Hacking the Factory Floor

Cybersecurity in Advanced Manufacturing Systems

Satyajit (Jit) Mojumder, PhD
Assistant Professor,
School of Mechanical and Materials Engineering
Washington State University, Pullman, WA
Website: https://labs.wsu.edu/cimpi/

What We Will Cover Today

- **I** Advanced Manufacturing Primer
- **II** Additive Manufacturing: Deep Dive
- **III** Other Advanced Manufacturing Domains
- **IV** Defensive Frameworks & Mitigations
- **V** Research Frontiers

Learning Objectives: *Understand the attack surface of modern manufacturing · Analyze AM-specific vulnerabilities · Evaluate mitigation frameworks*

Section I

Advanced Manufacturing Primer

- ***Industry 4.0***
- ***OT/IT Convergence***
- ***Cyber-Physical Risk***

Image source: Goodwin University

From Traditional to Advanced Manufacturing

Advanced manufacturing integrates traditional production with digital intelligence.

Traditional Manufacturing

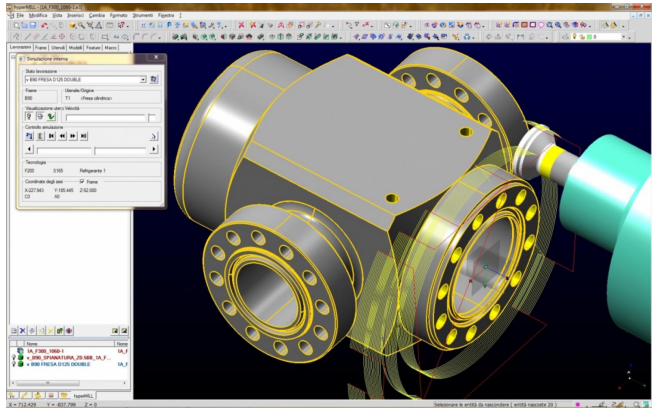
Mostly mechanical and local

- Standalone machines
- Manual setup and inspection
- Limited data collection
- Local operator control

Advanced Manufacturing

Software-defined and connected

- CAD/CAM connects design to production
- Industry 4.0 paradigm: Machine, sensors, and controllers communicate
- Key enabling technologies: Industrial IoT (IIoT), cloud manufacturing, digital twins, AI/ML-driven quality control



Key Paradigm Shift: Machines are no longer isolated — they are networked nodes with IP addresses, APIs, and software update mechanisms.

Convergence of OT and IT

Before Industry 4.0

Information Technology (IT) Network

Email ERP Databases Internet

Operational Technology (OT) Network

PLC SCADA Sensors Machines

Now Industry 4.0

Information Technology (IT) Network

ERP MES Cloud Analytics

Convergence Zone

Remote access Data historian IIoT gateway
OPC-UA/MQTT

Operational Technology (OT) Network

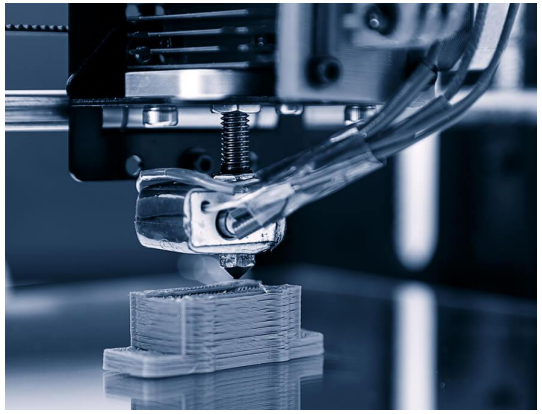
PLCs SCADA/HMI Robots/CNC Sensors/Actuators Machines

Compromised IT account → OT access path

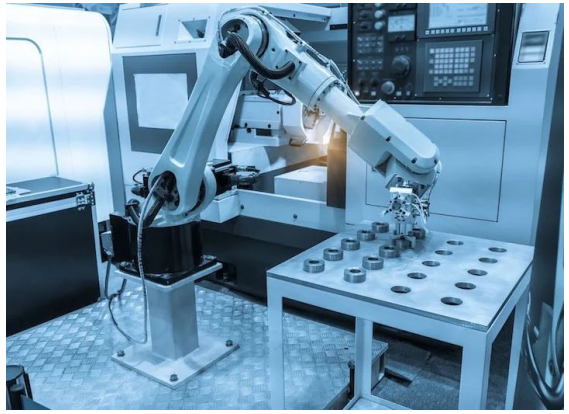
⚠️ **Critical Insight: When OT meets IT, cyber events gain physical, safety, and economic consequences far beyond data breaches.**

Advanced Manufacturing Technology Landscape

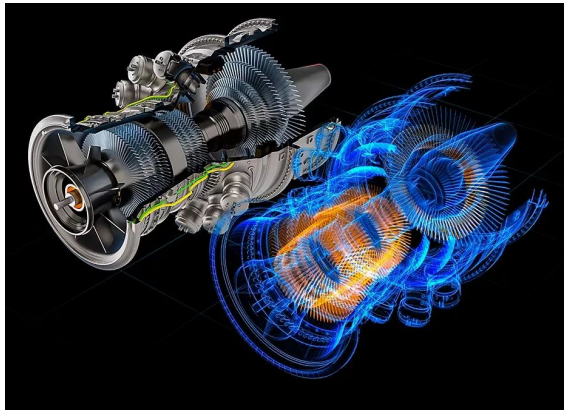
From 3D printers to robot arms, modern production systems are increasingly software-defined and networked.



Additive Manufacturing



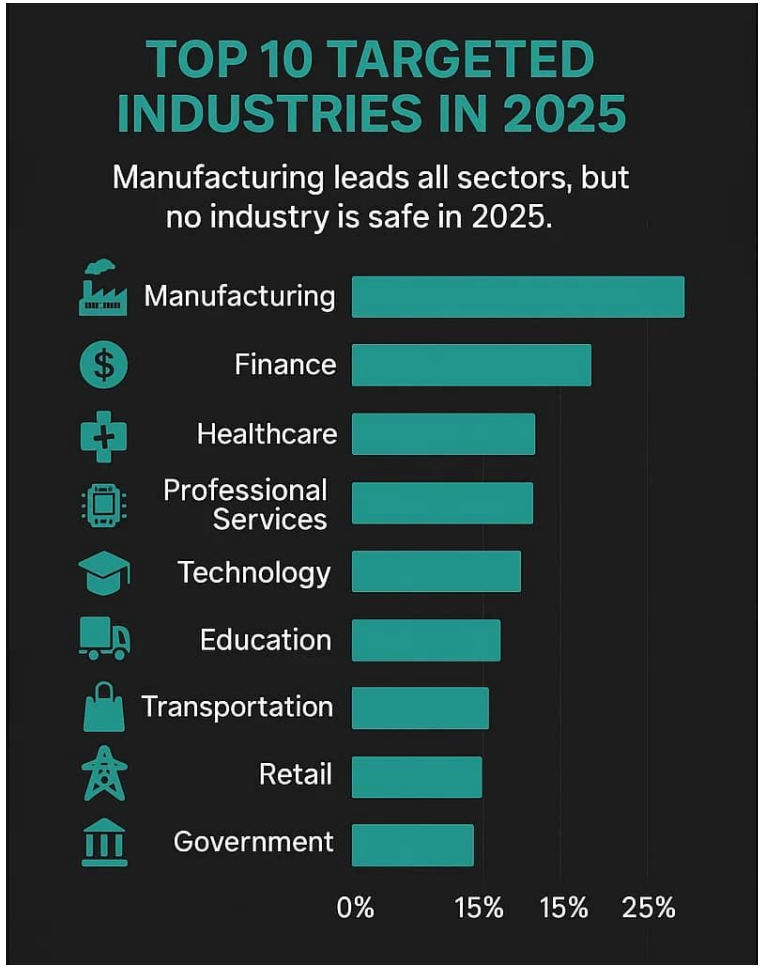
CNC Machining & Robotics



Digital Twins

Smart Factories & IIoT

The Stakes: Real-World Impact



From steel to semiconductors, manufacturing disruptions are costly and frequent.

Unimicron

Ransomware attack in 2025 disrupted operations in Taiwan

NUCOR

Ransomware attack in 2025 halted steel production

https://deepstrike.io/blog/top-industries-targeted-by-hackers-2025

Section II

Additive Manufacturing (AM) Deep Dive on Attack Surfaces

- ***How AM works***
- ***Digital design files***
- ***AM cyber-physical attack surface***
- ***Threat analysis for AM***
- ***Quality assurance***

Courtesy: 3D Native

https://www.youtube.com/shorts/aivO0mVgW0s?feature=share

Exploring the additive manufacturing landscape across various material systems

Additive Manufacturing Processes

Plastic, metal, wax

Droplets of materials are selectively deposited

Material Jetting

Plastic, metal, composite

Material Extrusion

Material is selectively dispensed through a nozzle or orifice

Plastic

Liquid photopolymer in a vat is cured by light-activated polymerization

VAT Photo polymerization

composite

Sheet Lamination

Sheet of materials are bonded to form a part

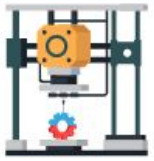
Plastic, metal

Powder Bed Fusion

Thermal energy to melt regions of a powder bed

Gypsum, sand metal

Liquid bonding agent is selectively deposited to join powder materials



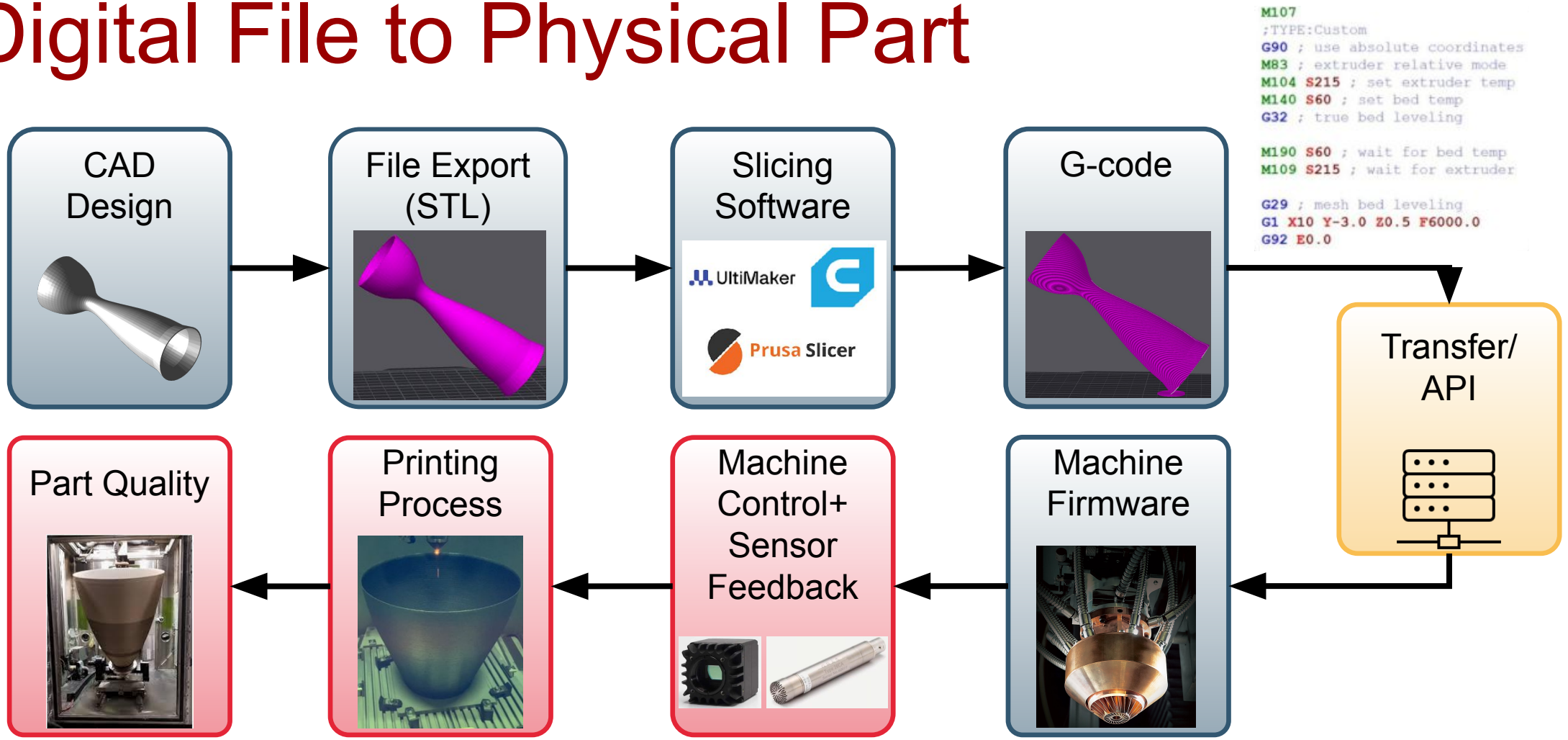
Binder Jetting

metal

Directed Energy Deposition

Thermal energy used to melt materials as they are deposited

How Additive Manufacturing Works: From Digital File to Physical Part



Each stage is a potential attack surface

AM Cyber-Physical Attack Surface

Software Layer

Design and control logic

- CAD/CAM and slicer software
- G-code generation and repository access
- Firmware and software vulnerabilities

Example: A malicious design STL file creates a hidden structural flaw.

Network Layer

Communication and remote access

- Cloud repositories and printer web interfaces
- Remote monitoring APIs
- Insecure industrial protocols

Example: An attacker bypasses the slicer and sends malicious G-code directly to the printer.

Physical Layer

Machine, material, and sensing environment

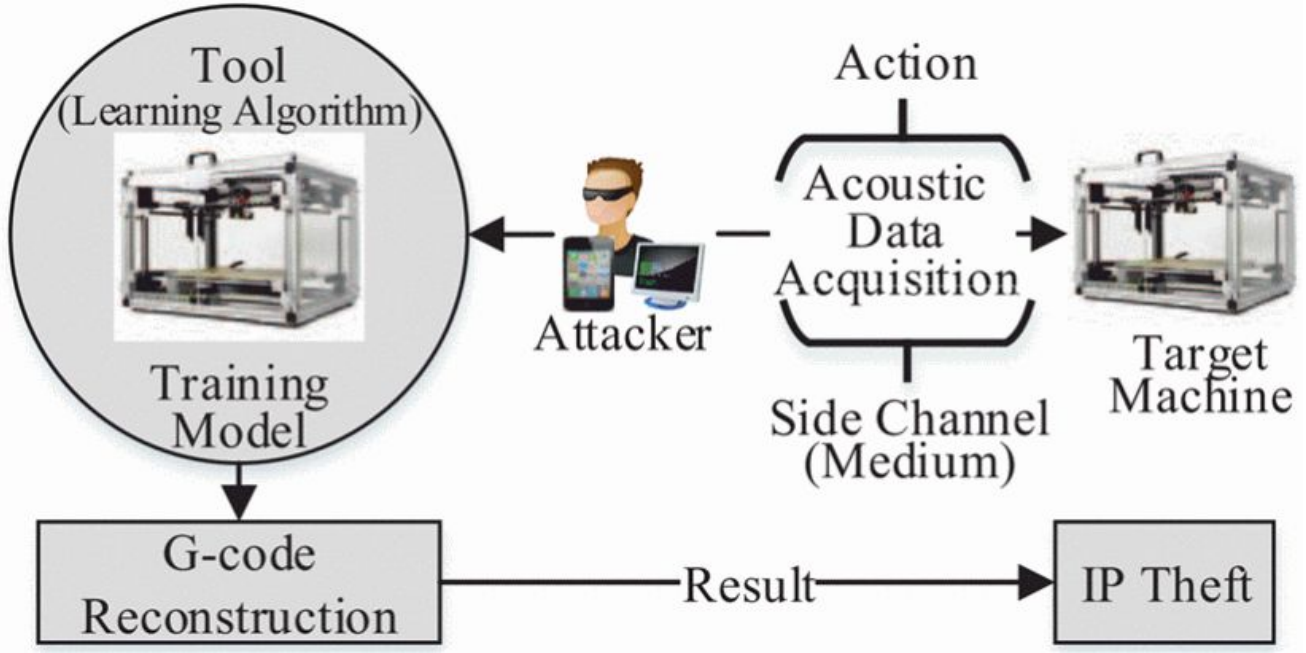
- Material integrity and print queue access
- Sensor manipulation
- Acoustic and power side channels

Example: A microphone near the printer infers the geometry of the part being printed.

Threat I : IP Theft and Design Leakage

In additive manufacturing, stealing the file may be enough to steal the product.

- Design files are high-value manufacturing assets
- A stolen CAD/STL file can enable physical reproduction
- Attack vectors: compromise of CAD workstations, cloud repository exfiltration, insider threat, supply chain partner access
- Side channels may leak geometry without network access

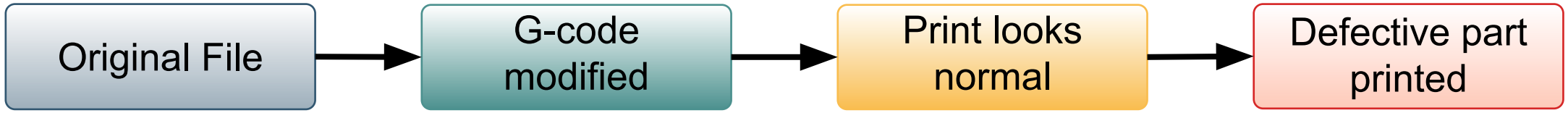


Acoustic side-channel attack on an FDM printer
Faruque et al., CCS 2016

Key insight: Unlike software IP theft (stealing source code), AM IP theft directly enables physical reproduction — no reverse engineering needed.

Threat II : Hidden Defects Injection

The part can look correct outside but be weakened inside.



- Internal infill or lattice pattern
- Layer bonding conditions
- Wall thickness or internal geometry
- Support structures and tolerances

- Covertly modified G-code for a drone propeller
- Reduced internal infill density by 20%
- Part passed visual inspection
- Propeller failed catastrophically mid-flight
- No external indication of tampering

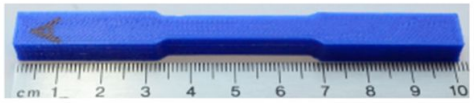


Figure 4: Example control group test specimen.

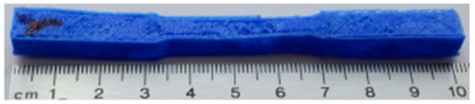
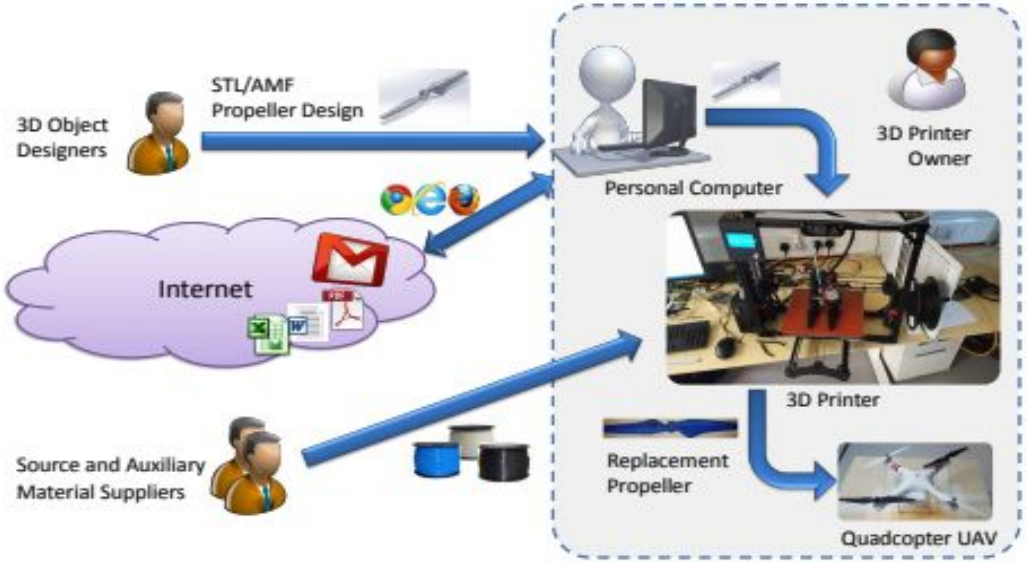


Figure 5: Example 50% material reduction.

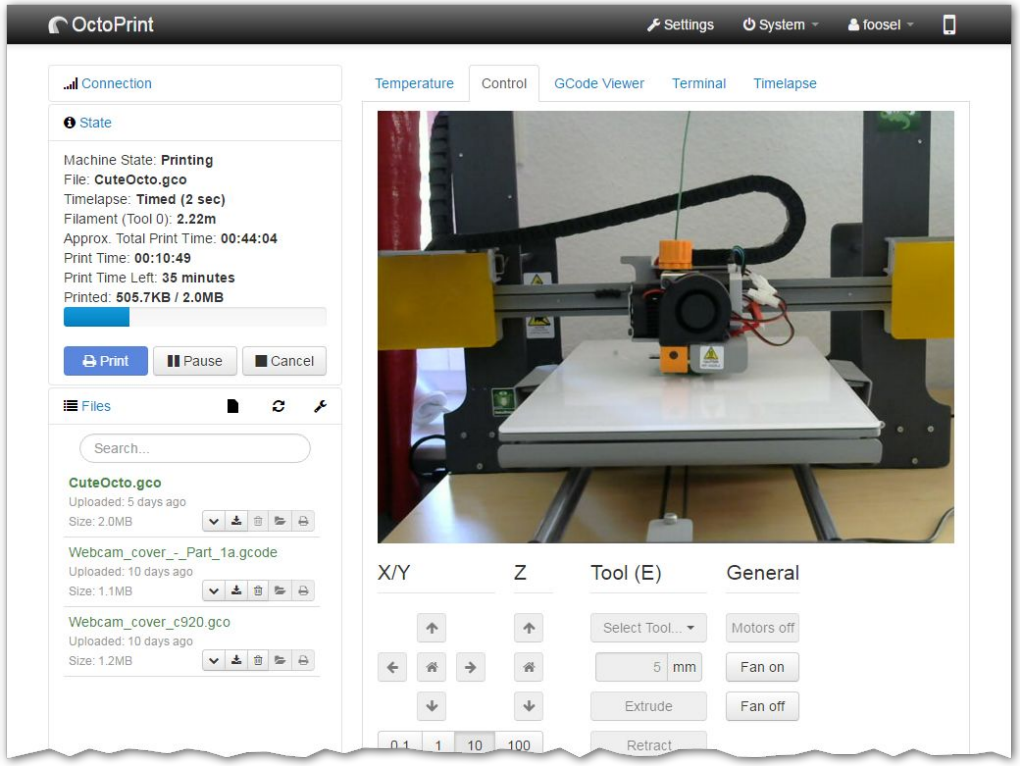


"dr0wned"- Cyber-Physical Attack with Additive Manufacturing, *Belikovetsky et al., 2017*

Threat III : Firmware and Embedded Systems Attacks

When attackers reach firmware, digital commands can become physical consequences.

- Firmware (Marlin/Klipper) controls all physical functions (motors, heaters, fans)
- Compromise grants full physical device control, surviving resets and power cycles
- Attack vectors: insecure OTA updates, exposed USB/UART, unauthenticated web UIs
- Temperature override risk → PTFE combustion and fire hazard
- Thousands of OctoPrint instances publicly exposed via Shodan with default credentials

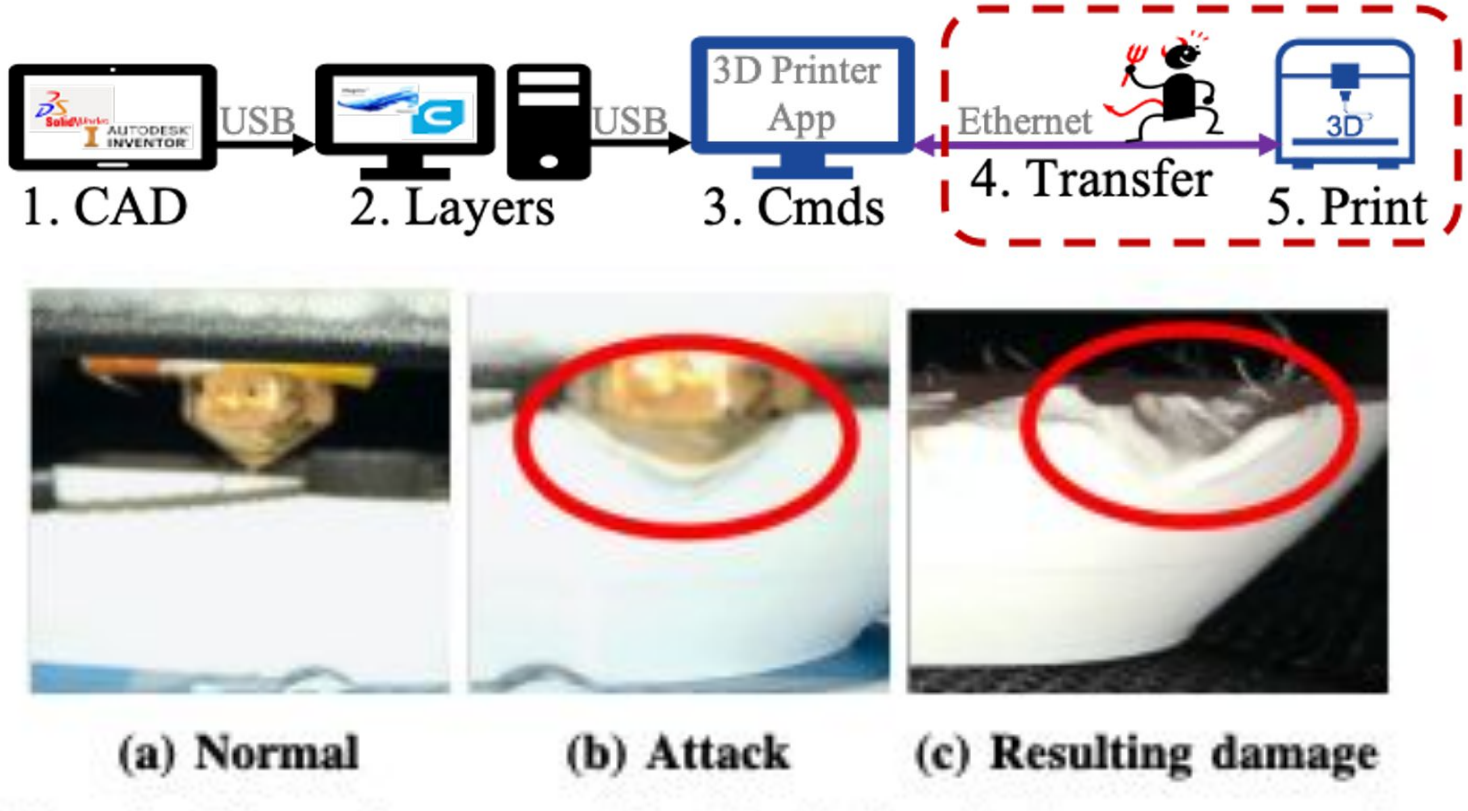


Attack consequence: firmware compromise = complete physical control of the printer

Threat IV : Network-Level Attacks

Network exposure can turn print-job transfer into physical machine control.

- Unencrypted print-job transfer
- Weak or missing authentication
- Exposed printer web interfaces
- Misconfigured industrial protocols



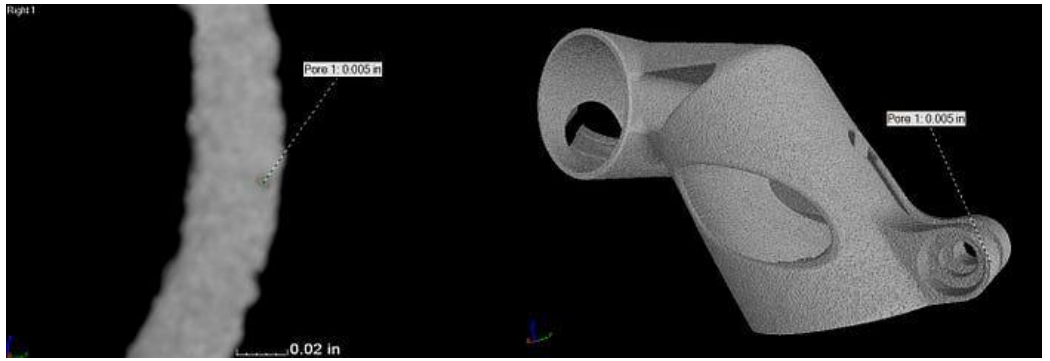
Security Analysis of Networked 3D Printers
McCormack et al., 2020

Quality Assurance as a Security Control

Detection becomes part of defense when cyberattacks change physical parts.

QA method	Limitation
Visual inspection	Cannot see internal defects
Dimensional inspection	Checks outside shape, not internal strength
CT scanning	Detects internal defects, but costly and slow
Ultrasonic testing	Useful, but geometry-dependent
Destructive testing	Strong evidence, but destroys the part

Key question
Can a compromised part look correct, pass basic checks, and still fail in use?



CIMP-3D, 2015

Source: xometry.com

Source: protolabs.com

Research Direction: In-situ process monitoring — ML anomaly detection on acoustic, thermal, and optical signals during printing, enabling real-time defect detection.

Securing the AM Workflow: Trust the File Before Print

The printer should verify both the file and the person who approved it.

- Print-job tampering during transfer
- Unauthorized file or G-code injection
- Untracked design changes before production

Defensive Mechanisms for AM

- **SHA-256 hashing** of STL/G-code at each pipeline stage detects any tampering
- **PKI signatures** printer verifies designer's signature before accepting a job
- **Design provenance chains** cryptographic log of every design modification (who, when, what)
- **Blockchain tracking** immutable custody record; emerging research area
- **HSMs** secure key storage, prevents exfiltration if workstation is compromised
- **Multi-party authorization** safety-critical jobs require approval before printing

Threat Modeling the AM Pipeline: STRIDE

A familiar CS framework applied to a cyber-physical manufacturing workflow.

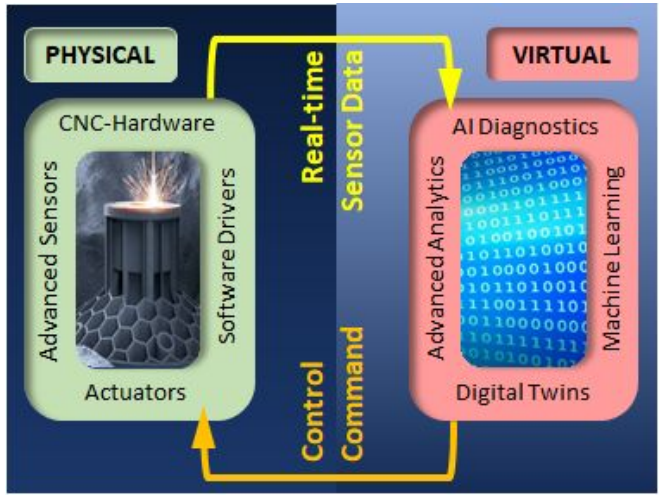
STRIDE	**AM example**
S — Spoofing	Fake designer submits a print job
T — Tampering	G-code modified before printing
R — Repudiation	No audit trail for who changed the file
I — Information Disclosure	CAD files or side-channel data leak part geometry
D — Denial of Service	Print queue locked, flooded, or disrupted
E — Elevation of Privilege	Slicer exploit gives access to CAD or printer systems

STRIDE mapping adapted from **Microsoft** threat modeling and AM security categorization in *Venkata et al., 2020.*

Section III

Beyond AM: Other Advanced Manufacturing Domains

- ❑ *CNC Machines*
- ❑ *Robotics*
- ❑ *Digital Twins*
- ❑ *IIoT Systems*



CNC Machining and Industrial Robotics

CNC Machining:

- Use toolpaths and G-code to control cutting motion
- Malicious commands can damage the part, tool, or machine
- CAM/controller systems may be connected to shop-floor networks

Source: omni-cnc.com

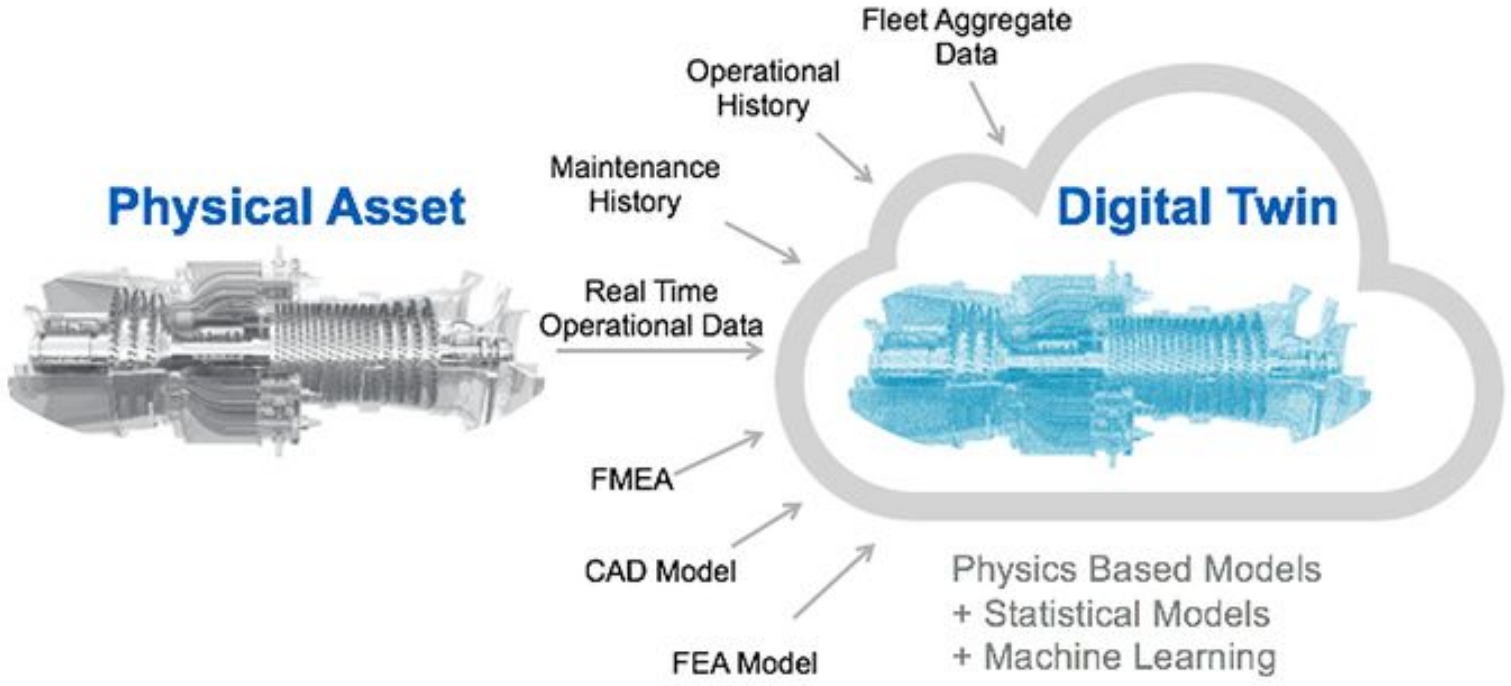
Industrial Robotics:

- Use software commands to control motion, speed, and safety zones
- Weak authentication can expose robot control interfaces
- A compromised robot creates physical safety and production risks

Source: ansi.org

Digital Twins: Virtual Replicas, Real Vulnerabilities

- False sensor data can mislead the virtual model
- A compromised twin can hide real process problems
- The twin can reveal sensitive process knowledge, including human workers
- Feedback loop exploitation
- Twin-physical synchronization attacks



A digital twin is only as trustworthy as the data feeding it.

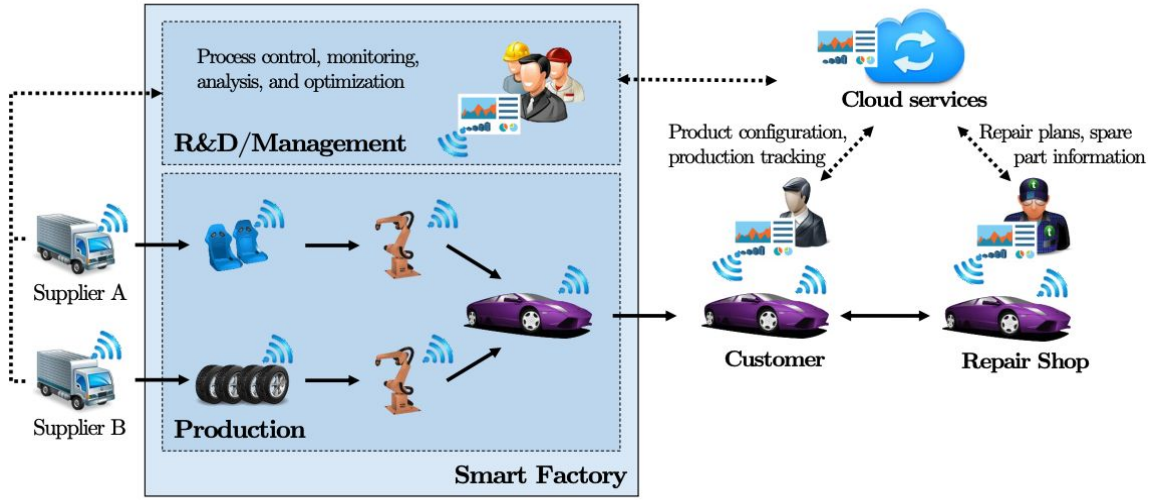
Security and Privacy of Digital Twins for Advanced Manufacturing: A Survey, *Zemskov et al., 2024*

Smart Factories and IIoT Security

Smart manufacturing depends on connected devices, but every connection expands the attack surface.

- Sensors, cameras, robots, gateways, and edge devices continuously send production data
- Weak authentication or unpatched firmware can expose factory systems
- If the network is flat, one compromised device can help attackers move toward PLCs, HMIs, or production databases

Source: cyngn.com



Security and Privacy Challenges in Industrial Internet of Things
Sadeghi et al., 2015

Cross-Domain Threat Comparison

Domain	Primary Attack Surface	Key Threat Scenario	Consequence	Detectability
Additive Manufacturing	G-code, firmware, repos	Covert part sabotage, IP theft	Critical	Very Low
CNC Machining	G-code, CAM software	Machine crash, toolpath exploit	High	Low
Industrial Robotics	ROS, proprietary APIs	Physical harm, process disruption	High	Low
Digital Twins	Sensor feeds, data APIs	Decision poisoning, espionage	High	Medium
Smart Factory / IIoT	Device firmware, protocols	Lateral movement, DoS	High	Medium
Supply Chain / ERP	APIs, RFID, ERP systems	Counterfeit parts, production halt	Critical	Medium

Section IV

Defensive Frameworks and Mitigations

- ❑ *Standards*
- ❑ *Frameworks*
- ❑ *Cryptography*
- ❑ *Detection*

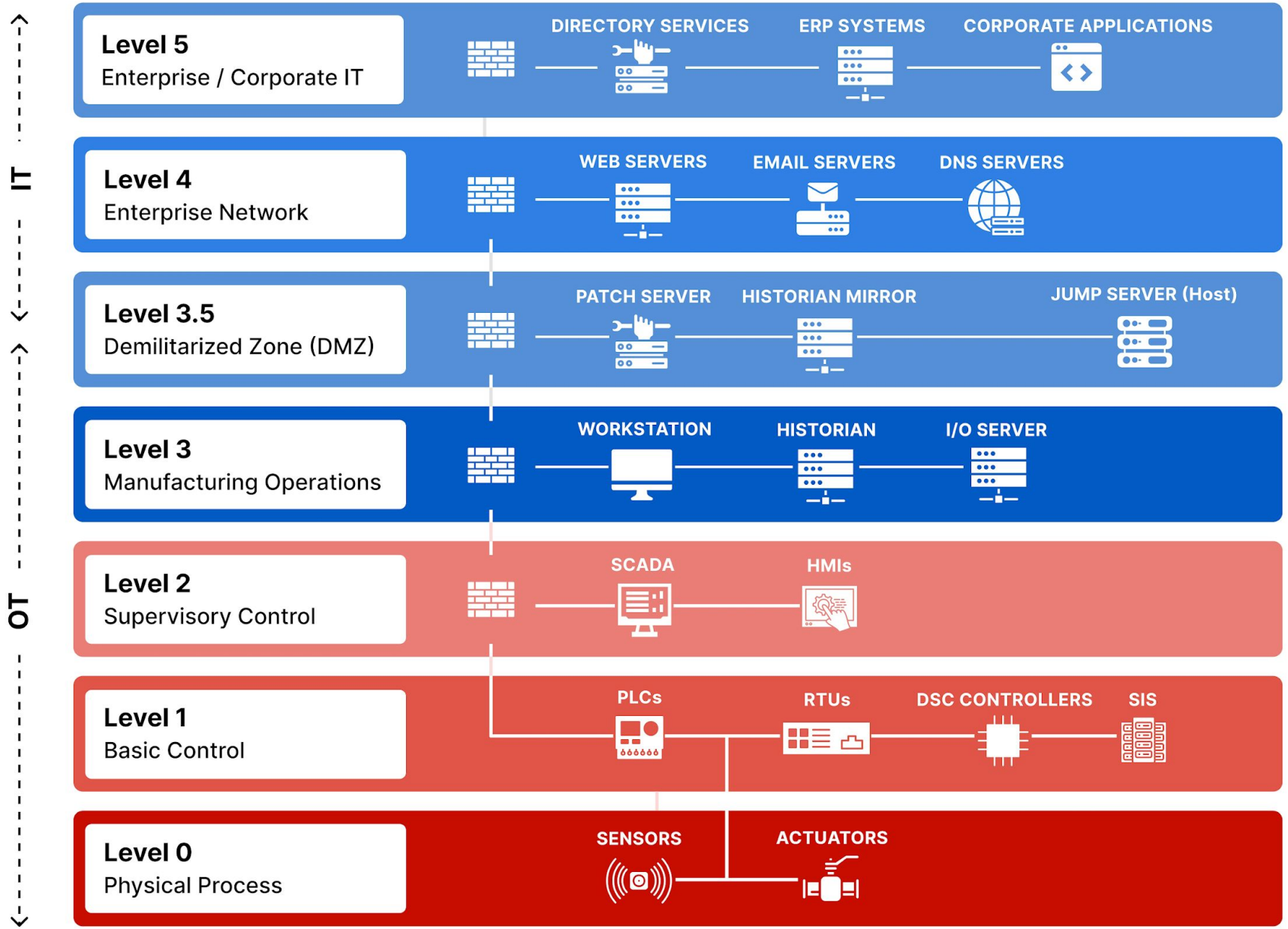
Image Source: IBITEK

Relevant Standards and Frameworks

Area	Standard / Framework	Purpose
OT Security	NIST SP 800-82 Rev. 3	Practical guide for securing factory control systems.
Industrial Security	IEC 62443	Uses zones and conduits to separate and protect OT systems.
AM-Specific	NIST AM Cybersecurity Roadmap, 2023	Identifies cybersecurity risks specific to additive manufacturing.
General Cybersecurity	NIST CSF 2.0	Organizes defense into Govern□Identify□ Protect□ Detect□ Respond□ Recover.
Security Management	ISA/IEC 62443-2-1	Builds policies, asset inventory, and risk management for industrial systems.

These standards translate cybersecurity from "technical tools" into factory-wide governance, architecture, and risk management.

The Purdue Model



Source: zscaler.com

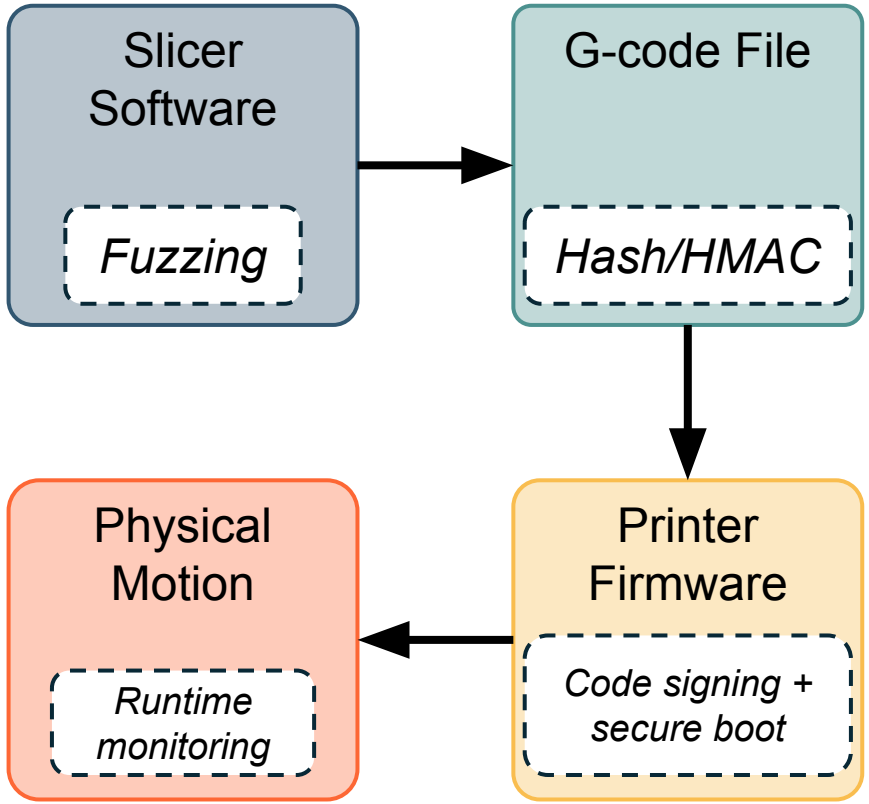
Secure Development for AM Software and Firmware

AM security is not only about protecting the network; slicer software, G-code, and firmware must be designed securely from the beginning.

Slicer software
Threat modeling, static analysis, fuzz testing

G-code file
Hash/HMAC detects unauthorized modification

Printer firmware
Signed updates and secure boot prevent malicious firmware



Anomaly Detection for Manufacturing Security

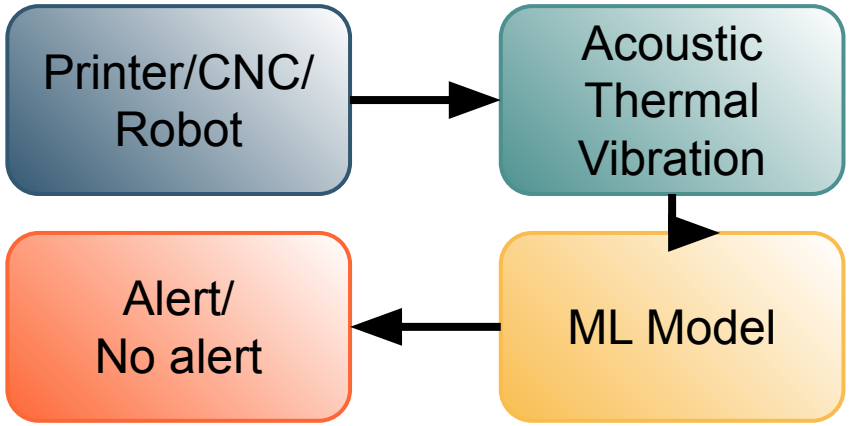
Attacks may not be visible in the file, but they can appear in machine behavior or network behavior.

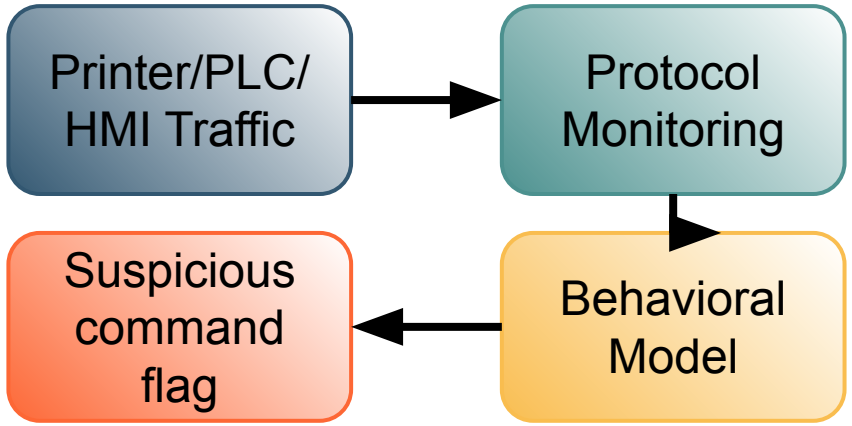
Process Signals

- Acoustic changes during printing or machining
- Thermal or optical deviations from expected layers
- Vibration changes caused by abnormal motion

Network Signals

- Unexpected commands to machines or controllers
- Unusual file transfer or external communication
- New or unauthorized devices on the OT network





⚠️ **Key Challenge: False positive rates must be extremely low in manufacturing environments. A false alarm that halts production costs $10,000–$1M+ per hour.**

Section V

Research Frontiers

- ❑ *Open Problems*
- ❑ *Emerging Risks*
- ❑ *Regulation Gaps*

Image Source: Inpro

Open Research Frontiers in Manufacturing Cybersecurity

Covert Defect Detection at Scale — AM

How can we detect hidden sabotage without CT scanning every part?

Lightweight Security for Small Devices — IIoT

Can constrained sensors use strong encryption without slowing production?

Adversarial ML in Quality Inspection — ML / Security

Can attackers design defects that fool vision-based QA systems?

Secure Design Collaboration — Crypto

Can partners co-design parts without revealing full CAD/IP data?

Forensics Without Shutdown — OT / IR

How do we investigate PLCs and printers without stopping production?

Trusted AM Provenance — AM

Can we track every design change from CAD file to final printed part?

Cybersecurity Is Becoming a Manufacturing Requirement

Regulation / Policy	Purpose
EU Cyber Resilience Act (CRA 2024)	Networked products must meet cybersecurity requirements before being sold in the EU.
CMMC 2.0	Defense manufacturers and AM suppliers need cybersecurity maturity to work on DoD contracts.
FDA Medical Device Cybersecurity Guidance	Networked medical devices need cybersecurity documentation, including SBOM and update plans.
CISA Critical Manufacturing Sector	Manufacturing is treated as critical infrastructure, so cyber incidents become national-level concerns.

Conclusion

1. **Industry 4.0 = Cyber-Physical Systems:** Manufacturing is increasingly connected; digital attacks can disrupt physical production (e.g. Stuxnet, Norsk Hydro).

2. **Additive Manufacturing Threats:** Design-file theft and malicious G-code can create defective parts; firmware or network compromises can change machine behavior.

3. **Layered Defense Required:** Use industrial frameworks (NIST SP 800-82, IEC 62443), **network segmentation** (Purdue model), and secure SDLC (sign/verify design files and firmware). Detect anomalies in both process (acoustic/thermal monitoring) and network traffic.

4. **Regulatory Mandates:** Cybersecurity is now legally required for many products. EU's Cyber Resilience Act and CMMC enforce *"secure by design"* and NIST SP 800-171 controls. Be ready for compliance.

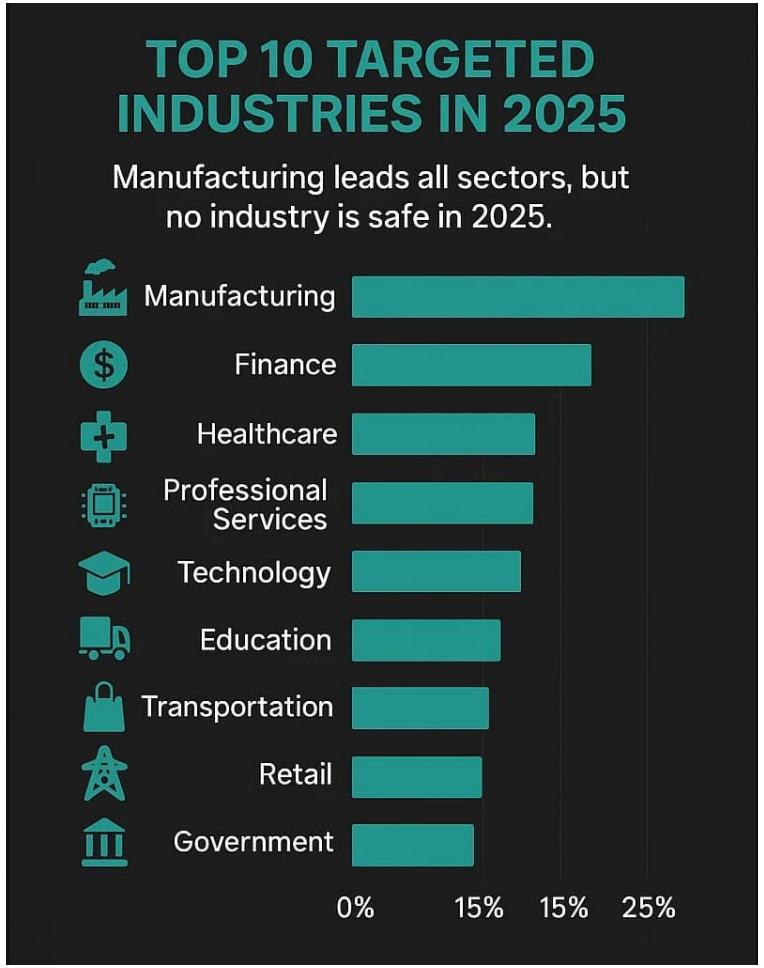
5. **Key Takeaway:** *Cybersecurity in manufacturing is not optional – engineers and future leaders must integrate security from design through production.*

THANK YOU

Any Questions?

satyajit.mojumder@wsu.edu

The Stakes: Real-World Impact



Stuxnet, 2010
Siemens PLCs
Malware manipulated industrial control systems and damaged machinery.

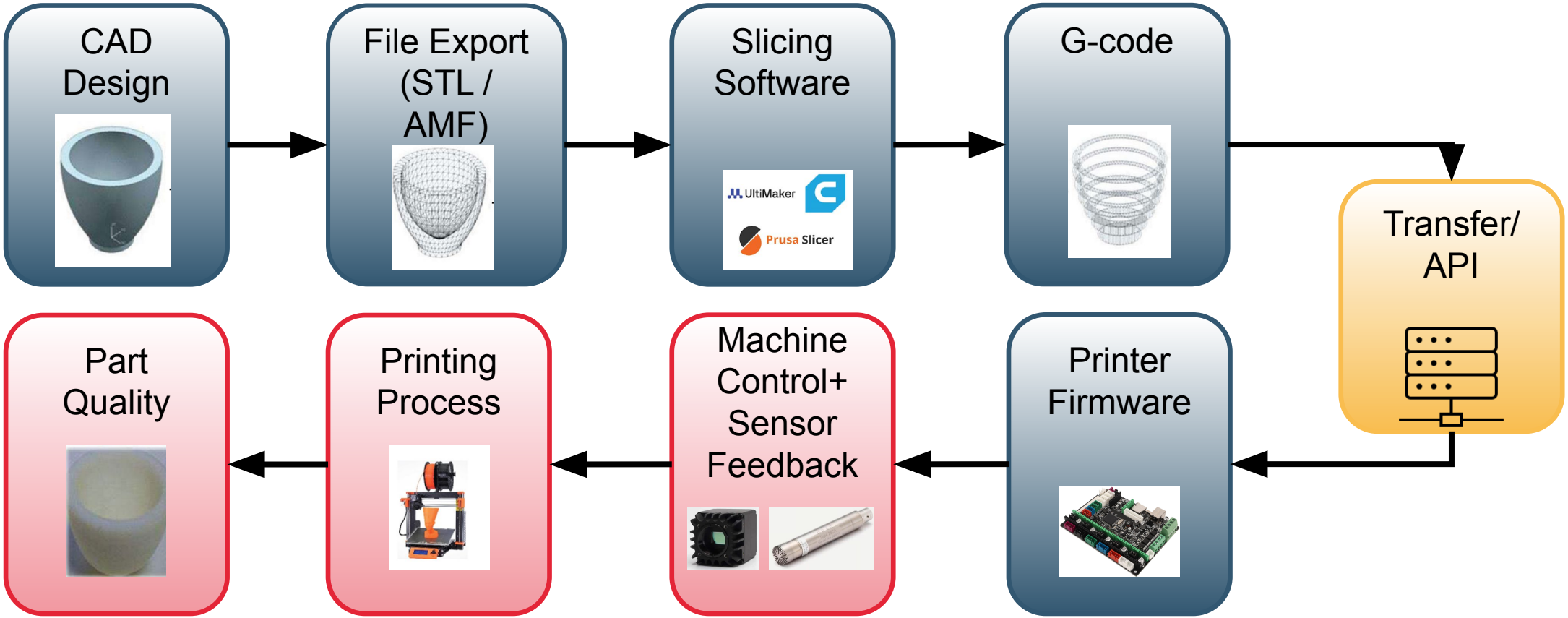
Triton/TRISIS/HatMan, 2017
Safety-system compromise
Attackers targeted systems designed to prevent dangerous failures.

Norsk Hydro, 2019 ($70 million USD**)**
Manufacturing downtime
Ransomware disrupted global aluminum production and forced manual workarounds.

AM Supply Chain, ongoing
Product integrity and IP risk
Design files, toolpaths, process parameters, and monitoring data become attack targets.

https://deepstrike.io/blog/top-industries-targeted-by-hackers-2025

AM Pipeline:
From Digital File to Physical Part



Threat III : Firmware and Embedded Systems Attacks

When attackers reach firmware, digital commands can become physical consequences.

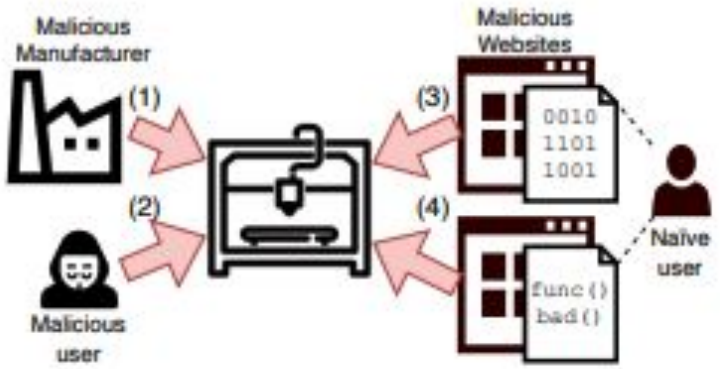


Figure 2: Attack surface for FLAW3D.

Figure 4: Example control group test specimen.

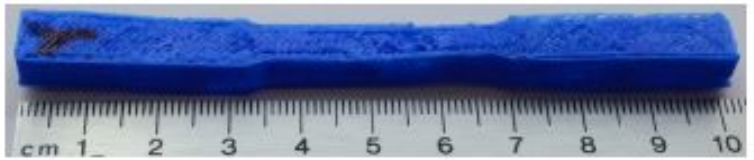
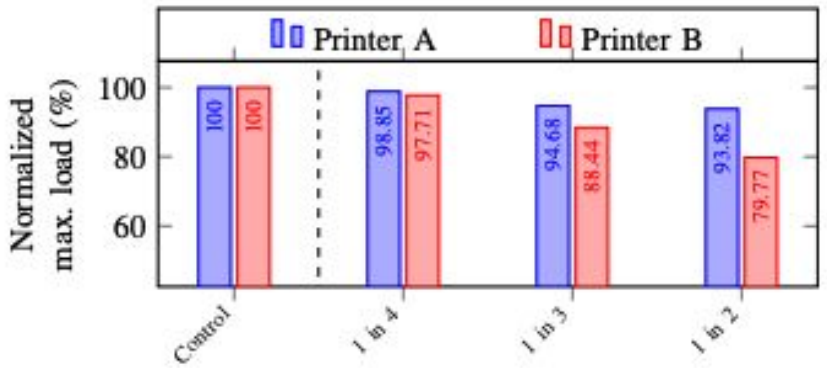


Figure 5: Example 50% material reduction.



FLAW3D: A Trojan-based Cyber Attack on the Physical Outcomes of Additive Manufacturing, Pearce *et al., 2021*