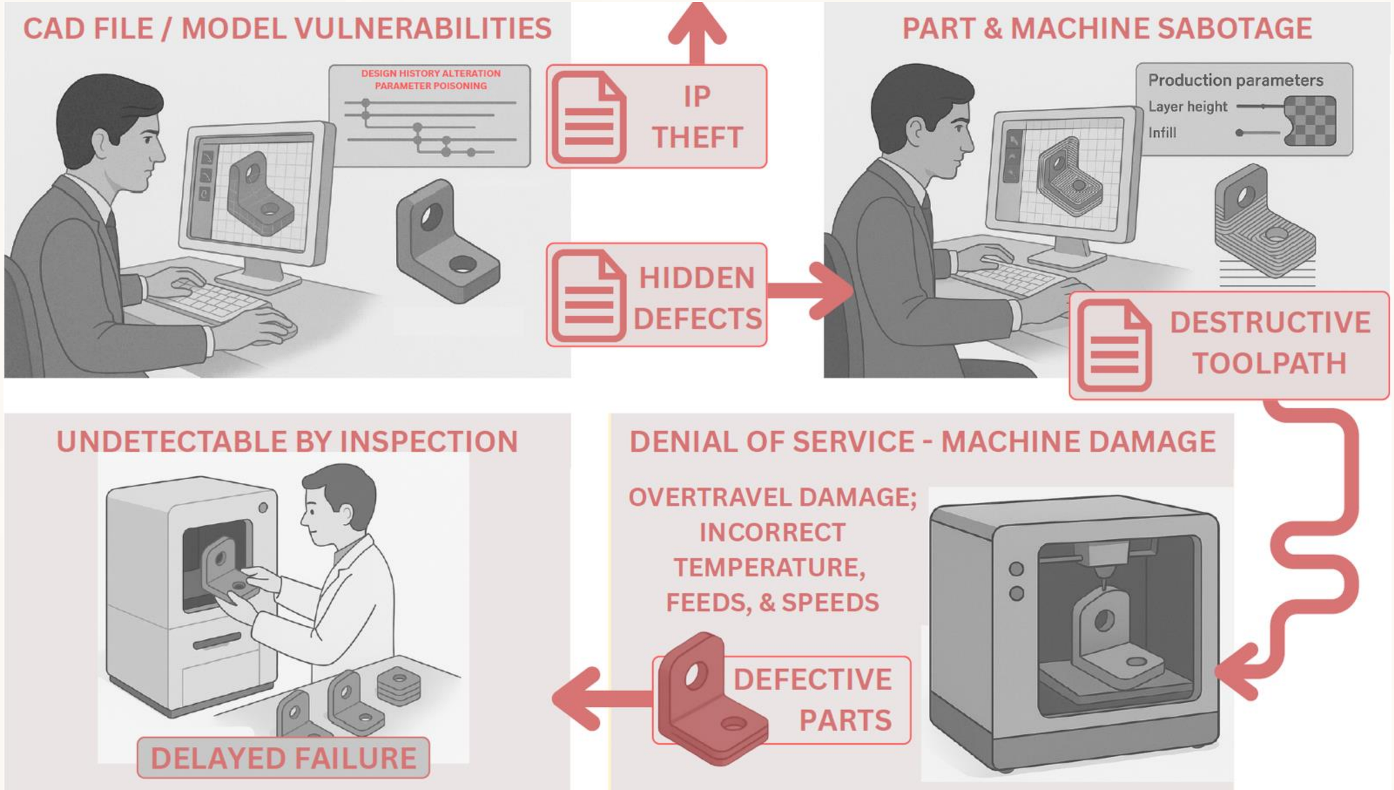
Contributions

1. CPSTRIDE – A better threat modeling framework for CPS
2. Comparative threat modeling: CPSTRIDE vs. STRIDE
3. LLM-assisted threat modeling

Additive manufacturing cyber-physical process chain


STEP 1: DIGITAL PART DESIGN
DESIGN HISTORY, SIMULATION RESULTS, PART USE PARAMETERS
3D MODEL
CAD FILES
3D MODEL
STEP 2: DIGITAL SLICING / TOOLPATH
Production parameters
Layer height
Infill
Toolpath
TOOL PATH
STEP 3: PHYSICAL PART BUILDING
Binder jet
Directed energy deposition
PRINTED PART
STEP 4: PHYSICAL POST-PROCESSING
Support removal
Curing
Rinsing
FINISHED PART

Additive manufacturing cyber-physical threats



CAD FILE / MODEL VULNERABILITIES

IP THEFT

HIDDEN DEFECTS

PART & MACHINE SABOTAGE

DESTRUCTIVE TOOLPATH

DENIAL OF SERVICE - MACHINE DAMAGE

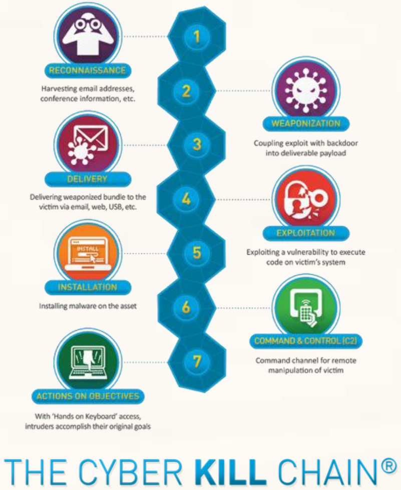
OVERTRAVEL DAMAGE; INCORRECT TEMPERATURE, FEEDS, & SPEEDS

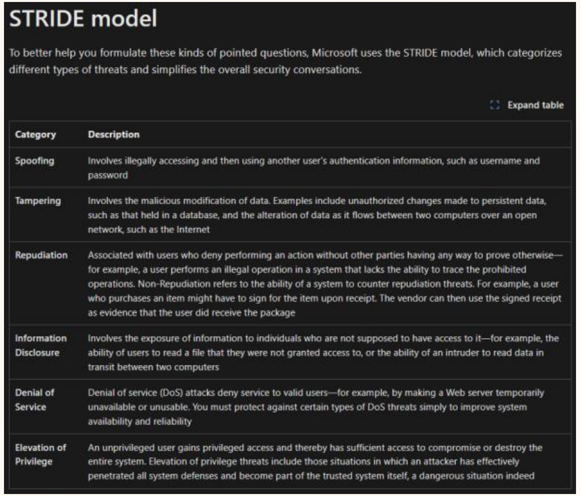
DEFECTIVE PARTS

UNDETECTABLE BY INSPECTION

DELAYED FAILURE

Popular threat modeling frameworks

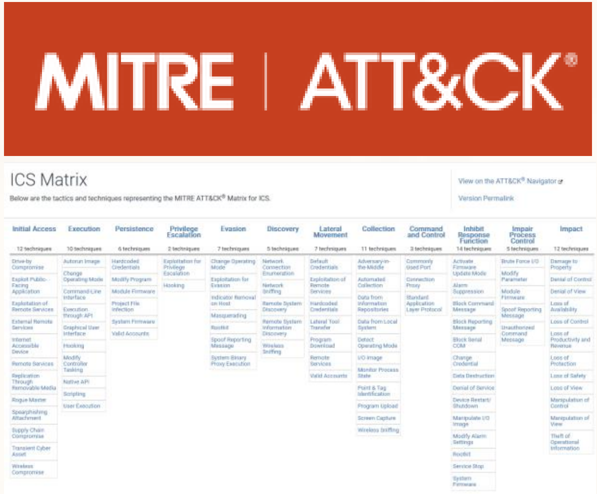

1
2
3
4
5
6
7
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
INSTALL
INSTALLATION
Installing malware on the asset
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals
THE CYBER KILL CHAIN®



STRIDE model

To better help you formulate these kinds of pointed questions, Microsoft uses the STRIDE model, which categorizes different types of threats and simplifies the overall security conversations.

Category	Description
Spoofing	Involves illegally accessing and then using another user's authentication information, such as username and password
Tampering	Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
Repudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
Information Disclosure	Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers
Denial of Service	Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
Elevation of Privilege	An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed



ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	10 techniques	6 techniques	2 techniques	7 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Autorun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

**None of these frameworks explicitly consider physical entities / processes.
Cyber-physical systems need first-class tickets.**

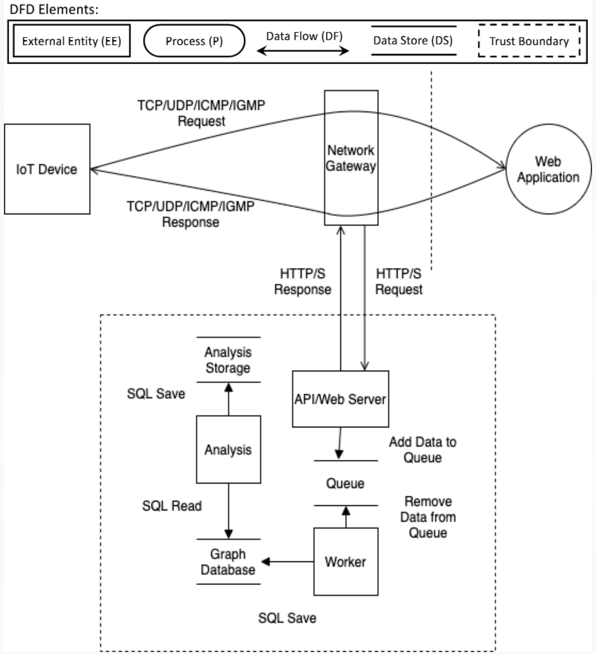
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats
https://attack.mitre.org/matrices/ics/

The STRIDE framework

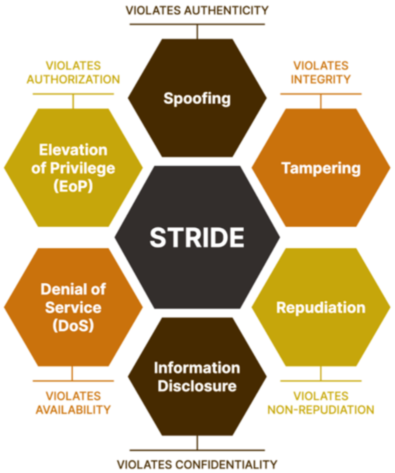
Mature, well-known and widely-used framework for cyber threats.

Threat modeling process:

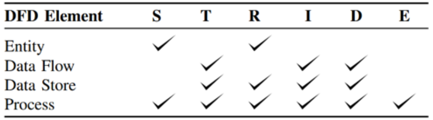
1. Create Data Flow Diagram
2. Identify threats to DFD elements
3. Investigate & prioritize threats
4. Mitigate vulnerabilities



Step 1: Create DFD



Susceptibility of DFD elements to STRIDE threats.



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

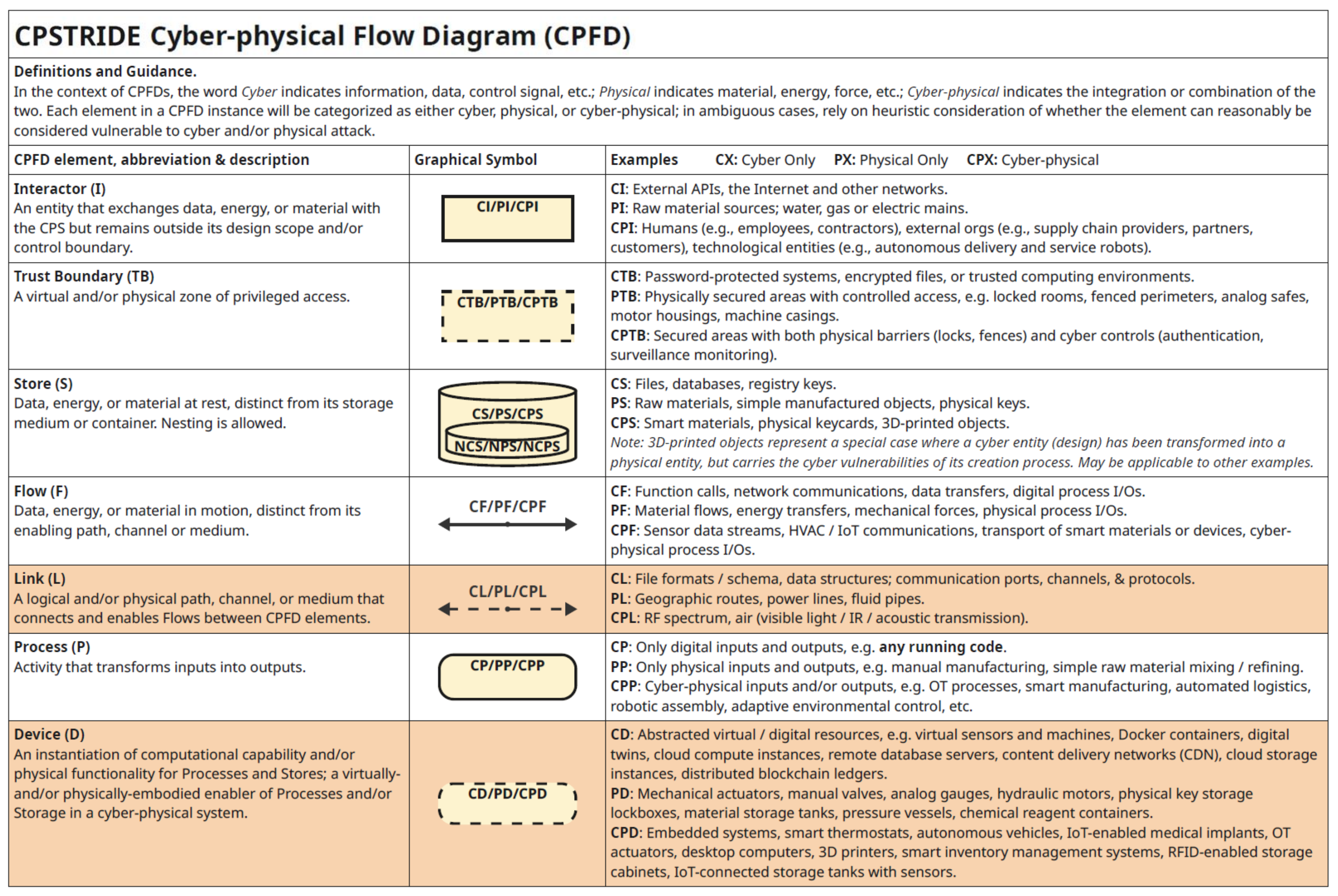
Step 2: Identify Threats

DFD Example: Oreilly, Jonathon & Nagappan, Ramesh. (2019). Passive Data Collection and Threat Identification through use of a Graph Database in IoT Devices.
STRIDE threats diagram: https://medium.com/@arielhacking/examples-of-stride-threats-for-payment-applications-87a0ad0c3a21

CPSTRIDE framework specification

What parts of STRIDE need to be expanded to be a better cyber-physical security framework?

1. Data Flow Diagram
2. Security Properties
3. Security Threats
4. Susceptibility Matrix



CPSTRIDE Cyber-physical Flow Diagram (CPFD)

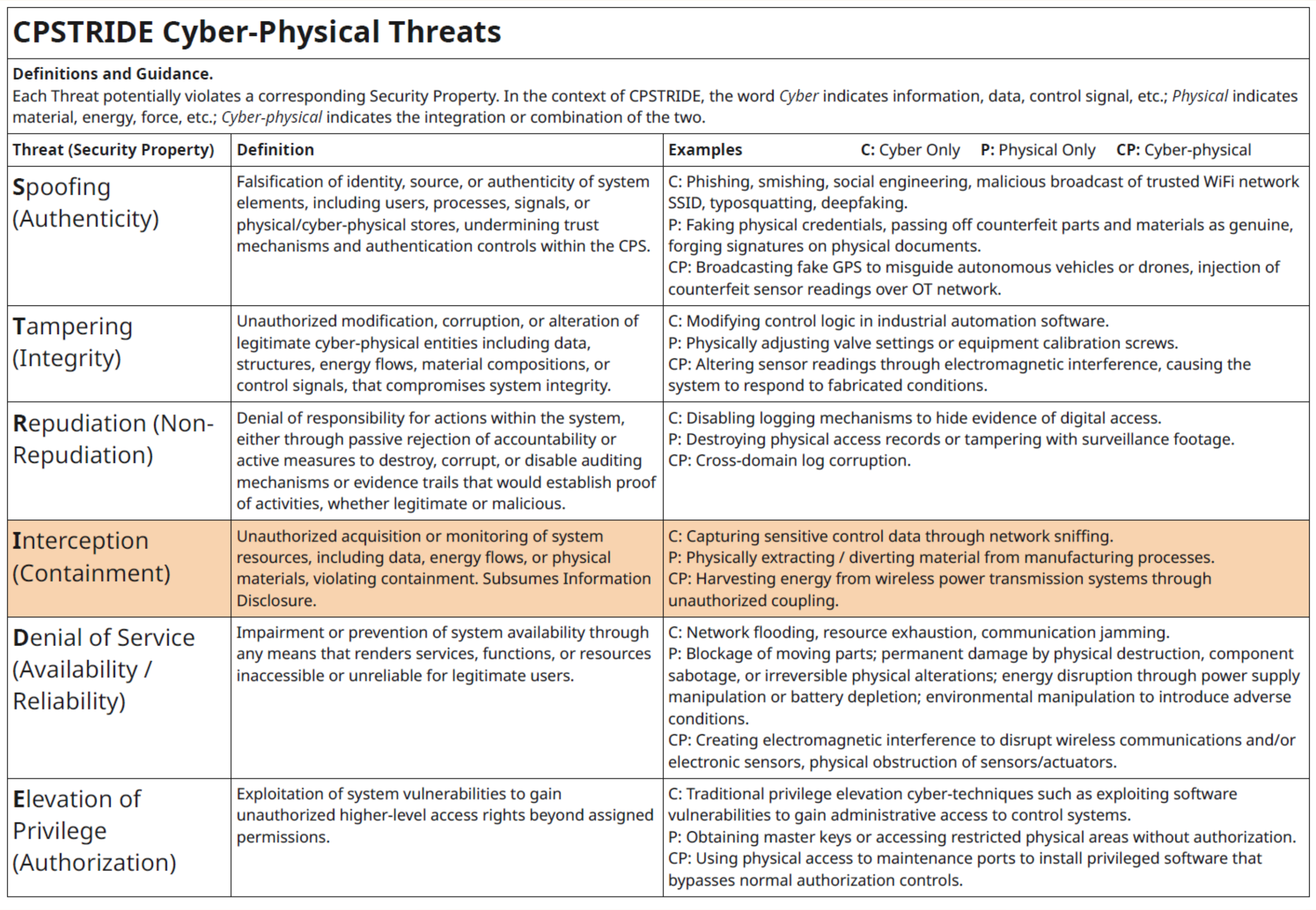
Definitions and Guidance.
In the context of CPFDs, the word *Cyber* indicates information, data, control signal, etc.; *Physical* indicates material, energy, force, etc.; *Cyber-physical* indicates the integration or combination of the two. Each element in a CPFD instance will be categorized as either cyber, physical, or cyber-physical; in ambiguous cases, rely on heuristic consideration of whether the element can reasonably be considered vulnerable to cyber and/or physical attack.

CPFD element, abbreviation & description	Graphical Symbol	Examples **CX:** Cyber Only **PX:** Physical Only **CPX:** 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/PI/CPI	**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/PTB/CPTB	**CTB**: Password-protected systems, encrypted files, or trusted computing environments. **PTB**: Physically secured areas with controlled access, e.g. 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/PS/CPS NCS/NPS/NCPS	**CS**: Files, databases, registry keys. **PS**: Raw materials, simple manufactured objects, physical keys. **CPS**: Smart materials, physical keycards, 3D-printed objects. *Note: 3D-printed objects represent a special case where a cyber entity (design) has been transformed into a physical entity, but carries the cyber vulnerabilities of its creation process. May be applicable to other examples.*
Flow (F) Data, energy, or material in motion, distinct from its enabling path, channel or medium.	CF/PF/CPF	**CF**: Function calls, network communications, data transfers, digital process I/Os. **PF**: Material flows, energy transfers, mechanical forces, physical process I/Os. **CPF**: Sensor data streams, HVAC / IoT communications, transport of smart materials or devices, cyber-physical process I/Os.
Link (L) A logical and/or physical path, channel, or medium that connects and enables Flows between CPFD elements.	CL/PL/CPL	**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/PP/CPP	**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) 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/PD/CPD	**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.

CPSTRIDE Cyber-Physical Security Properties

Property	Definition
Authenticity (subsumes 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 subsumes the traditional Authentication 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 (subsumes 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 subsumes traditional data Confidentiality while encompassing physical confinement of materials and energy to prevent unauthorized 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.

Cyber Fellows



CPSTRIDE Cyber-Physical Threats

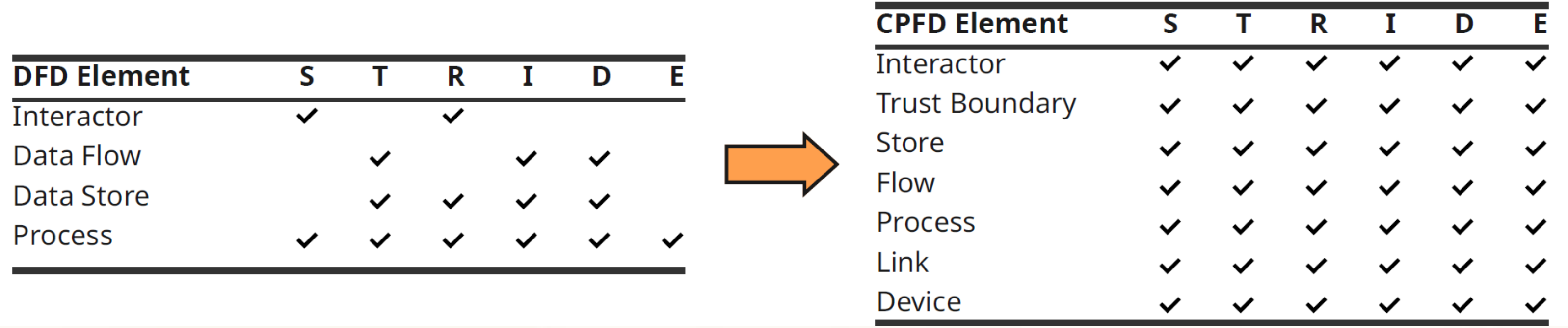
Definitions and Guidance.
Each Threat potentially violates a corresponding Security Property. In the context of CPSTRIDE, the word *Cyber* indicates information, data, control signal, etc.; *Physical* indicates material, energy, force, etc.; *Cyber-physical* indicates the integration or combination of the two.

Threat (Security Property)	**Definition**	**Examples** **C:** Cyber Only **P:** Physical Only **CP:** Cyber-physical
Spoofing (Authenticity)	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.	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 sensor readings over OT network.
Tampering (Integrity)	Unauthorized modification, corruption, or alteration of legitimate cyber-physical entities including data, structures, energy flows, material compositions, or control signals, that compromises system 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 (Non-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, whether legitimate or malicious.	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 (Containment)	Unauthorized acquisition or monitoring of system resources, including data, energy flows, or physical materials, violating containment. Subsumes Information Disclosure.	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 (Availability / Reliability)	Impairment or prevention of system availability through any means that renders services, functions, or resources inaccessible or unreliable for legitimate users.	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 (Authorization)	Exploitation of system vulnerabilities to gain unauthorized higher-level access rights beyond assigned permissions.	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.

THE UNIVERSITY of TULSA

Cyber Fellows

CPSTRIDE Susceptibility Matrix

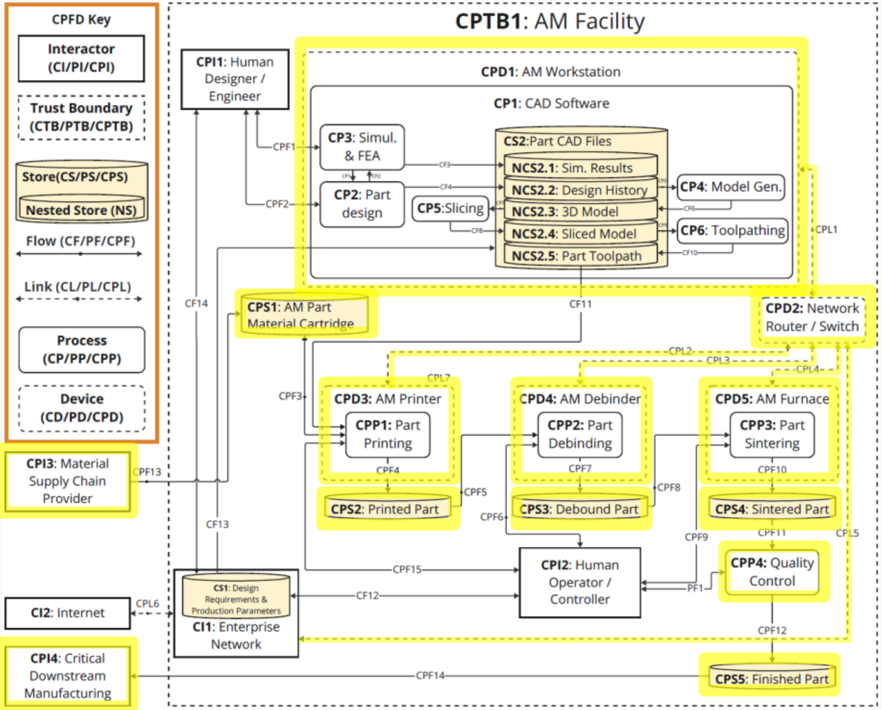


DFD Element	S	T	R	I	D	E
Interactor	✓		✓			
Data Flow		✓		✓	✓	
Data Store		✓	✓	✓	✓	
Process	✓	✓	✓	✓	✓	✓

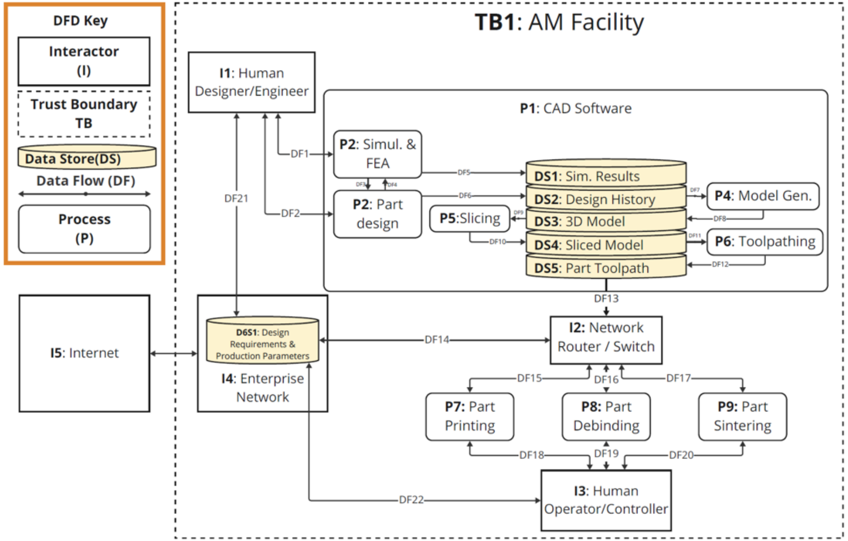
CPFD Element	S	T	R	I	D	E
Interactor	✓	✓	✓	✓	✓	✓
Trust Boundary	✓	✓	✓	✓	✓	✓
Store	✓	✓	✓	✓	✓	✓
Flow	✓	✓	✓	✓	✓	✓
Process	✓	✓	✓	✓	✓	✓
Link	✓	✓	✓	✓	✓	✓
Device	✓	✓	✓	✓	✓	✓

Comparative threat modeling for AM CPS

CPSTRIDE CPFD



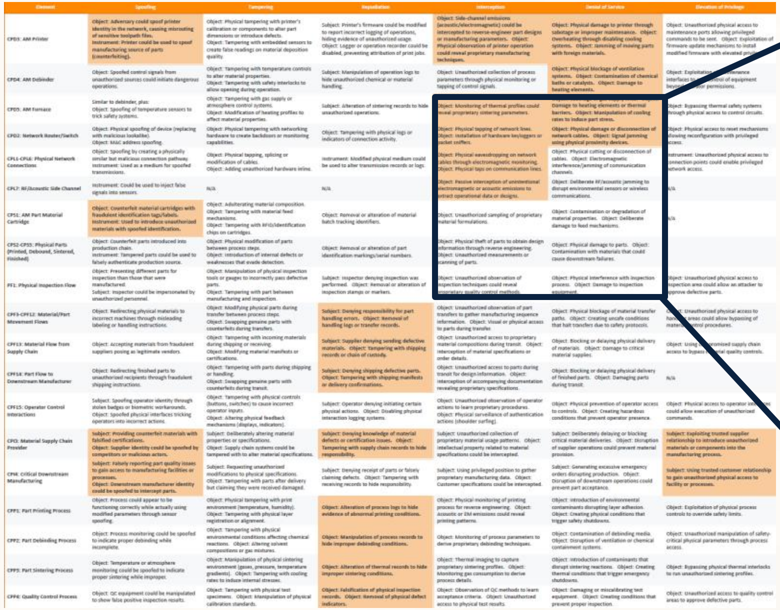
STRIDE DFD



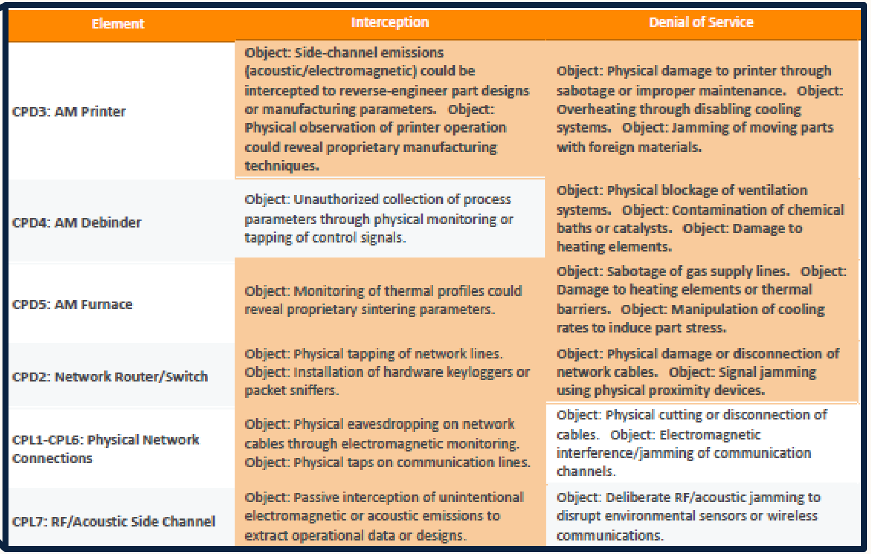
LLM-assisted comparative threat modeling for AM CPS

- Claude 3.7 Sonnet assumes role of subject matter expert.
- Orange Highlights: Physical & cyber-physical threats

STRIDE



Element	Spoofing	Tampering	Repudiation	Interception	Denial of Service	Elevation of Privilege
CPD3: AM Printer	Object: Adversary could spoof printer identity in the network, causing misrouting of sensitive toolpath files. Instrument: Printer could be used to spoof manufacturing source of parts (counterfeiting).	Object: Physical tampering with printer's calibration or components to alter part dimensions or introduce defects. Object: Tampering with embedded sensors to create false readings on material deposition quality.	Subject: Printer's firmware could be modified to report incorrect logging of operations, hiding evidence of unauthorized usage. Object: Logger or operation recorder could be disabled, preventing attribution of print jobs.	Object: Side-channel emissions (acoustic/electromagnetic) could be intercepted to reverse-engineer part designs or manufacturing parameters. Object: Physical observation of printer operation could reveal proprietary manufacturing techniques.	Object: Physical damage to printer through sabotage or improper maintenance. Object: Overheating through disabling cooling systems. Object: Jamming of moving parts with foreign materials.	Object: Unauthorized physical access to maintenance ports allowing privileged commands to be sent. Object: Exploitation of firmware update mechanisms to install modified firmware with elevated privileges.
CPD4: AM Debinder	Object: Spoofed control signals from unauthorized sources could initiate dangerous operations.	Object: Tampering with temperature controls to alter material properties. Object: Tampering with safety interlocks to allow opening during operation.	Subject: Manipulation of operation logs to hide unauthorized chemical or material handling.	Object: Unauthorized collection of process parameters through physical monitoring or tapping of control signals.	Object: Physical blockage of ventilation systems. Object: Contamination of chemical baths or catalysts. Object: Damage to heating elements.	Object: Exploitation [illegible] maintenance interfaces to [illegible] control of equipment beyond [illegible] permissions.
CPD5: AM Furnace	Similar to debinder, plus: Object: Spoofing of temperature sensors to trick safety systems.	Object: Tampering with gas supply or atmosphere control systems. Object: Modification of heating profiles to affect material properties.	Subject: Alteration of sintering records to hide unauthorized operations.	Object: Monitoring of thermal profiles could reveal proprietary sintering parameters.	Object: Sabotage of gas supply lines. Object: Damage to heating elements or thermal barriers. Object: Manipulation of cooling rates to induce part stress.	Object: Bypassing thermal safety systems through physical access to control circuits.
CPD2: Network Router/Switch	Object: Physical spoofing of device (replacing with malicious lookalike). Object: MAC address spoofing.	Object: Physical tampering with networking hardware to create backdoors or monitoring capabilities.	Object: Tampering with physical logs or indicators of connection activity.	Object: Physical tapping of network lines. Object: Installation of hardware keyloggers or packet sniffers.	Object: Physical damage or disconnection of network cables. Object: Signal jamming using physical proximity devices.	Object: Physical access to reset mechanisms allowing reconfiguration with privileged access.
CPL1-CPL6: Physical Network Connections	Object: Spoofing by creating a physically similar but malicious connection pathway. Instrument: Used as a medium for spoofed transmissions.	Object: Physical tapping, splicing or modification of cables. Object: Adding unauthorized hardware inline.	Instrument: Modified physical medium could be used to alter transmission records or logs.	Object: Physical eavesdropping on network cables through electromagnetic monitoring. Object: Physical taps on communication lines.	Object: Physical cutting or disconnection of cables. Object: Electromagnetic interference/jamming of communication channels.	Instrument: Unauthorized physical access to connection points could enable privileged network access.
CPL7: RF/Acoustic Side Channel	Instrument: Could be used to inject false signals into sensors.	N/A	N/A	Object: Passive interception of unintentional electromagnetic or acoustic emissions to extract operational data or designs.	Object: Deliberate RF/acoustic jamming to disrupt environmental sensors or wireless communications.	N/A
CPS1: AM Part Material Cartridge	Object: Counterfeit material cartridges with fraudulent identification tags/labels. Instrument: Used to introduce unauthorized materials with spoofed identification.	Object: Adulterating material composition. Object: Tampering with material feed mechanisms. Object: Tampering with RFID/identification chips on cartridges.	Object: Removal or alteration of material batch tracking identifiers.	Object: Unauthorized sampling of proprietary material formulations.	Object: Contamination or degradation of material properties. Object: Deliberate damage to feed mechanisms.	N/A
CPS2-CPS5: Physical Parts (Printed, Debound, Sintered, Finished)	Object: Counterfeit parts introduced into production chain. Instrument: Tampered parts could be used to falsely authenticate production source.	Object: Physical modification of parts between process steps. Object: Introduction of internal defects or weaknesses that evade detection.	Object: Removal or alteration of part identification markings/serial numbers.	Object: Physical theft of parts to obtain design information through reverse engineering. Object: Unauthorized measurements or scanning of parts.	Object: Physical damage to parts. Object: Contamination with materials that could cause downstream failures.	
PF1: Physical Inspection Flow	Object: Presenting different parts for inspection than those that were manufactured. Subject: Inspector could be impersonated by unauthorized personnel.	Object: Manipulation of physical inspection tools or gauges to incorrectly pass defective parts. Object: Tampering with part between manufacturing and inspection.	Subject: Inspector denying inspection was performed. Object: Removal or alteration of inspection stamps or markers.	Object: Unauthorized observation of inspection techniques could reveal proprietary quality control methods.	Object: Physical interference with inspection process. Object: Damage to inspection equipment.	Object: Unauthorized physical access to inspection area could allow an attacker to approve defective parts.
CPF3-CPF12: Material/Part Movement Flows	Object: Redirecting physical materials to incorrect machines through misleading labeling or handling instructions.	Object: Modifying physical parts during transfer between process steps. Object: Swapping genuine parts with counterfeits during transfers.	Subject: Denying responsibility for part handling errors. Object: Removal of handling logs or transfer records.	Object: Unauthorized observation of part transfers to gather manufacturing sequence information. Object: Visual or physical access to parts during transfer.	Object: Physical blockage of material transfer paths. Object: Creating unsafe conditions that halt transfers due to safety protocols.	Object: Unauthorized physical access to handling areas could allow bypassing of material control procedures.
CPF13: Material Flow from Supply Chain	Object: Accepting materials from fraudulent suppliers posing as legitimate vendors.	Object: Tampering with incoming materials during shipping or receiving. Object: Modifying material manifests or certifications.	Subject: Supplier denying sending defective materials. Object: Tampering with shipping records or chain of custody.	Object: Unauthorized access to proprietary material compositions during transit. Object: Interception of material specifications or order details.	Object: Blocking or delaying physical delivery of materials. Object: Damage to critical material supplies.	Object: Using compromised supply chain access to bypass material quality controls.
CPF14: Part Flow to Downstream Manufacturer	Object: Redirecting finished parts to unauthorized recipients through fraudulent shipping instructions.	Object: Tampering with parts during shipping or handling. Object: Swapping genuine parts with counterfeits during transit.	Subject: Denying shipping defective parts. Object: Tampering with shipping manifests or delivery confirmations.	Object: Unauthorized access to parts during transit for design information. Object: Interception of accompanying documentation revealing proprietary specifications.	Object: Blocking or delaying physical delivery of finished parts. Object: Damaging parts during transit.	N/A
CPF15: Operator Control Interactions	Subject: Spoofing operator identity through stolen badges or biometric workarounds. Object: Spoofed physical interfaces tricking operators into incorrect actions.	Object: Tampering with physical controls (buttons, switches) to cause incorrect operator inputs. Object: Altering physical feedback mechanisms (displays, indicators).	Subject: Operator denying initiating certain physical actions. Object: Disabling physical interaction logging systems.	Object: Unauthorized observation of operator actions to learn proprietary procedures. Object: Physical surveillance of authentication actions (shoulder surfing).	Object: Physical prevention of operator access to controls. Object: Creating hazardous conditions that prevent operator presence.	Object: Physical access to operator interfaces could allow execution of unauthorized commands.
CPO: Material Supply Chain Provider	Subject: Providing counterfeit materials with falsified certifications. Object: Supplier identity could be spoofed by competitors or malicious actors.	Subject: Deliberately altering material properties or specifications. Object: Supply chain systems could be tampered with to alter material specifications.	Subject: Denying knowledge of material defects or certification issues. Object: Tampering with supply chain records to hide responsibility.	Subject: Unauthorized collection of proprietary material usage patterns. Object: Intellectual property related to material specifications could be intercepted.	Subject: Deliberately delaying or blocking critical material deliveries. Object: Disruption of supplier operations could prevent material provision.	Subject: Exploiting trusted supplier relationship to introduce unauthorized materials or components into the manufacturing process.
CPI4: Critical Downstream Manufacturing	Subject: Falsely reporting part quality issues to gain access to manufacturing facilities or processes. Object: Downstream manufacturer identity could be spoofed to intercept parts.	Subject: Requesting unauthorized modifications to physical specifications. Object: Tampering with parts after delivery but claiming they were received damaged.	Subject: Denying receipt of parts or falsely claiming defects. Object: Tampering with receiving records to hide responsibility.	Subject: Using privileged position to gather proprietary manufacturing data. Object: Customer specifications could be intercepted.	Subject: Generating excessive emergency orders disrupting production. Object: Disruption of downstream operations could prevent part acceptance.	Subject: Using trusted customer relationship to gain unauthorized physical access to facility or processes.
CPP1: Part Printing Process	Object: Process could appear to be functioning correctly while actually using modified parameters through sensor spoofing.	Object: Physical tampering with print environment (temperature, humidity). Object: Tampering with physical layer registration or alignment.	Object: Alteration of process logs to hide evidence of abnormal printing conditions.	Object: Physical monitoring of printing process for reverse engineering. Object: Acoustic or EM emissions could reveal printing patterns.	Object: Introduction of environmental contaminants disrupting layer adhesion. Object: Creating physical conditions that trigger safety shutdowns.	Object: Exploitation of physical process controls to override safety limits.
CPP2: Part Debinding Process	Object: Process monitoring could be spoofed to indicate proper debinding while incomplete.	Object: Tampering with physical environmental conditions affecting chemical reactions. Object: Altering solvent compositions or gas mixtures.	Object: Manipulation of process records to hide improper debinding conditions.	Object: Monitoring of process parameters to derive proprietary debinding techniques.	Object: Contamination of debinding media. Object: Disruption of ventilation or chemical containment systems.	Object: Unauthorized manipulation of safety-critical physical parameters through process access.
CPP3: Part Sintering Process	Object: Temperature or atmosphere monitoring could be spoofed to indicate proper sintering while improper.	Object: Manipulation of physical sintering environment (gases, pressure, temperature gradients). Object: Tampering with cooling rates to induce internal stresses.	Object: Alteration of thermal records to hide improper sintering conditions.	Object: Thermal imaging to capture proprietary sintering profiles. Object: Monitoring gas consumption to derive process details.	Object: Introduction of contaminants that disrupt sintering reactions. Object: Creating thermal conditions that trigger emergency shutdowns.	Object: Bypassing physical thermal interlocks to run unauthorized sintering profiles.
CPP4: Quality Control Process	Object: QC equipment could be manipulated to show false positive inspection results.	Object: Tampering with physical test specimens. Object: Manipulation of physical calibration standards.	Object: Falsification of physical inspection records. Object: Removal of physical defect indicators.	Object: Observation of QC methods to learn acceptance criteria. Object: Unauthorized access to physical test results.	Object: Damaging or miscalibrating test equipment. Object: Creating conditions that prevent proper inspection.	Object: Unauthorized access to quality control areas to approve defective parts.

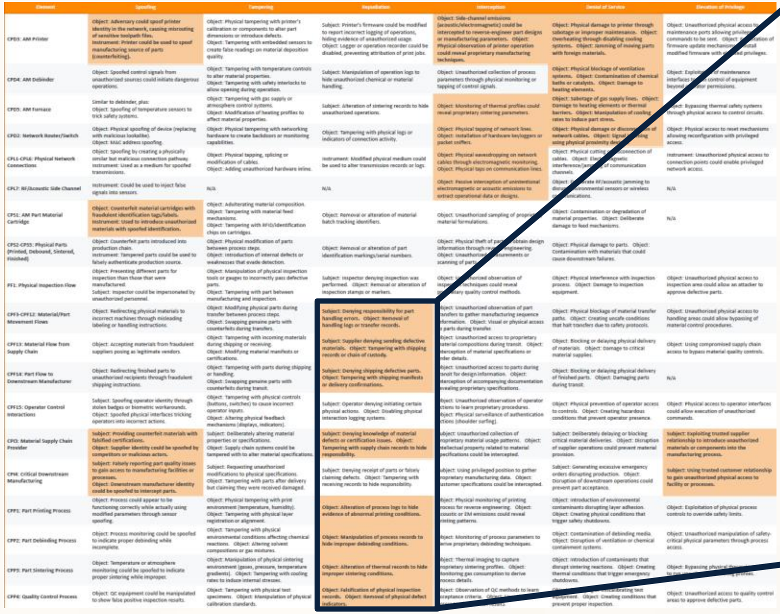


Element	Interception	Denial of Service
CPD3: AM Printer	Object: Side-channel emissions (acoustic/electromagnetic) could be intercepted to reverse-engineer part designs or manufacturing parameters. Object: Physical observation of printer operation could reveal proprietary manufacturing techniques.	Object: Physical damage to printer through sabotage or improper maintenance. Object: Overheating through disabling cooling systems. Object: Jamming of moving parts with foreign materials.
CPD4: AM Debinder	Object: Unauthorized collection of process parameters through physical monitoring or tapping of control signals.	Object: Physical blockage of ventilation systems. Object: Contamination of chemical baths or catalysts. Object: Damage to heating elements.
CPD5: AM Furnace	Object: Monitoring of thermal profiles could reveal proprietary sintering parameters.	Object: Sabotage of gas supply lines. Object: Damage to heating elements or thermal barriers. Object: Manipulation of cooling rates to induce part stress.
CPD2: Network Router/Switch	Object: Physical tapping of network lines. Object: Installation of hardware keyloggers or packet sniffers.	Object: Physical damage or disconnection of network cables. Object: Signal jamming using physical proximity devices.
CPL1-CPL6: Physical Network Connections	Object: Physical eavesdropping on network cables through electromagnetic monitoring. Object: Physical taps on communication lines.	Object: Physical cutting or disconnection of cables. Object: Electromagnetic interference/jamming of communication channels.
CPL7: RF/Acoustic Side Channel	Object: Passive interception of unintentional electromagnetic or acoustic emissions to extract operational data or designs.	Object: Deliberate RF/acoustic jamming to disrupt environmental sensors or wireless communications.

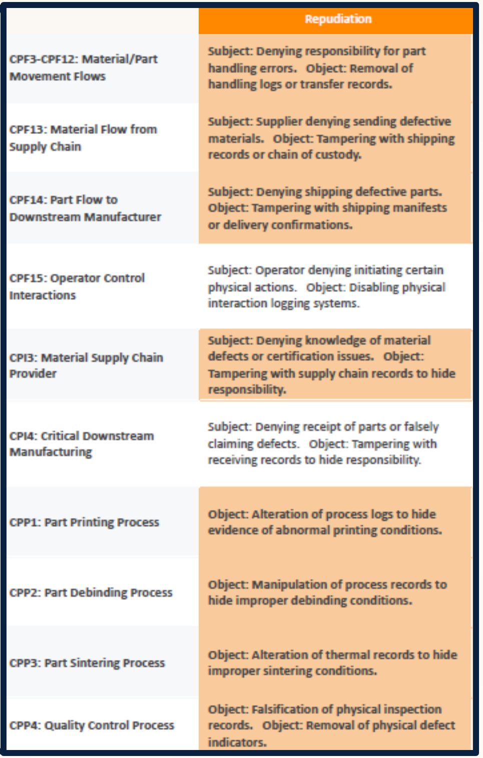
LLM-assisted comparative threat modeling for AM CPS

- Claude 3.7 Sonnet assumes role of subject matter expert.
- Orange Highlights: Physical & cyber-physical threats

S T R I D E



Element	Spoofing	Tampering	Repudiation	Interception	Denial of Service	Elevation of Privilege
CPD3: AM Printer	Object: Adversary could spoof printer identity in the network, causing misrouting of sensitive toolpath files. Instrument: Printer could be used to spoof manufacturing source of parts (counterfeiting).	Object: Physical tampering with printer's calibration or components to alter part dimensions or introduce defects. Object: Tampering with embedded sensors to create false readings on material deposition quality.	Subject: Printer's firmware could be modified to report incorrect logging of operations, hiding evidence of unauthorized usage. Object: Logger or operation recorder could be disabled, preventing attribution of print jobs.	Object: Side-channel emissions (acoustic/electromagnetic) could be intercepted to reverse-engineer part designs or manufacturing parameters. Object: Physical observation of printer operation could reveal proprietary manufacturing techniques.	Object: Physical damage to printer through sabotage or improper maintenance. Object: Overheating through disabling cooling systems. Object: Jamming of moving parts with foreign materials.	Object: Unauthorized physical access to maintenance ports allowing privileged commands to be sent. Object: Exploitation of firmware update mechanisms to install modified firmware with elevated privileges.
CPD4: AM Debinder	Object: Spoofed control signals from unauthorized sources could initiate dangerous operations.	Object: Tampering with temperature controls to alter material properties. Object: Tampering with safety interlocks to allow opening during operation.	Subject: Manipulation of operation logs to hide unauthorized chemical or material handling.	Object: Unauthorized collection of process parameters through physical monitoring or tapping of control signals.	Object: Physical blockage of ventilation systems. Object: Contamination of chemical baths or catalysts. Object: Damage to heating elements.	Object: Exploitation of maintenance interfaces to gain control of equipment beyond operator permissions.
CPD5: AM Furnace	Similar to debinder, plus: Object: Spoofing of temperature sensors to trick safety systems.	Object: Tampering with gas supply or atmosphere control systems. Object: Modification of heating profiles to affect material properties.	Subject: Alteration of sintering records to hide unauthorized operations.	Object: Monitoring of thermal profiles could reveal proprietary sintering parameters.	Object: Sabotage of gas supply lines. Object: Damage to heating elements or thermal barriers. Object: Manipulation of cooling rates to induce part stress.	Object: Bypassing thermal safety systems through physical access to control circuits.
CPD2: Network Router/Switch	Object: Physical spoofing of device (replacing with malicious lookalike). Object: MAC address spoofing.	Object: Physical tampering with networking hardware to create backdoors or monitoring capabilities.	Object: Tampering with physical logs or indicators of connection activity.	Object: Physical tapping of network lines. Object: Installation of hardware keyloggers or packet sniffers.	Object: Physical damage or disconnection of network cables. Object: Signal jamming using physical proximity devices.	Object: Physical access to reset mechanisms allowing reconfiguration with privileged access.
CPL1-CPL6: Physical Network Connections	Object: Spoofing by creating a physically similar but malicious connection pathway. Instrument: Used as a medium for spoofed transmissions.	Object: Physical tapping, splicing or modification of cables. Object: Adding unauthorized hardware inline.	Instrument: Modified physical medium could be used to alter transmission records or logs.	Object: Physical eavesdropping on network cables through electromagnetic monitoring. Object: Physical taps on communication lines.	Object: Physical cutting or disconnection of cables. Object: Electromagnetic interference/jamming of communication channels.	Instrument: Unauthorized physical access to connection points could enable privileged network access.
CPL7: RF/Acoustic Side Channel	Instrument: Could be used to inject false signals into sensors.	N/A	N/A	Object: Passive interception of unintentional electromagnetic or acoustic emissions to extract operational data or designs.	Object: Deliberate RF/acoustic jamming to disrupt environmental sensors or wireless communications.	N/A
CPS1: AM Part Material Cartridge	Object: Counterfeit material cartridges with fraudulent identification tags/labels. Instrument: Used to introduce unauthorized materials with spoofed identification.	Object: Adulterating material composition. Object: Tampering with material feed mechanisms. Object: Tampering with RFID/identification chips on cartridges.	Object: Removal or alteration of material batch tracking identifiers.	Object: Unauthorized sampling of proprietary material formulations.	Object: Contamination or degradation of material properties. Object: Deliberate damage to feed mechanisms.	N/A
CPS2-CPS5: Physical Parts (Printed, Debound, Sintered, Finished)	Object: Counterfeit parts introduced into production chain. Instrument: Tampered parts could be used to falsely authenticate production source.	Object: Physical modification of parts between process steps. Object: Introduction of internal defects or weaknesses that evade detection.	Object: Removal or alteration of part identification markings/serial numbers.	Object: Physical theft of parts to obtain design information through reverse engineering. Object: Unauthorized measurements or scanning of parts.	Object: Physical damage to parts. Object: Contamination with materials that could cause downstream failures.	
PF1: Physical Inspection Flow	Object: Presenting different parts for inspection than those that were manufactured. Subject: Inspector could be impersonated by unauthorized personnel.	Object: Manipulation of physical inspection tools or gauges to incorrectly pass defective parts. Object: Tampering with part between manufacturing and inspection.	Subject: Inspector denying inspection was performed. Object: Removal or alteration of inspection stamps or markers.	Object: Unauthorized observation of inspection techniques could reveal proprietary quality control methods.	Object: Physical interference with inspection process. Object: Damage to inspection equipment.	Object: Unauthorized physical access to inspection area could allow an attacker to approve defective parts.
CPF3-CPF12: Material/Part Movement Flows	Object: Redirecting physical materials to incorrect machines through misleading labeling or handling instructions.	Object: Modifying physical parts during transfer between process steps. Object: Swapping genuine parts with counterfeits during transfers.	Subject: Denying responsibility for part handling errors. Object: Removal of handling logs or transfer records.	Object: Unauthorized observation of part transfers to gather manufacturing sequence information. Object: Visual or physical access to parts during transfer.	Object: Physical blockage of material transfer paths. Object: Creating unsafe conditions that halt transfers due to safety protocols.	Object: Unauthorized physical access to handling areas could allow bypassing of material control procedures.
CPF13: Material Flow from Supply Chain	Object: Accepting materials from fraudulent suppliers posing as legitimate vendors.	Object: Tampering with incoming materials during shipping or receiving. Object: Modifying material manifests or certifications.	Subject: Supplier denying sending defective materials. Object: Tampering with shipping records or chain of custody.	Object: Unauthorized access to proprietary material compositions during transit. Object: Interception of material specifications or order details.	Object: Blocking or delaying physical delivery of materials. Object: Damage to critical material supplies.	Object: Using compromised supply chain access to bypass material quality controls.
CPF14: Part Flow to Downstream Manufacturer	Object: Redirecting finished parts to unauthorized recipients through fraudulent shipping instructions.	Object: Tampering with parts during shipping or handling. Object: Swapping genuine parts with counterfeits during transit.	Subject: Denying shipping defective parts. Object: Tampering with shipping manifests or delivery confirmations.	Object: Unauthorized access to parts during transit for design information. Object: Interception of accompanying documentation revealing proprietary specifications.	Object: Blocking or delaying physical delivery of finished parts. Object: Damaging parts during transit.	N/A
CPF15: Operator Control Interactions	Subject: Spoofing operator identity through stolen badges or biometric workarounds. Object: Spoofed physical interfaces tricking operators into incorrect actions.	Object: Tampering with physical controls (buttons, switches) to cause incorrect operator inputs. Object: Altering physical feedback mechanisms (displays, indicators).	Subject: Operator denying initiating certain physical actions. Object: Disabling physical interaction logging systems.	Object: Unauthorized observation of operator actions to learn proprietary procedures. Object: Physical surveillance of authentication actions (shoulder surfing).	Object: Physical prevention of operator access to controls. Object: Creating hazardous conditions that prevent operator presence.	Object: Physical access to operator interfaces could allow execution of unauthorized commands.
CPI3: Material Supply Chain Provider	Subject: Providing counterfeit materials with falsified certifications. Object: Supplier identity could be spoofed by competitors or malicious actors.	Subject: Deliberately altering material properties or specifications. Object: Supply chain systems could be tampered with to alter material specifications.	Subject: Denying knowledge of material defects or certification issues. Object: Tampering with supply chain records to hide responsibility.	Subject: Unauthorized collection of proprietary material usage patterns. Object: Intellectual property related to material specifications could be intercepted.	Subject: Deliberately delaying or blocking critical material deliveries. Object: Disruption of supplier operations could prevent material provision.	Subject: Exploiting trusted supplier relationship to introduce unauthorized materials or components into the manufacturing process.
CPI4: Critical Downstream Manufacturing	Subject: Falsely reporting part quality issues to gain access to manufacturing facilities or processes. Object: Downstream manufacturer identity could be spoofed to intercept parts.	Subject: Requesting unauthorized modifications to physical specifications. Object: Tampering with parts after delivery but claiming they were received damaged.	Subject: Denying receipt of parts or falsely claiming defects. Object: Tampering with receiving records to hide responsibility.	Subject: Using privileged position to gather proprietary manufacturing data. Object: Customer specifications could be intercepted.	Subject: Generating excessive emergency orders disrupting production. Object: Disruption of downstream operations could prevent part acceptance.	Subject: Using trusted customer relationship to gain unauthorized physical access to facility or processes.
CPP1: Part Printing Process	Object: Process could appear to be functioning correctly while actually using modified parameters through sensor spoofing.	Object: Physical tampering with print environment (temperature, humidity). Object: Tampering with physical layer registration or alignment.	Object: Alteration of process logs to hide evidence of abnormal printing conditions.	Object: Physical monitoring of printing process for reverse engineering. Object: Acoustic or EM emissions could reveal printing patterns.	Object: Introduction of environmental contaminants disrupting layer adhesion. Object: Creating physical conditions that trigger safety shutdowns.	Object: Exploitation of physical process controls to override safety limits.
CPP2: Part Debinding Process	Object: Process monitoring could be spoofed to indicate proper debinding while incomplete.	Object: Tampering with physical environmental conditions affecting chemical reactions. Object: Altering solvent compositions or gas mixtures.	Object: Manipulation of process records to hide improper debinding conditions.	Object: Monitoring of process parameters to derive proprietary debinding techniques.	Object: Contamination of debinding media. Object: Disruption of ventilation or chemical containment systems.	Object: Unauthorized manipulation of safety-critical physical parameters through process access.
CPP3: Part Sintering Process	Object: Temperature or atmosphere monitoring could be spoofed to indicate proper sintering while improper.	Object: Manipulation of physical sintering environment (gases, pressure, temperature gradients). Object: Tampering with cooling rates to induce internal stresses.	Object: Alteration of thermal records to hide improper sintering conditions.	Object: Thermal imaging to capture proprietary sintering profiles. Object: Monitoring gas consumption to derive process details.	Object: Introduction of contaminants that disrupt sintering reactions. Object: Creating thermal conditions that trigger emergency shutdowns.	Object: Bypassing physical [illegible] to gain [illegible] profiles.
CPP4: Quality Control Process	Object: QC equipment could be manipulated to show false positive inspection results.	Object: Tampering with physical test specimens. Object: Manipulation of physical calibration standards.	Object: Falsification of physical inspection records. Object: Removal of physical defect indicators.	Object: Observation of QC methods to learn acceptance criteria. Object: [illegible] results.	Object: [illegible] miscalibrating test equipment. Object: Creating conditions that prevent proper inspection.	Object: Unauthorized access to quality control areas to approve defective parts.



	Repudiation
CPF3-CPF12: Material/Part Movement Flows	Subject: Denying responsibility for part handling errors. Object: Removal of handling logs or transfer records.
CPF13: Material Flow from Supply Chain	Subject: Supplier denying sending defective materials. Object: Tampering with shipping records or chain of custody.
CPF14: Part Flow to Downstream Manufacturer	Subject: Denying shipping defective parts. Object: Tampering with shipping manifests or delivery confirmations.
CPF15: Operator Control Interactions	Subject: Operator denying initiating certain physical actions. Object: Disabling physical interaction logging systems.
CPI3: Material Supply Chain Provider	Subject: Denying knowledge of material defects or certification issues. Object: Tampering with supply chain records to hide responsibility.
CPI4: Critical Downstream Manufacturing	Subject: Denying receipt of parts or falsely claiming defects. Object: Tampering with receiving records to hide responsibility.
CPP1: Part Printing Process	Object: Alteration of process logs to hide evidence of abnormal printing conditions.
CPP2: Part Debinding Process	Object: Manipulation of process records to hide improper debinding conditions.
CPP3: Part Sintering Process	Object: Alteration of thermal records to hide improper sintering conditions.
CPP4: Quality Control Process	Object: Falsification of physical inspection records. Object: Removal of physical defect indicators.

Discussion: CPSTRIDE Advantages

- Allows explicit modeling of physical & cyber-physical entities, e.g., material and energy flows, hybrid security measures, geographic proximity, humans
- Allows differentiation of Links from Flows, Processes from Devices
- Facilitates modeling the physical effects of cyber-attacks
- Invites the use of LLMs to augment human expertise

Discussion: CPSTRIDE Limitations & Challenges

- More complex & time-intensive than STRIDE
- Ambiguity of broadened threat susceptibility for elements
- Abstract conceptual threats vs. cyber-physical databases
- Technological costs of physical vs. digital threat scanning
- Dangers of overreliance on AI / LLMs

Discussion: Future Work

- Application of CPSTRIDE to other CPS domains.
  In development: CPSTRIDE for Water CI and UAS threats

- Development of automated tools leveraging AI & LLMs

- Integration with existing security frameworks & standards

    NIST Cybersecurity Framework

    IEC62443

    ISO/IEC 27001

Slutsats (Conclusion)

Q&A

Contact
dallas-elleman@utulsa.edu
QR: https://www.linkedin.com/in/dallas-elleman

Cyber Fellows

THE UNIVERSITY OF TULSA