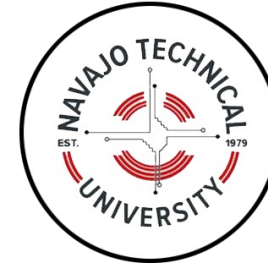
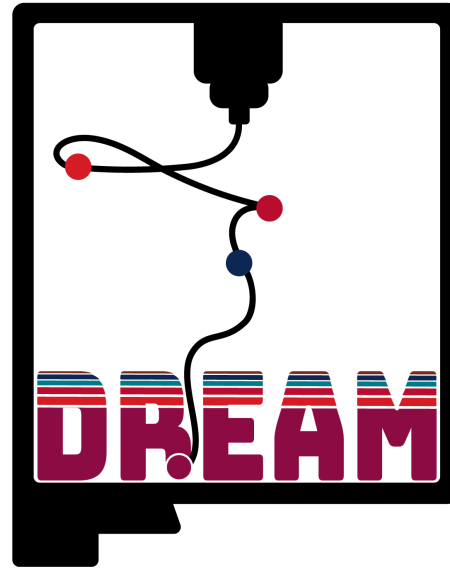




National
Science
Foundation



**DISTRIBUTED RESILIENT AND EMERGENT
INTELLIGENCE-BASED ADDITIVE MANUFACTURING**

NSF E-RISE RII Award #OIA-2417062

Principal Investigator:

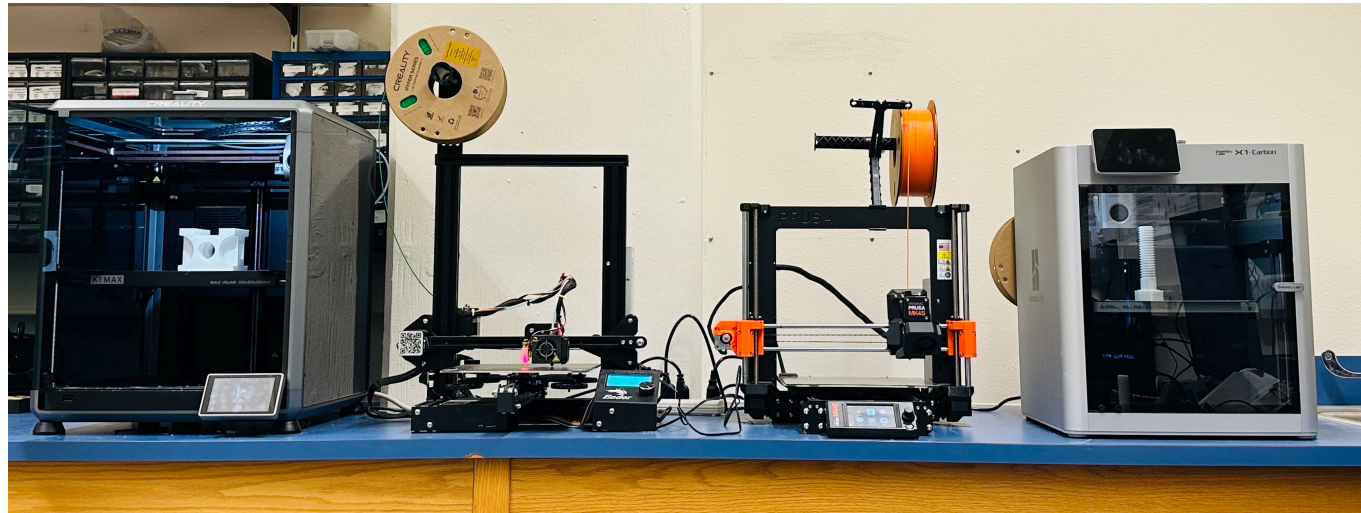
Satyajayant Misra

Co-Principal Investigators:

Mihail Devetsikiotis, Roopa Vishwanathan, Marceline Masumbe Netongo, Krishna Roy

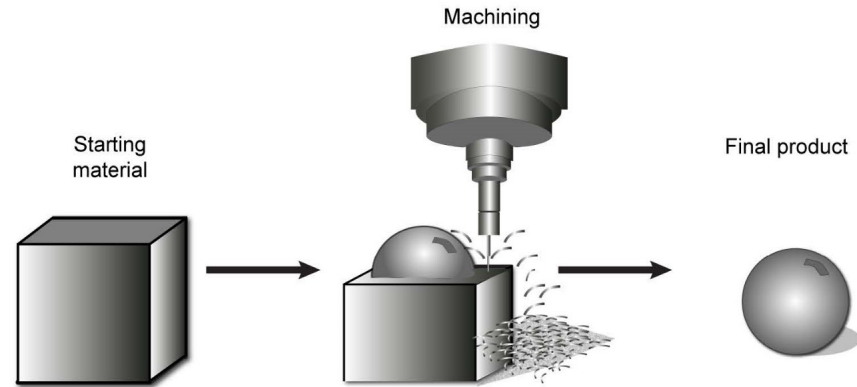
Overview of Operational DREAM Center Acquired 3D Printers

Krishna Roy and Chaitanya Mahajan

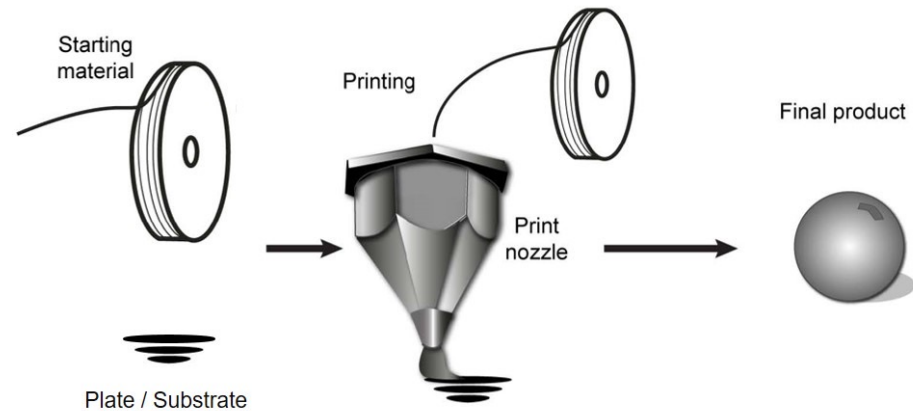


Subtractive vs Additive Manufacturing

Subtractive

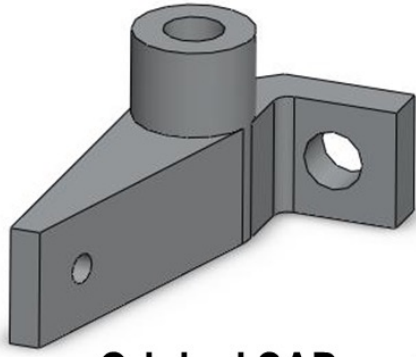


Additive

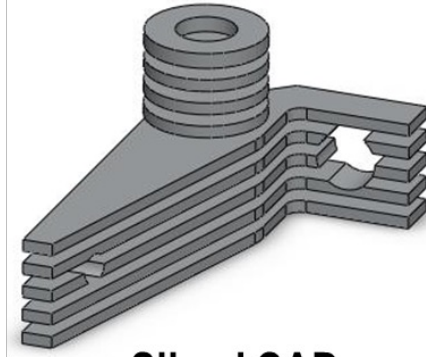


Additive Manufacturing (AM)

- 3D printing, additive manufacturing, solid freeform fabrication, digital printing, rapid prototyping, etc.
- 2.5D, 3D, and 4D printing
- Layer-by-layer printing



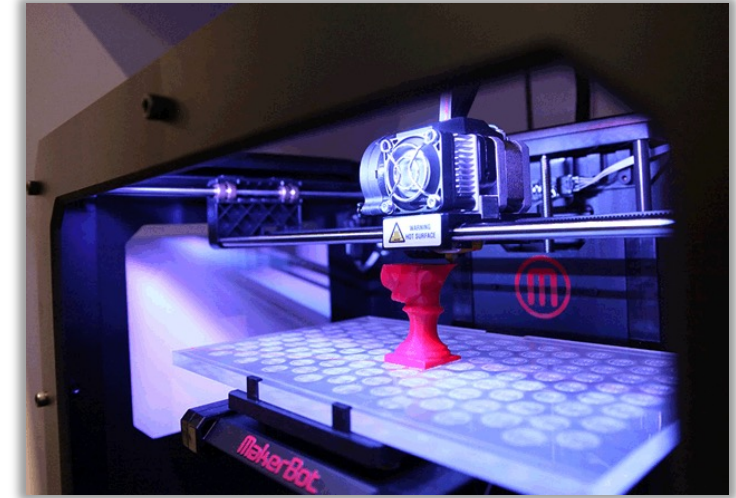
Original CAD
Model



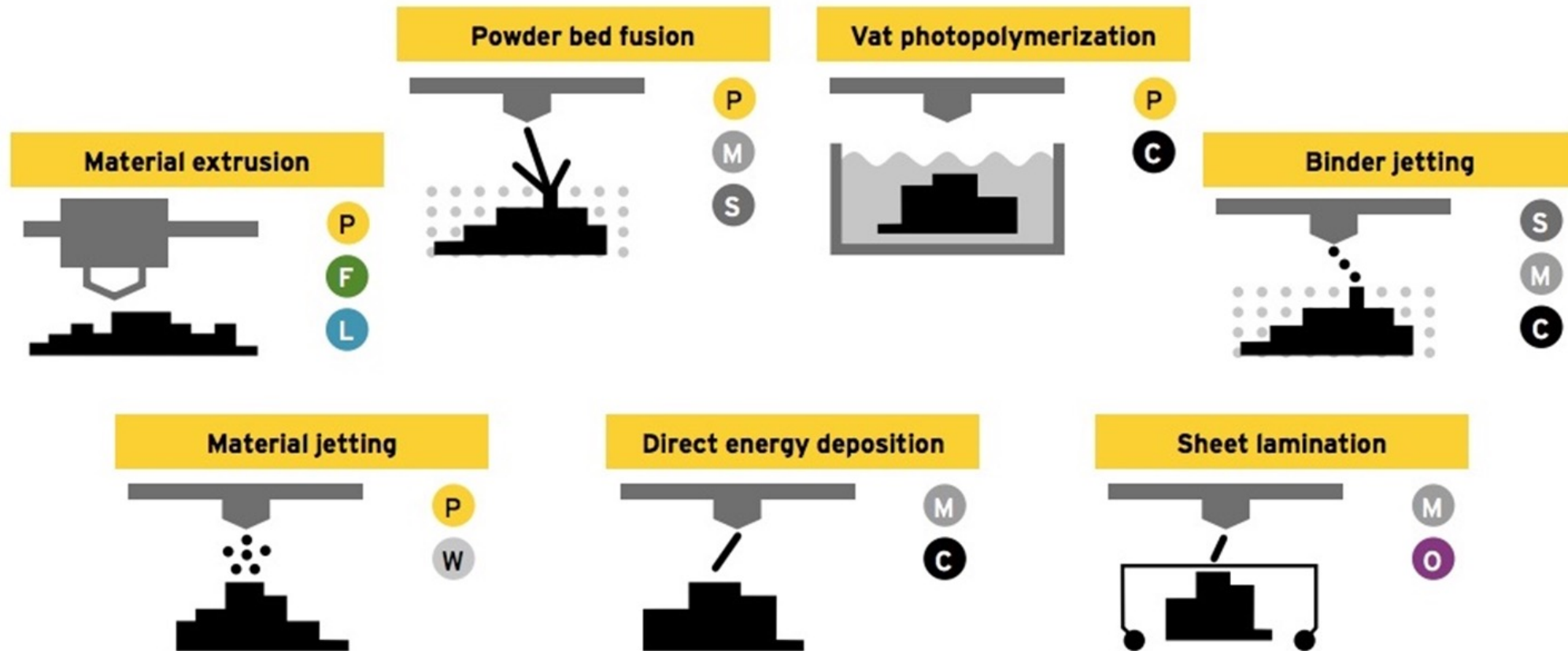
Sliced CAD
Model



First Printed
Layer

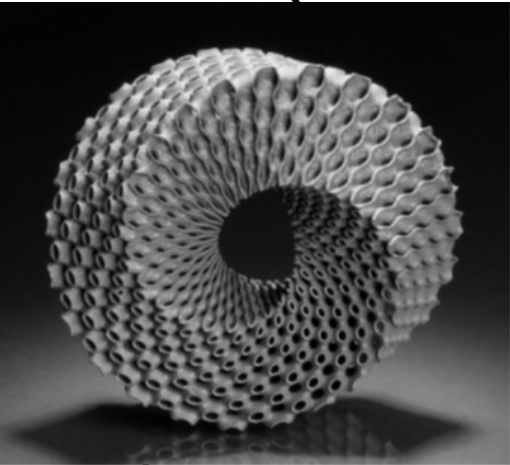


Different AM Processes



Material key: P=Polymer, M=Metal, O=Organic material, C=Ceramic, S=Sand, L=Live cells, F=Food, W=Wax

Complex Geometry



Art piece by AM
From <http://www.3ders.org/>



Prosthesis



Teeth Aligner
From <https://www.invisalign.com>



hearing aid bud
From <https://enviontec.com>



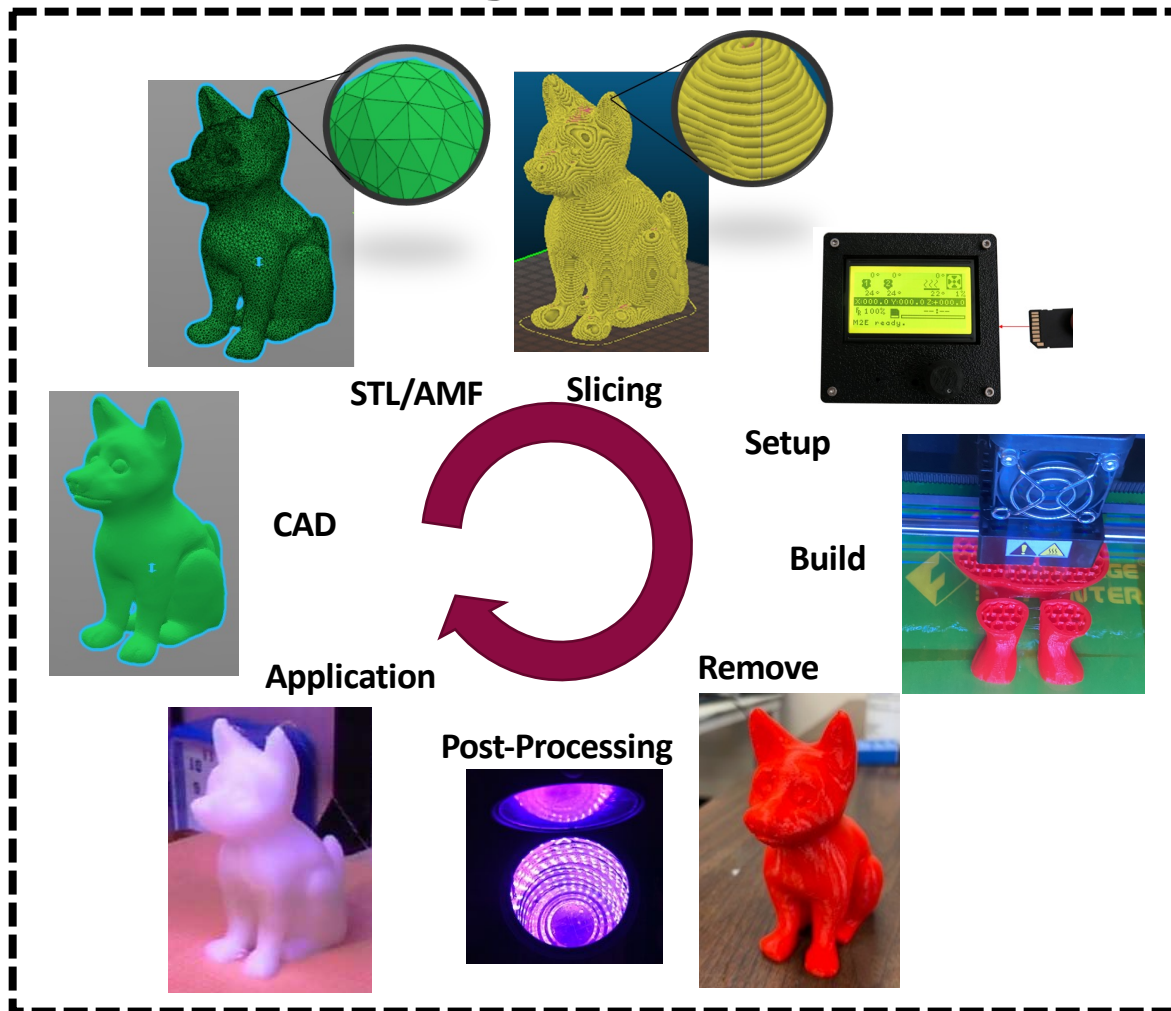
fuel nozzle 25% lighter, 5x stronger
From <http://www.gereports.com/>



Airbus A320 nacelle bracket 30% lighter
From <http://www.altairhyperworks.com/>





AM Production Cycle



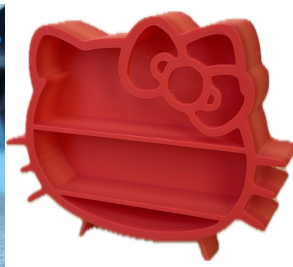
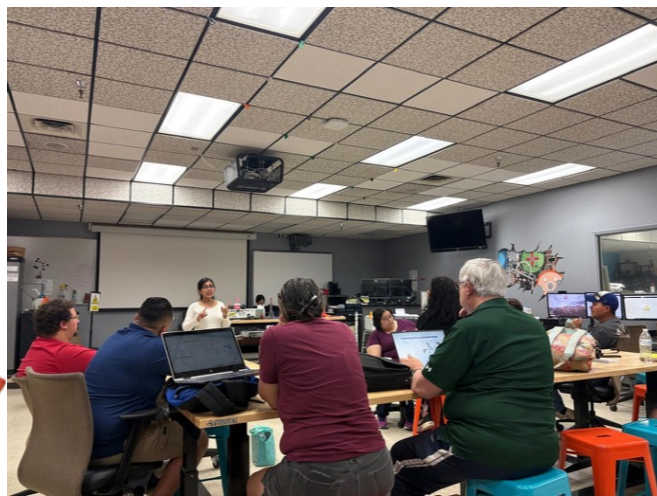
Additive Manufacturing Process Flow: CAD → STL/AMF → Slicing → Setup → Build (Print) → Remove → Post-Processing → Application



Challenges to Adopt AM

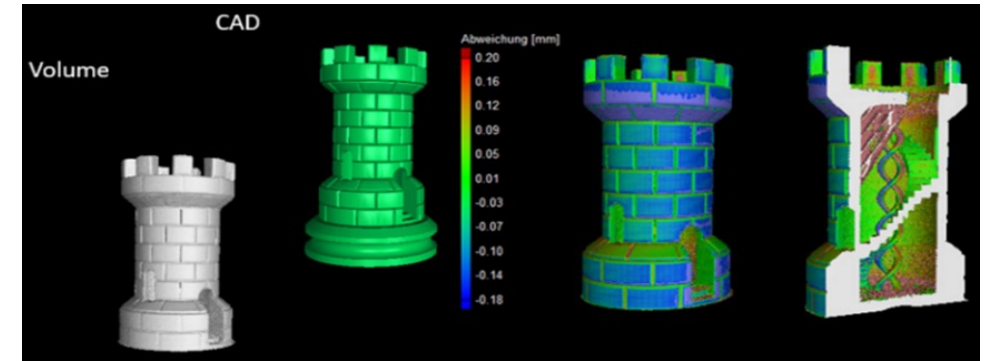
- 
- Quality of AM parts
 - Anomaly identification
 - Data safety
 - Teaching and workforce
- 

Workshop: K-12 Teachers

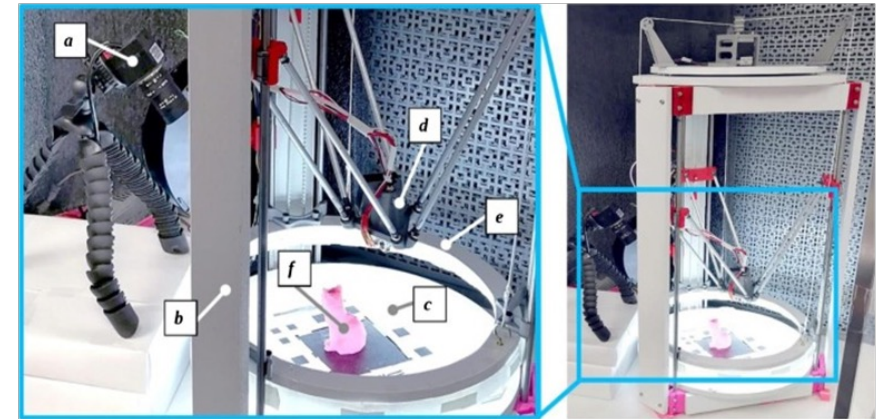


Additive Manufacturing Quality Control

- Quality control within Additive Manufacturing (AM)
 - Non-destructive testing
 - Computer vision
- Benefits of utilizing a computer vision-based quality control:
 - Cost efficiency in optical lenses
 - Applicable across different AM processes
 - Visually interpretable data and results
 - in-situ process monitoring/inspection



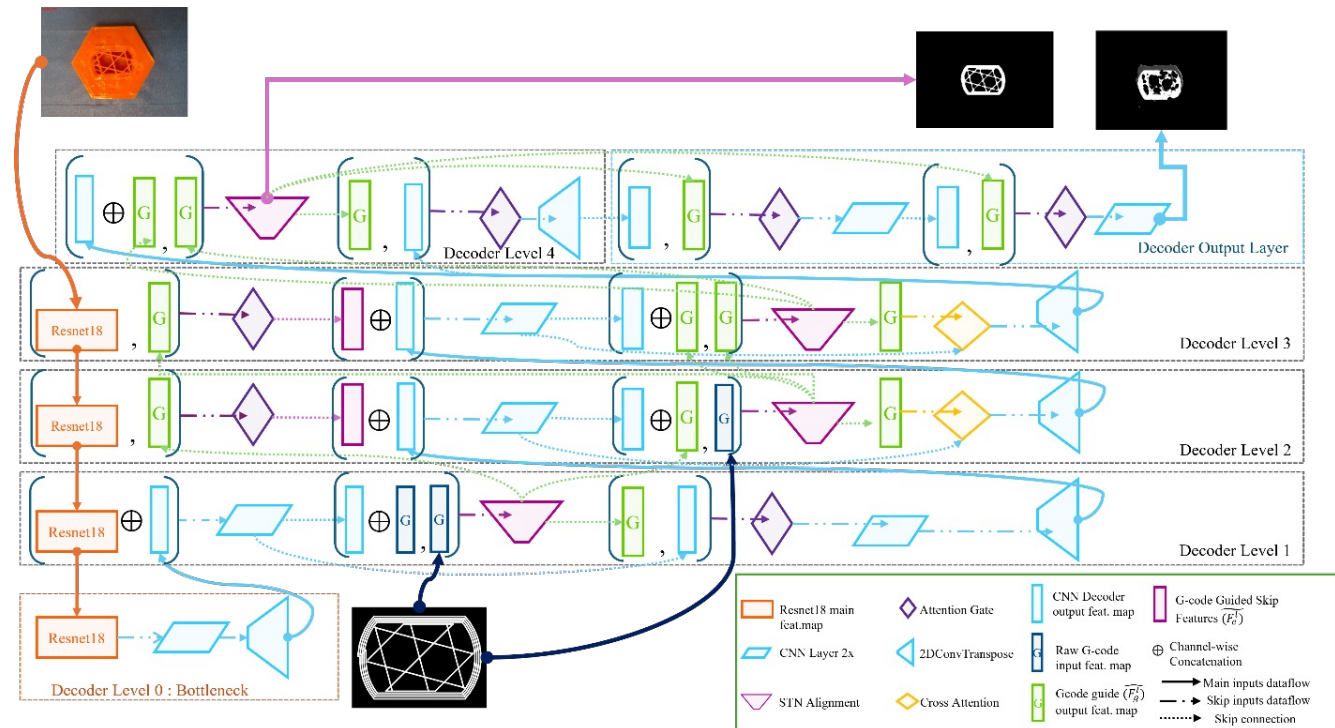
[1] CT Scan comparison to CAD model



[2] Computer Vision in 3D Printing

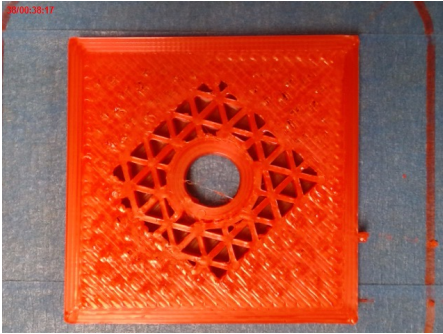
G-code Gated U-Net (GG-Net)

- G-code Gated U-Net (GG-Net) integrates the encoder/decoder architecture of the standard U-Net
- GG-Net is designed for top-layer (TL) segmentation from images captured from a top-view perspective

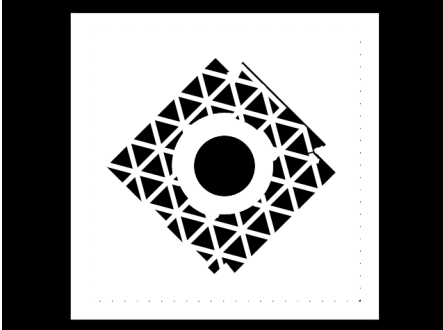


GG-Net Architecture

G-code Gated U-Net (GG-Net)

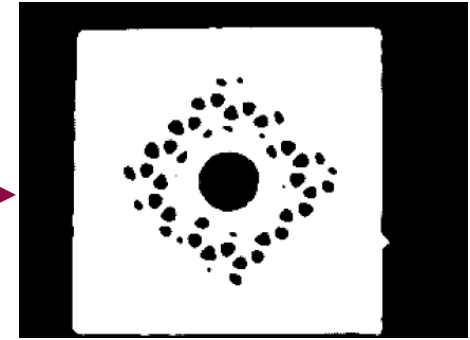


In-Situ Image captured using a webcam

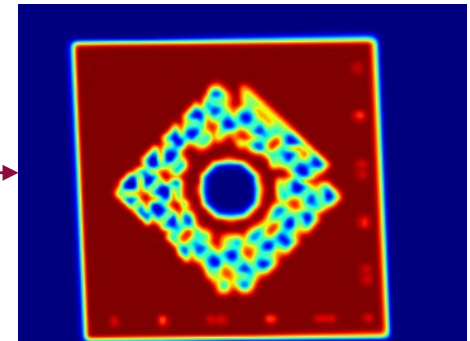


Nominal Image from G-code

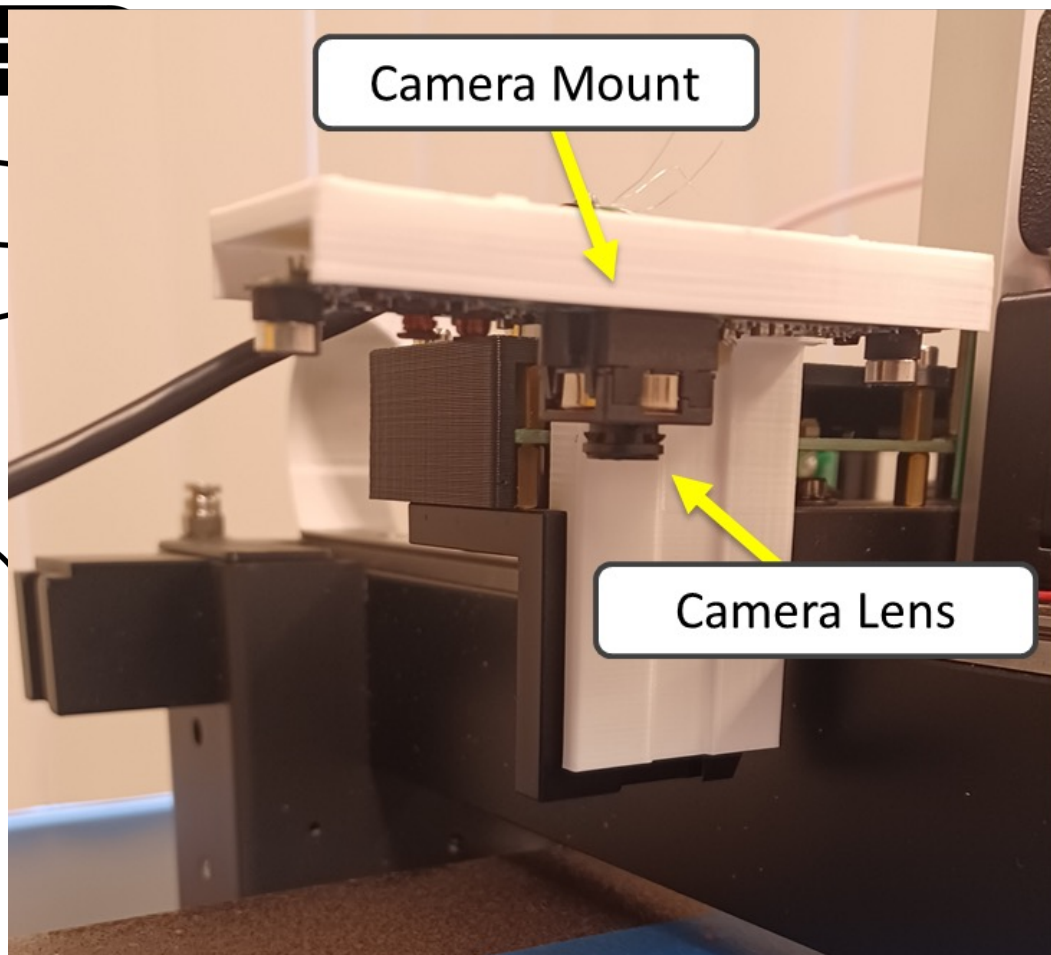
GG-Net



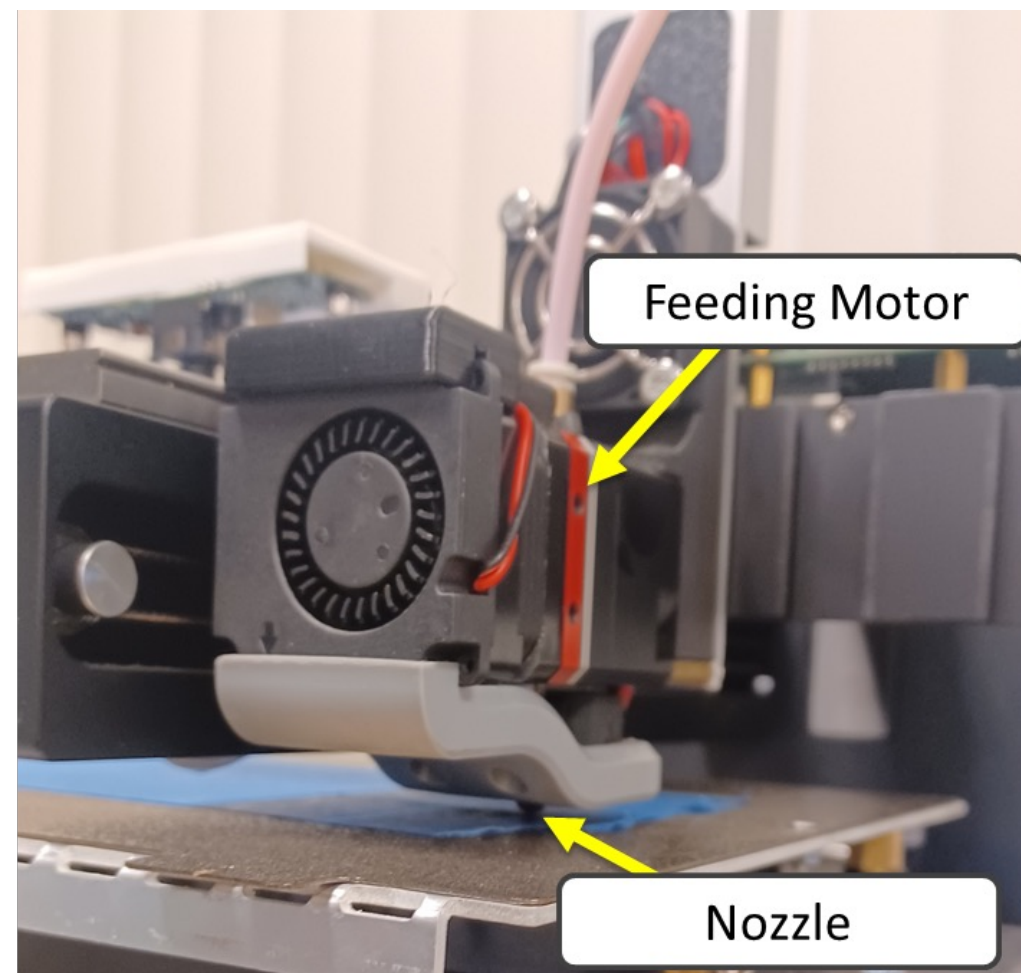
Binary segmentation of top layer



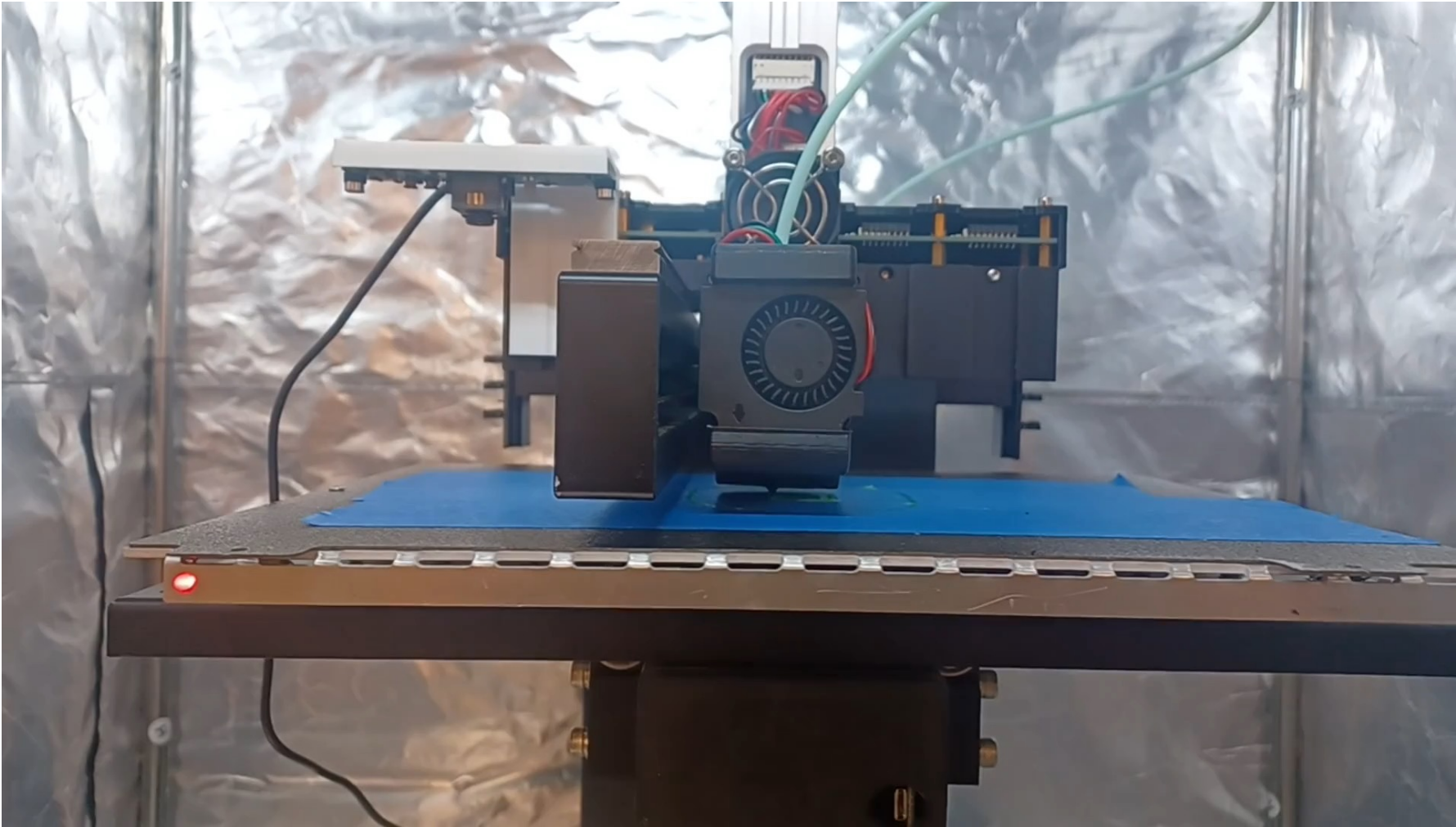
Nominal image aligned
(predicted top layer)



Camera

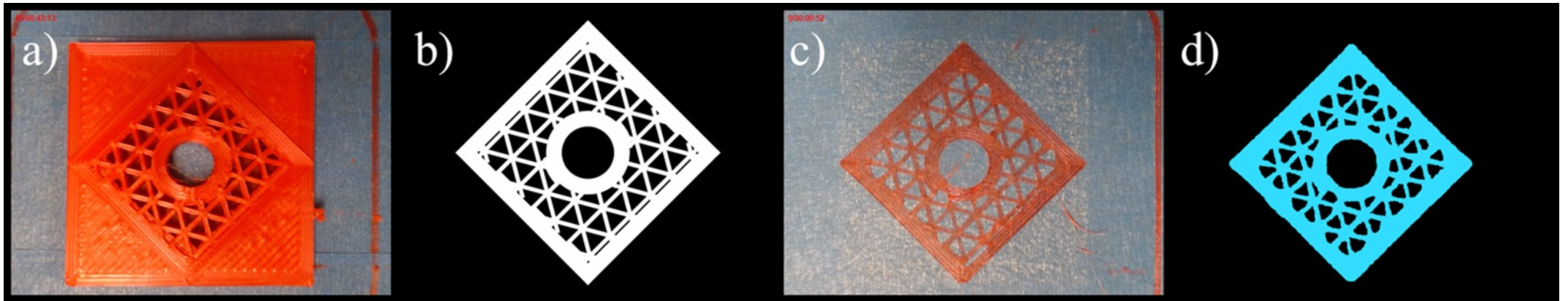


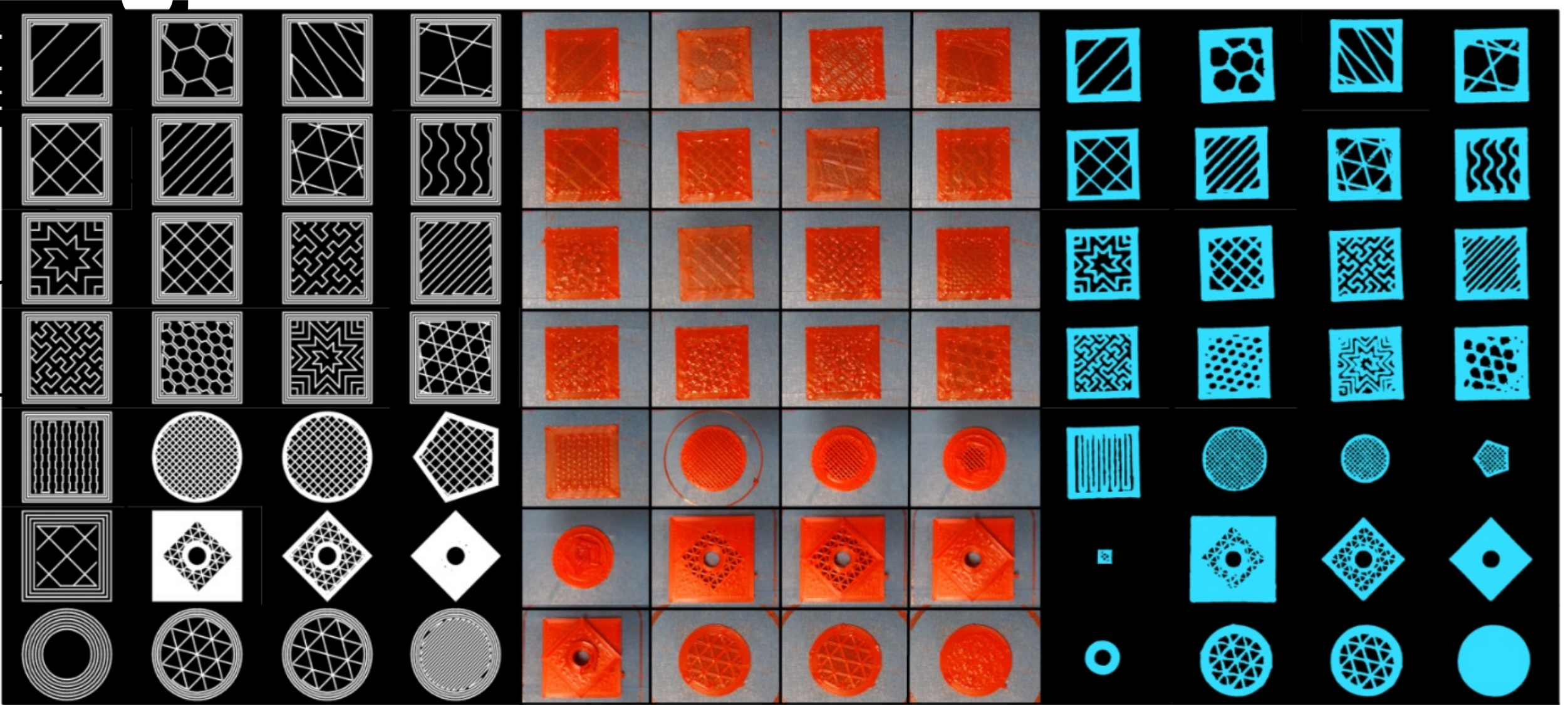
FH2-260 Extruder



Labeling Training Data

- Once raw images were gathered, training masks were developed through human labeling on custom software
 - capture images pertaining to the isolated layer's extrusion at the same camera offset and conditions as its training counterpart
 - segment the captured images of individual layers into generated mask labels
 - match the mask labels to the training dataset.





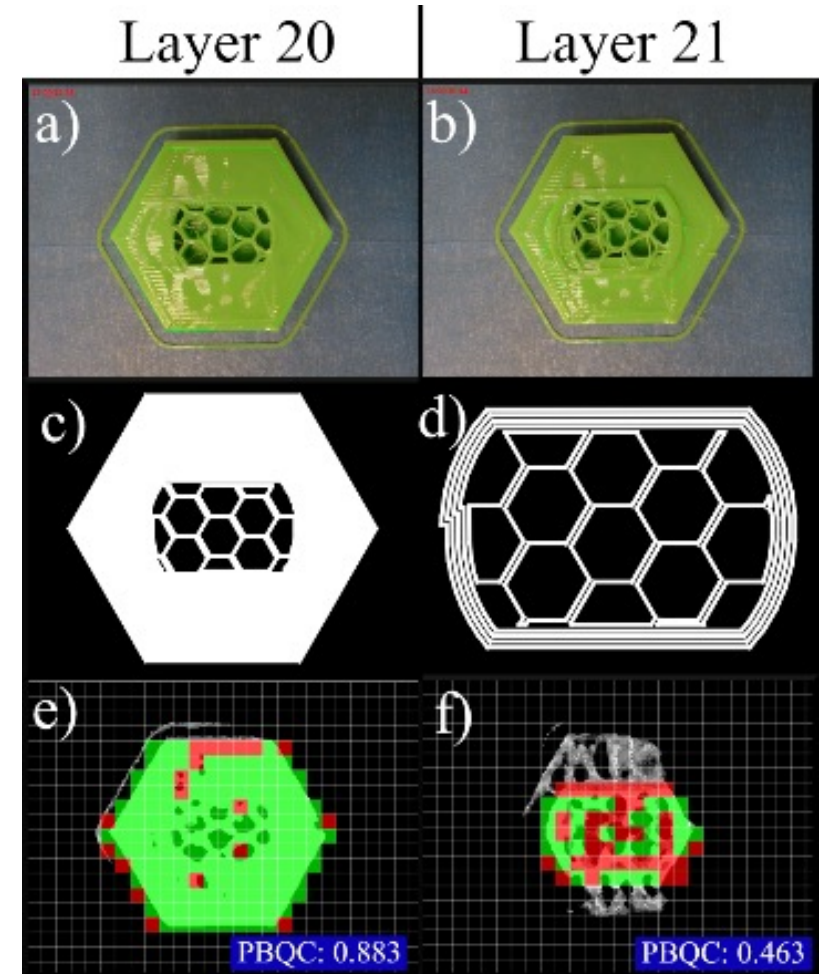
G-code Nominal References

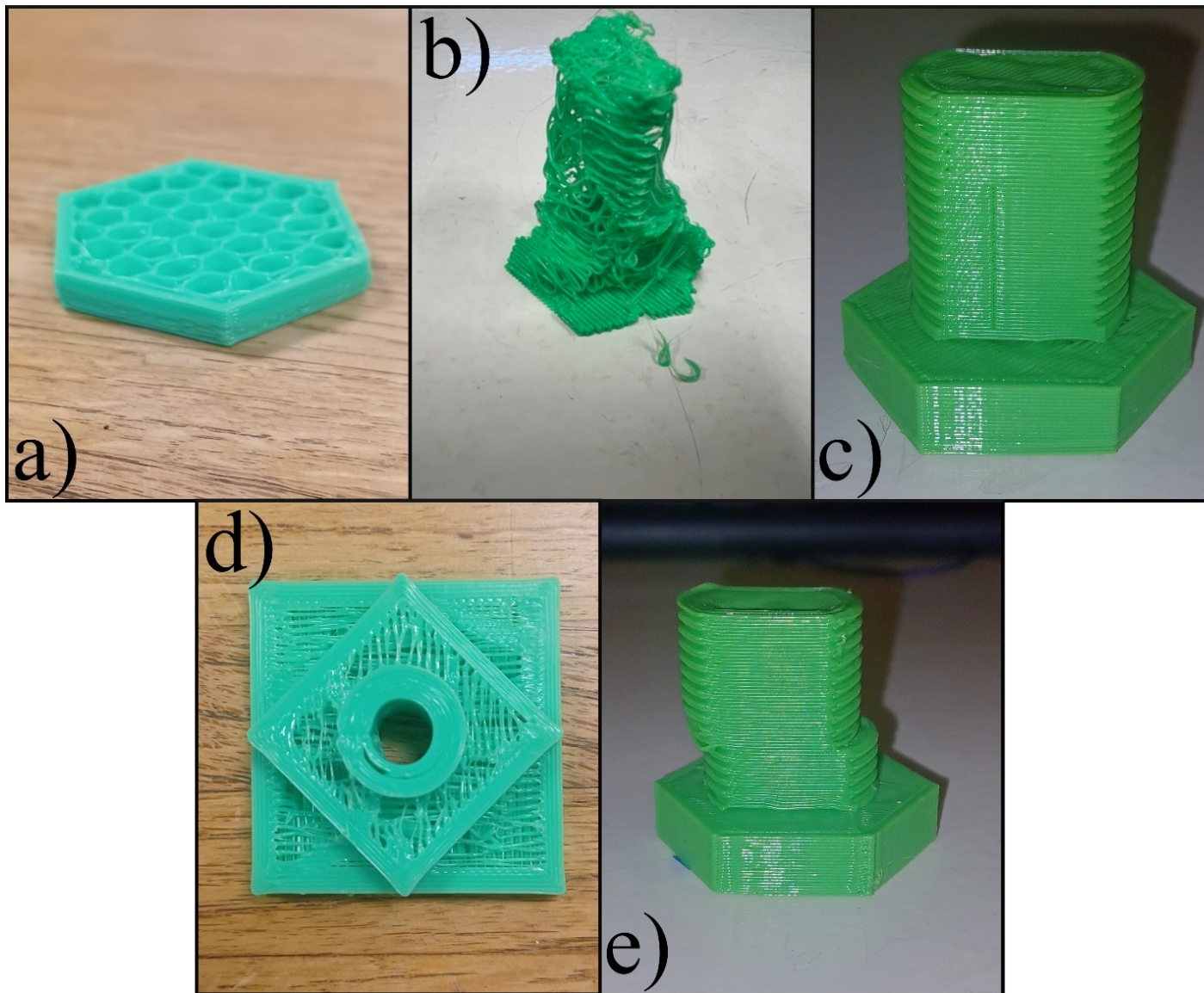
In-situ Photos

Target Mask Labels

Patch Based Quality Characteristic (PBQC)

- Patch Based Quality Characteristic (PBQC) is the measuring characteristic used to evaluate GG-Net
- PBQC breaks the aligned nominal image and binary segmentation of the TL into 24x24 patches, each evaluated independently
- The final score is a ratio of compliant to total evaluated patches

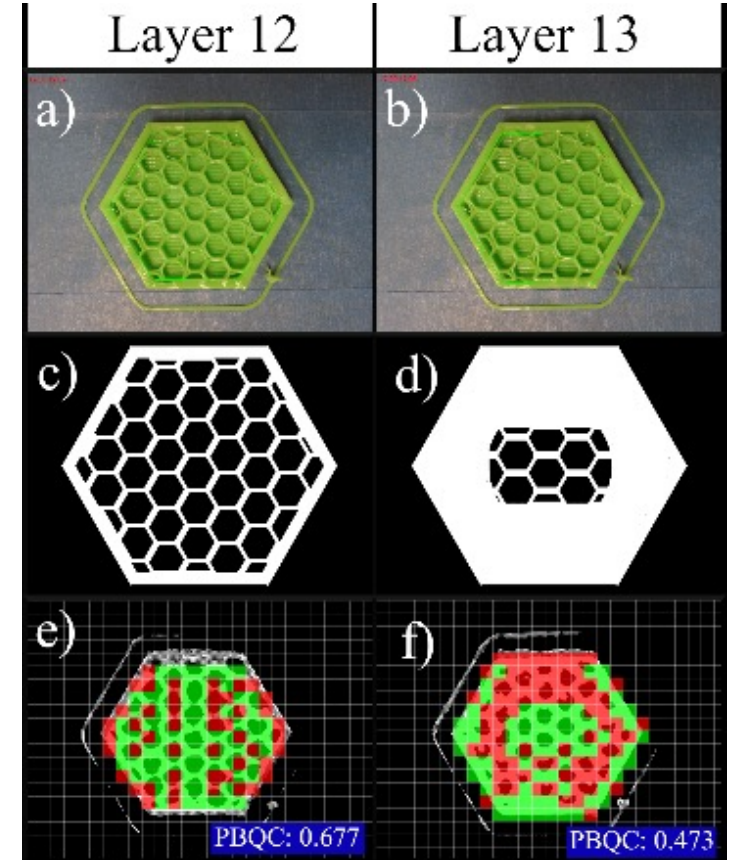
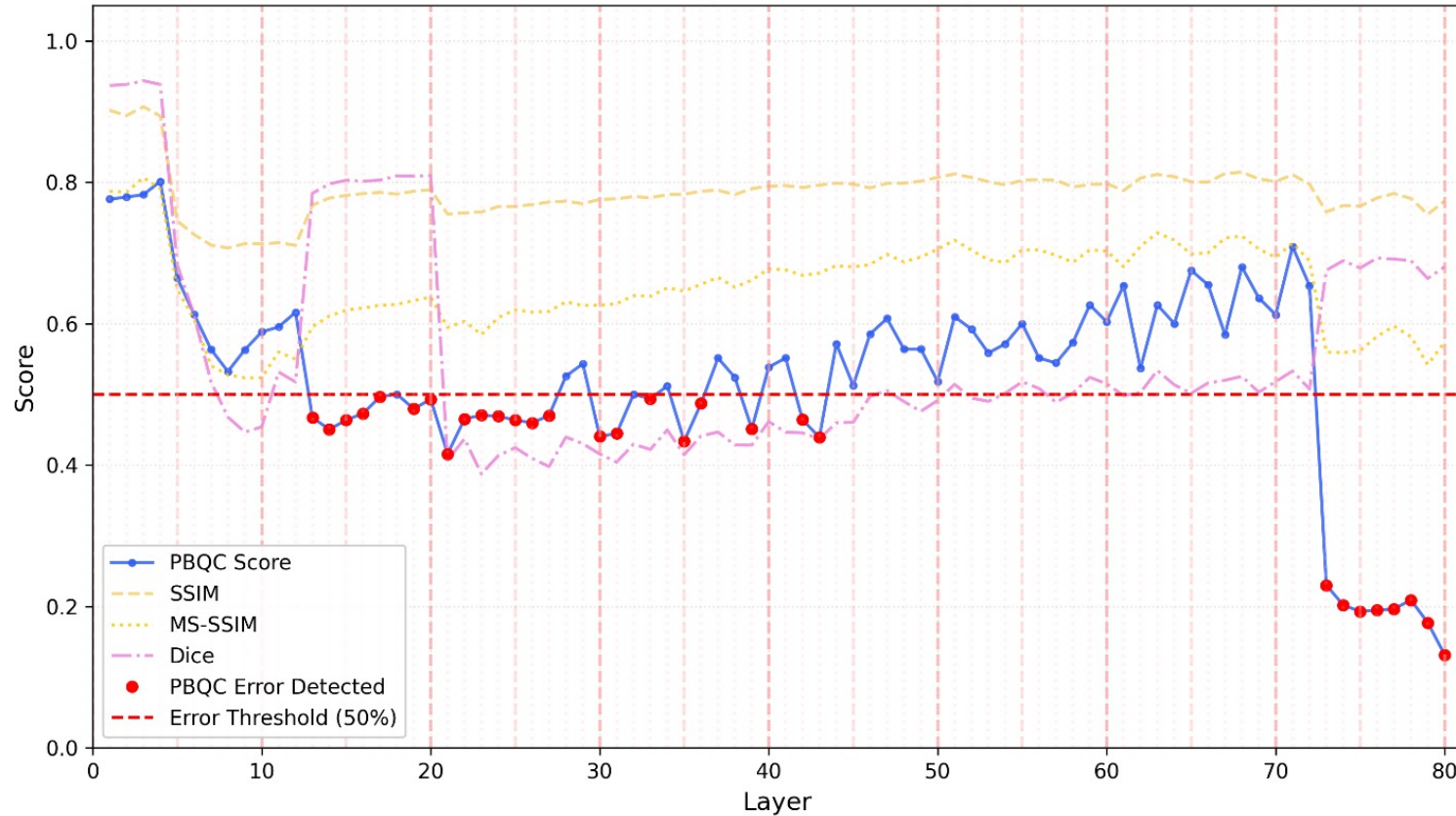




Evaluating GG-Net with Errors: Nozzle Clog


- Induced by continuously capturing images after the completion of the twelfth layer

Metrics Comparison Across Layers

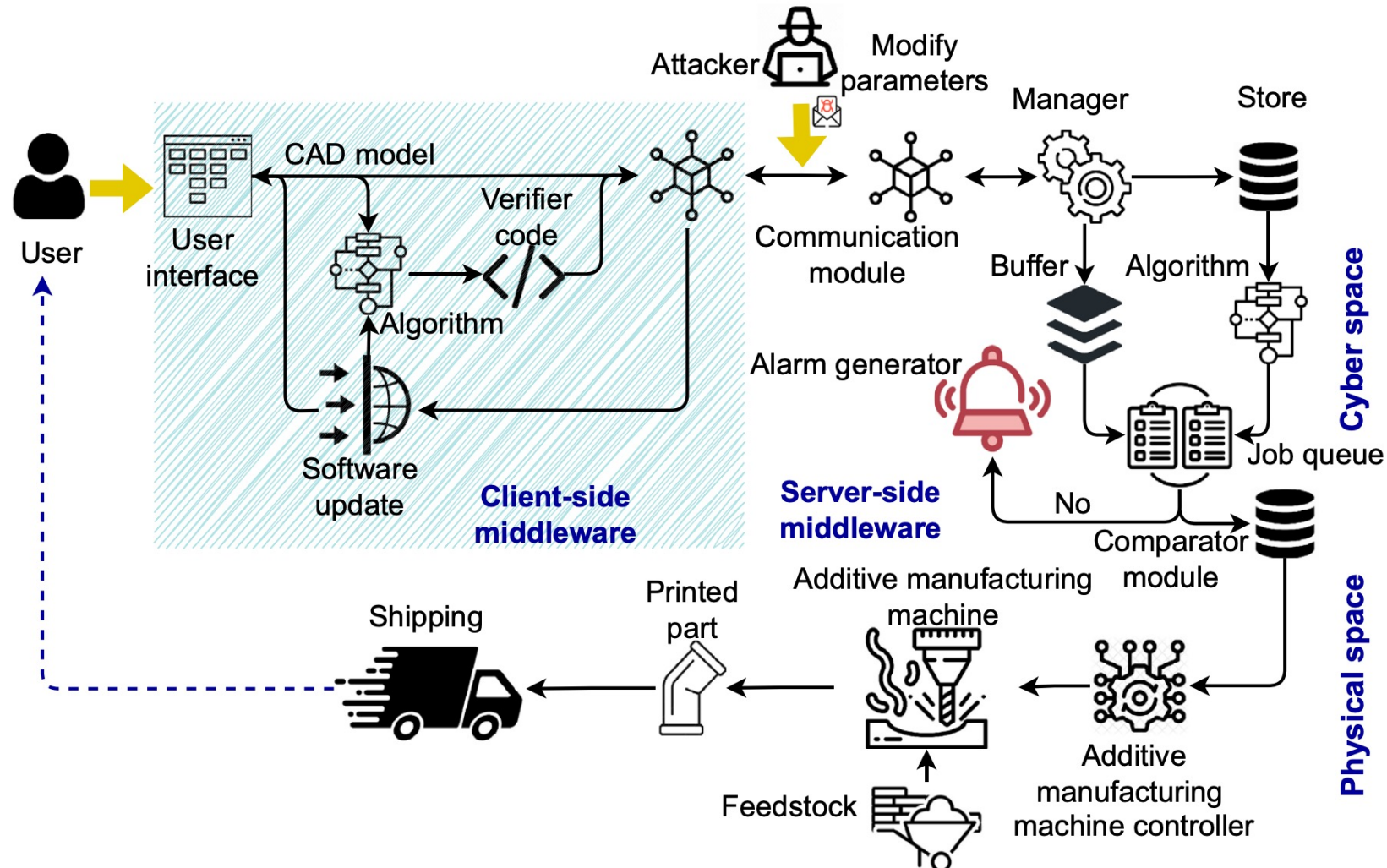




Current Status

- Expanding the training dataset to include more complex geometries and different printing parameters
 - Evaluate zero-shot testing of our approach on complex geometries
 - Describe current obstacles to networked/remote printing and quality assessment capabilities (with estimated timeline to solve each obstacle, if possible, to reference strategic plan)
- 

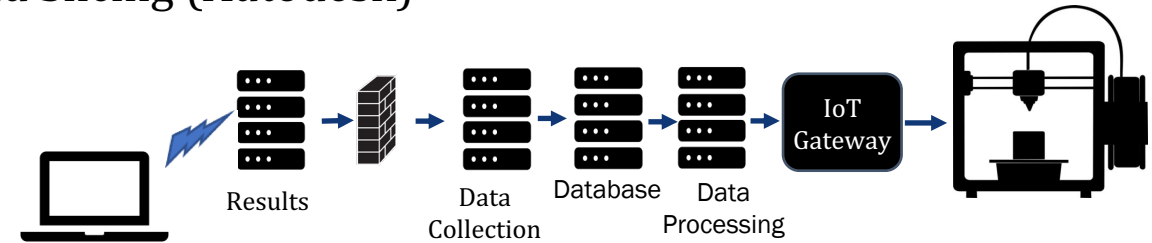
AM Cyber and Physical Space



Network Architecture

Baseline

Printer ↔ OctoPrint/WebUI (WiFi/Eth) → Cloud Slicing (Autodesk)



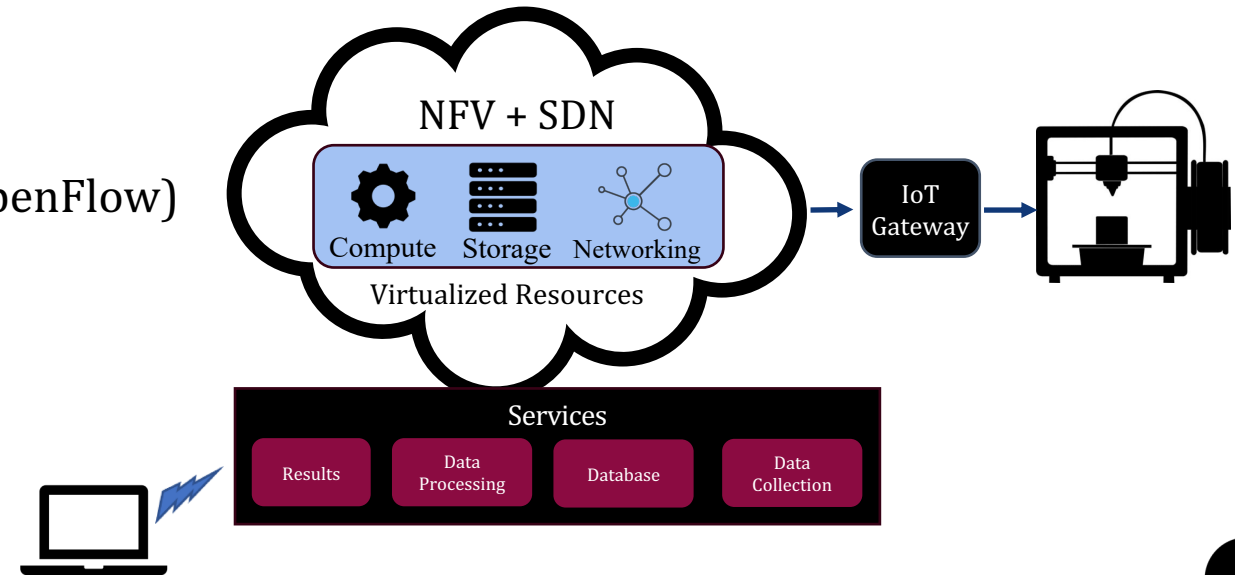
Advanced

SDN for IIoT orchestration

- Centralized control for printer fleets (OpenFlow)

NFV virtual slicers in Industry 4.0 CPS

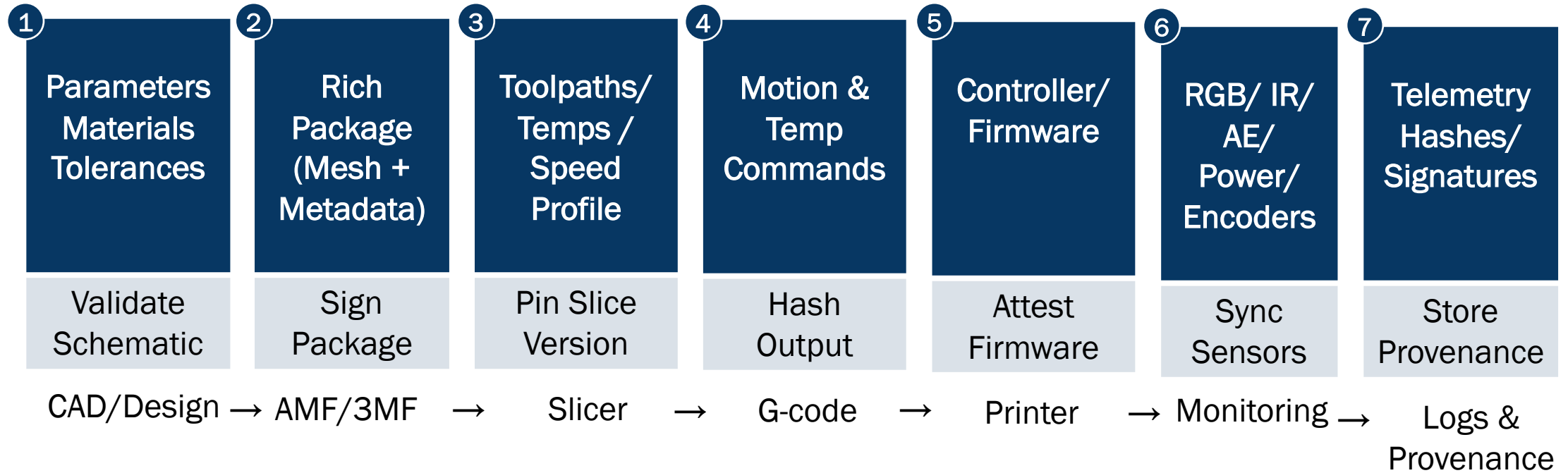
- Cloud-orchestrated slicing



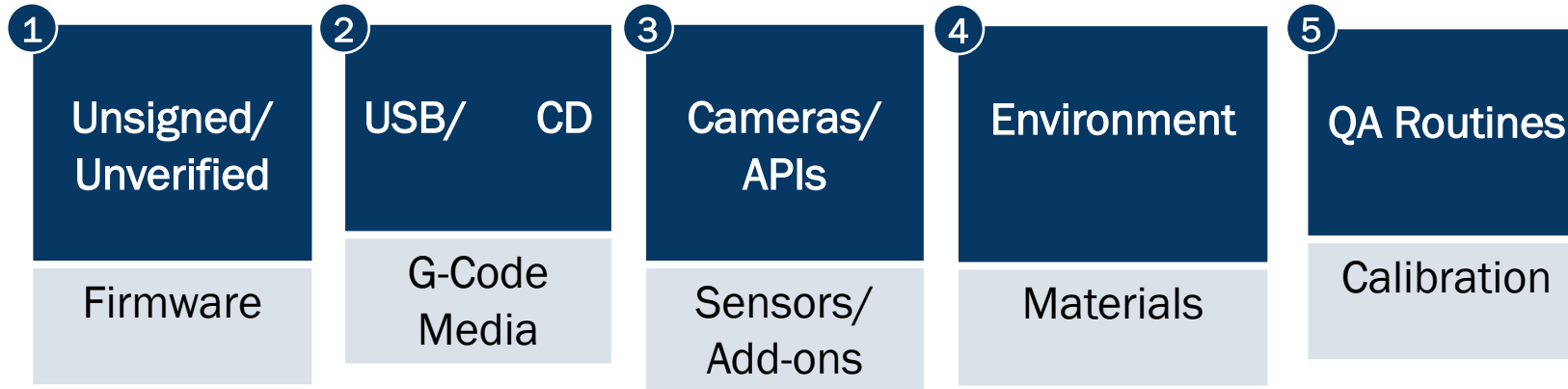
Slicer & Print-Server Ecosystem

Printer	Default Slicer	Print Server / Control Interface	Cloud Integration	Notes
Creality K1 Max	Creality Print (uses Cura engine)	Fluidd / Mainsail / Creality OS UI via Moonraker	Optional Creality Cloud	Rooted unit can use Klipper APIs & custom scripts
Creality Ender 3	Ultimaker Cura / Prusa Slicer / Orca Slicer	OctoPrint / Mainsail / Fluidd (when Klipper installed)	None by default	Highly modular and open-source
Prusa MK4s	Prusa Slicer	Prusa Connect / OctoPrint(Via Raspberry Pi)	Prusa Cloud (optional)	Native integration with Prusa ecosystem
Bambu X1 Carbon	Bambu Studio (closed)	Bambu Handy App / Bambu Cloud	Mandatory Cloud for updates & monitoring	Encrypted .3mf container with G-code and metadata

Networking and AM Data Flow

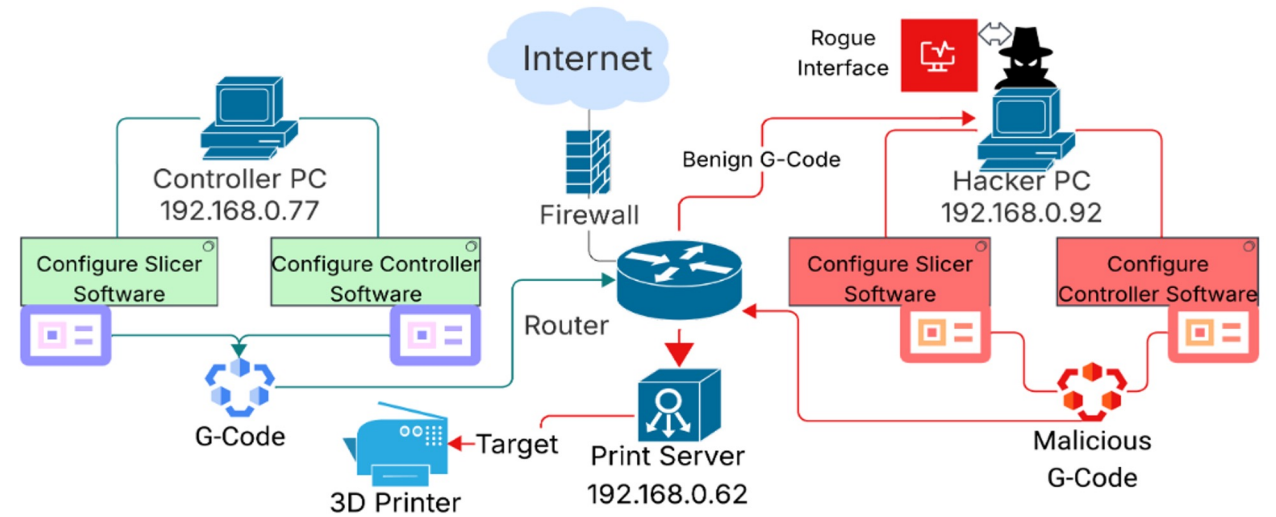


Physical/Operational Vulnerabilities



- Unverified Firmware: debug ports (UART/JTAG), OTA downgrades
- USB/SD Removable Media (malicious G-code, autorun macros)
- Material/Environment: filament swaps, powder contamination, humidity/temp drift
- Sensor Tampering: camera occlusion, IR/light injection, AE masking
- Side-channels: optical/acoustic/power leakage of IP/toolpaths
- Power/EMI events; physical access to controllers and storage

Network Vulnerabilities



- Rogue AP / Wi-Fi spoof → MitM (API keys, tokens, job tamper)
- Weak TLS (no pinning), cookie/session hijack, CSRF on controllers
- Insecure protocols & config: HTTP/MQTT, OPC UA with anonymous creds
- LAN/VLAN gaps: client-to-client access, missing egress control
- TSN/PTP timing abuse → micro-jitter impacts process quality
- Remote access/VPN misuse; exposed admin interfaces

Literature Demonstrated Attacks

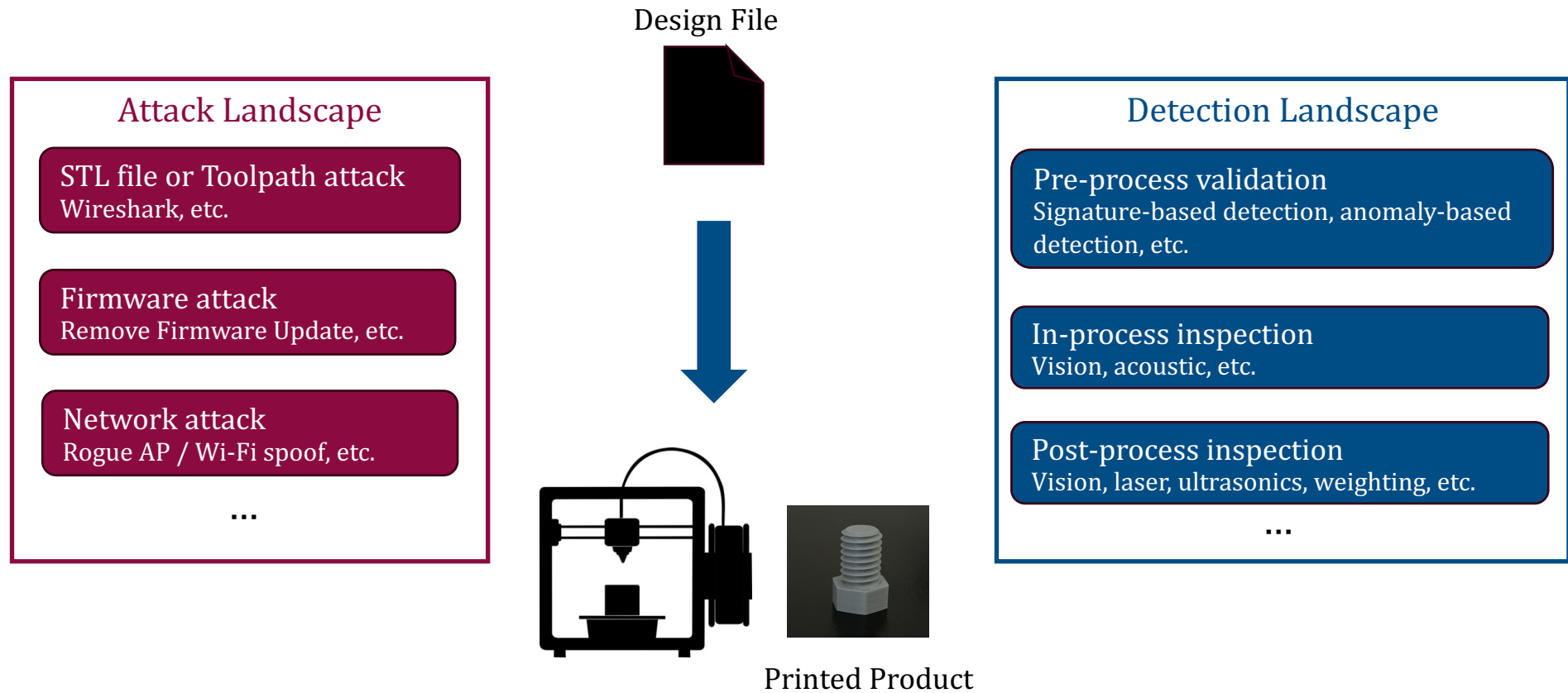
Attacker Model	Access	Example Attack	Success Rate (8 Printers)
AC1	Pre-exec inject	M928 IP theft	100%
AC2	Slicer config	Over-extrude (M200)	87.5%
AC3	On-fly inject	Voids (M28)	75%

Attack vectors causing physical damage

- **G1 Z-1:** Nozzle crash into bed
- **M907:** Motor current overload — leads to burnout.
- **dr0wned (WOOT 2017):** Cyber-induced **internal voids** cause **fatigue failure** under load

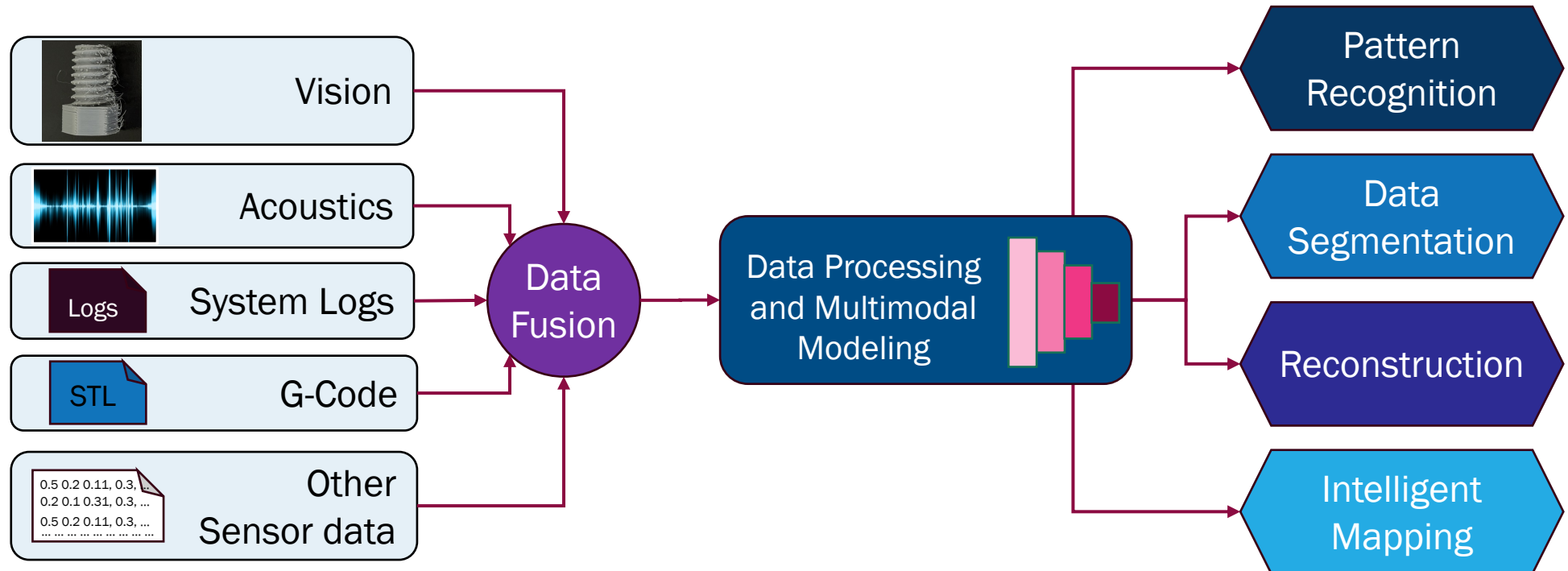
1. Rossel, Jost, Vladislav Mladenov, Nico Wördenweber, and Juraj Somorovsky. "Security Implications of Malicious {G-Codes} in 3D Printing." In 34th USENIX Security Symposium (USENIX Security 25), pp. 1867-1885. 2025.
2. Belikovetsky, Sofia, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, and Yuval Elovici. "dr0wned—{Cyber-Physical} attack with additive manufacturing." In 11th USENIX workshop on offensive technologies (WOOT 17). 2017.

Anomaly Detection Baselines

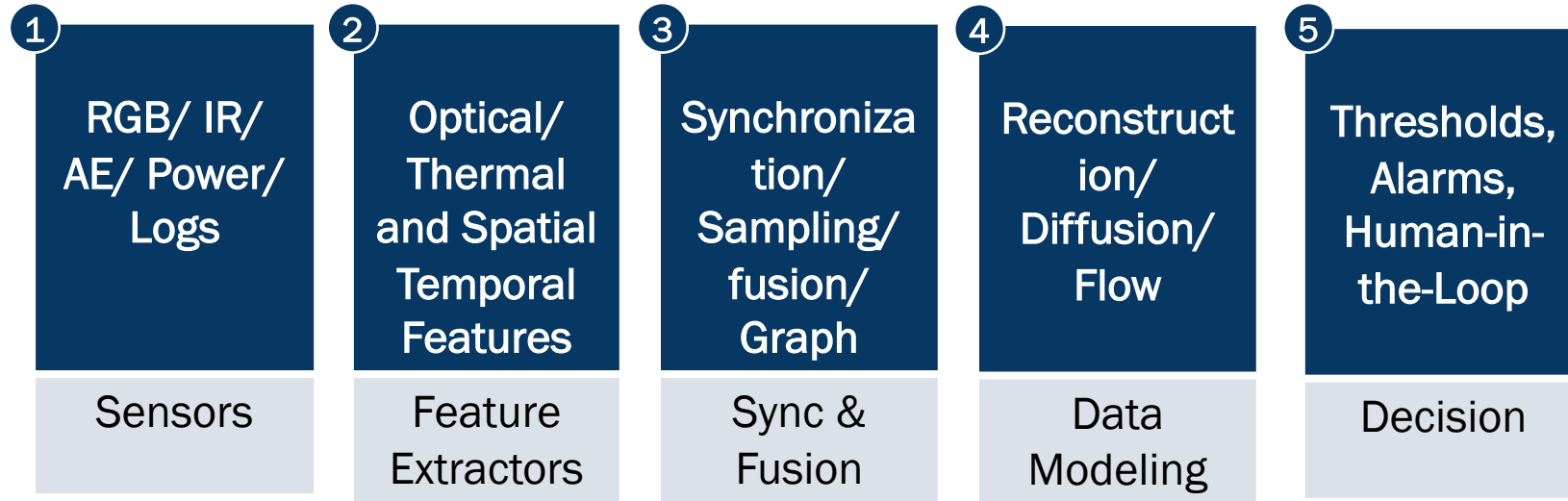


Multimodal Data Modeling

- Network and host logs and data provenance
- Print Progression Videos
- Acoustic or vibration signatures
- G-code etc.



Anomaly Detection Baselines

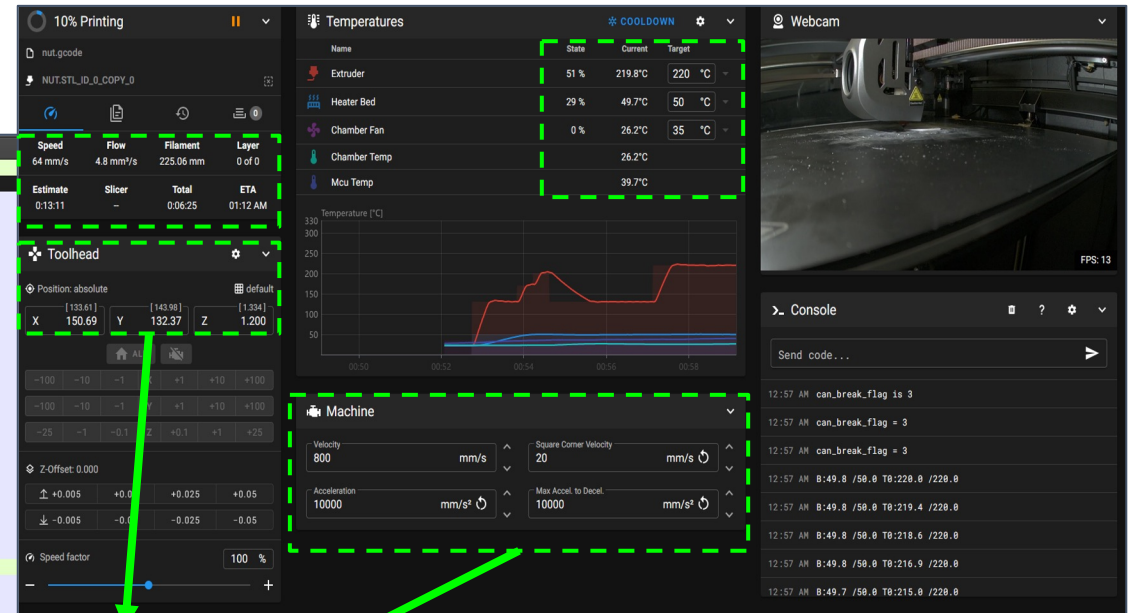


Anomaly Detection from System Logs

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.62	192.168.0.77	TCP	128	8080 → 54502 [PSH, ACK] Seq=1 Ack=1 Win=946 Len=74
2	0.000946	192.168.0.62	192.168.0.77	TCP	2974	8080 → 54502 [ACK] Seq=75 Ack=1 Win=946 Len=2920
3	0.000971	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=2995 Win=1023 Len=0
4	0.012674	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=2995 Ack=1 Win=946 Len=1460
5	0.012674	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=4455 Ack=1 Win=946 Len=1460
6	0.012674	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=5915 Ack=1 Win=946 Len=1460
7	0.012674	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=7375 Ack=1 Win=946 Len=1460
8	0.012713	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=8835 Win=1023 Len=0
9	0.017452	192.168.0.62	192.168.0.77	TCP	38014	8080 → 54502 [ACK] Seq=8835 Ack=1 Win=946 Len=37960
10	0.017491	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=46795 Win=1023 Len=0
11	0.021606	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=46795 Ack=1 Win=946 Len=1460
12	0.021606	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=48255 Ack=1 Win=946 Len=1460
13	0.021606	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=49715 Ack=1 Win=946 Len=1460
14	0.021629	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=51175 Win=1023 Len=0
15	0.022761	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=51175 Ack=1 Win=946 Len=1460
16	0.022761	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=52635 Ack=1 Win=946 Len=1460
17	0.022761	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=54095 Ack=1 Win=946 Len=1460
18	0.022761	192.168.0.62	192.168.0.77	TCP	1514	8080 → 54502 [ACK] Seq=55555 Ack=1 Win=946 Len=1460
19	0.022772	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=57015 Win=1023 Len=0
20	0.024603	192.168.0.62	192.168.0.77	TCP	10274	8080 → 54502 [ACK] Seq=57015 Ack=1 Win=946 Len=10220
21	0.024603	20.150.179.224	192.168.0.77	TCP	60	443 → 54124 [ACK] Seq=1 Ack=1 Win=501 Len=0
22	0.024603	20.150.179.224	192.168.0.77	TLSv1.2	87	Application Data
23	0.024603	192.168.0.62	192.168.0.77	TCP	10274	8080 → 54502 [ACK] Seq=67235 Ack=1 Win=946 Len=10220
24	0.024603	192.168.0.62	192.168.0.77	TCP	193	8080 → 54502 [PSH, ACK] Seq=77455 Ack=1 Win=946 Len=139
25	0.024649	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=77594 Win=1023 Len=0
26	0.063859	192.168.0.62	192.168.0.77	TCP	128	8080 → 54502 [PSH, ACK] Seq=77594 Ack=1 Win=946 Len=74
27	0.063892	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=77668 Win=1023 Len=0
28	0.065807	192.168.0.62	192.168.0.77	TCP	2974	8080 → 54502 [ACK] Seq=77668 Ack=1 Win=946 Len=2920
29	0.065828	192.168.0.77	192.168.0.62	TCP	54	54502 → 8080 [ACK] Seq=1 Ack=80588 Win=1023 Len=0

```
Frame 2: 2974 bytes on wire (23792 bits), 2974 bytes captured (23792 bits) on interface \Device\NPF...
Ethernet II, Src: fc:ee:28:07:32:ed (fc:ee:28:07:32:ed), Dst: Intel_9c:83:30 (a0:b3:39:9c:83:30)
  Destination: Intel_9c:83:30 (a0:b3:39:9c:83:30)
  Source: fc:ee:28:07:32:ed (fc:ee:28:07:32:ed)
  Type: IPv4 (0x0800)
  [Stream index: 0]
  Internet Protocol Version 4, Src: 192.168.0.62, Dst: 192.168.0.77
  Transmission Control Protocol, Src Port: 8080, Dst Port: 54502, Seq: 75, Ack: 1, Len: 2920
    Source Port: 8080
    Destination Port: 54502
    [Stream index: 0]
    [Stream Packet Number: 2]
    [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 2920]
    Sequence Number: 75 (relative sequence number)
    Sequence Number (raw): 1338224668
    [Next Sequence Number: 2995 (relative sequence number)]
    Acknowledgment Number: 1 (relative ack number)
    Acknowledgment number (raw): 1274239089
    0101 .... = Header Length: 20 bytes (5)
    Flags: 0x010 (ACK)
    Window: 946
    [Calculated window size: 946]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x0000 [unverified]
    [Checksum Status: Unverified]
```

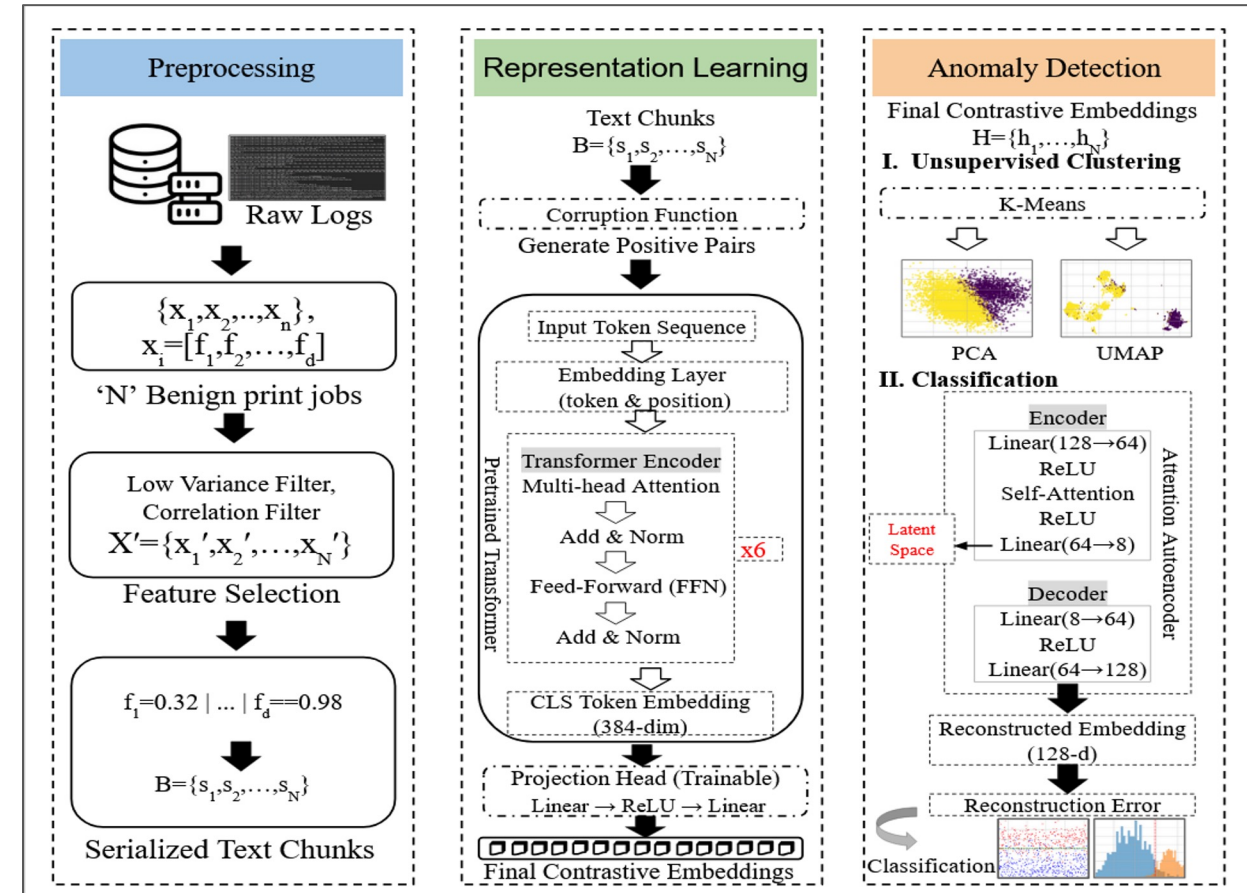
```
0000 a0 b3 39 9c 83 30 fc ee 28 07 32 ed 08 00 45 00 ..9..0..(2..E..
0010 0b 90 aa 93 40 00 00 06 02 f9 c0 a8 00 3e c0 a8 .....@.....
0020 00 4d 1f 90 d4 e6 4f c3 b0 1c 4b f3 58 71 50 10 ..M...0...K.XqP..
0030 03 b2 00 00 00 00 ff d8 ff e0 00 10 4a 46 49 46 ...b2000000ff d8 ff e0 00 10 4a 46 49 46 .....JFIF
0040 00 01 01 00 00 01 00 01 00 00 ff fe 00 05 00 00 ...00010000010000 ff fe 00 05 00 00 .....C.....
0050 00 ff db 00 43 00 06 04 05 06 05 04 06 06 05 06 ...ff db 00 43 00 06 04 05 06 05 04 06 06 05 06 .....
0060 07 07 06 08 0a 10 0a 0a 09 09 0a 14 0e 0f 0c 10 ...7706080a100a0a09090a140e0f0c10 .....%..#..
0070 17 14 18 18 17 14 16 16 1a 1d 25 1f 1a 1b 23 1c ...17141818171416161a1d251f1a1b231c .....%..#..
0080 16 16 20 2c 20 23 26 27 29 2a 29 1f 2d 30 2d ...1616202c20232627292a291f2d302d .....%..#..
0090 28 30 25 28 29 28 ff fe 00 05 00 00 ff db 00 ...283025282928ff fe 00 05 00 00 ff db 00 .....(0x())(.....
00a0 43 01 07 07 0a 08 0a 13 0a 0a 13 28 1a 16 1a ...430107070a080a130a0a13281a161a .....C.....
00b0 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 ...28282828282828282828282828282828 .....
00c0 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 ...28282828282828282828282828282828 .....
00d0 28 28 28 28 28 28 28 28 28 28 28 28 28 28 28 ...28282828282828282828282828282828 .....
00e0 28 28 ff c0 00 11 08 02 d0 05 00 03 01 22 00 02 ...2828ffc000110802d005000301220002 .....
00f0 11 01 03 11 01 ff c4 00 1f 00 00 01 05 01 01 01 ...1101031101ffc4001f00000105010101 .....
0100 01 01 01 00 00 00 00 00 00 00 01 02 03 04 05 ...01010100000000000000000102030405 .....
0110 06 07 08 09 0a 0b ff fe 00 05 00 00 ff c4 00 ...060708090a0bff fe 00 05 00 00 ff c4 00 .....
0120 b5 10 00 02 01 03 03 02 04 03 05 05 04 04 00 00 ...b5100002010303020403050504040000 .....
0130 01 7d 01 02 03 00 04 11 05 12 21 31 41 06 13 51 ...017d0102030004110512213141061351 .....}.....1A..Q
0140 61 07 22 71 14 32 81 91 a1 08 23 42 b1 c1 15 52 ...6107227114328191a1082342b1c11552 ...a"q2...B..R
0150 d1 f0 24 33 62 72 82 09 0a 16 17 18 19 1a 25 26 ...d1f02433627282090a161718191a2526 ...$br...%
0160 27 28 29 2a 34 35 36 37 38 39 3a 43 44 45 46 47 ...2728292a3435363738393a4344454647 ...()*456789:CDEF
0170 48 49 4a 53 54 55 56 57 58 59 5a 63 64 65 66 67 ...48494a535455565758595a6364656667 HIJSTUVW XYZcdefg
0180 68 69 6a 73 74 75 76 77 78 79 7a 83 84 85 86 87 ...68696a737475767778797a8384858687 hijstuvw xyz ....
0190 88 89 8a 92 93 94 95 96 97 98 99 9a a2 a3 a4 a5 ...88898a92939495969798999a a2 a3 a4 a5 .....
```



Anomaly Detection from System Logs

- Under-extrusion / Over-extrusion (extrusion multiplier changes)
- Noisy G-code injection (random hops / travel inserts)
- Dimensionality change (scale / offset edits)
- Internal cavity insertion (insert internal void prints)

Class Type	Attack Category	Samples
Benign	-	98,720
Attack	Under-extrusion	10120
	Over-extrusion	9950
	Noise Injection	15456
	Dimensional Change	9324
	Cavity Insertion	10521

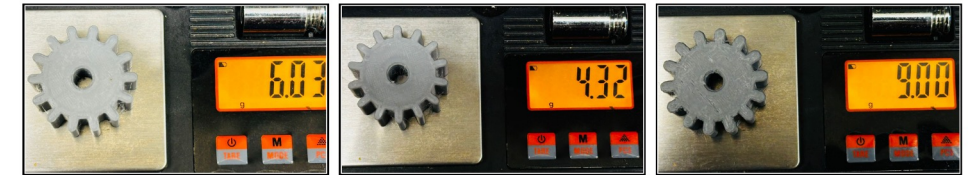


Anomaly Detection Performance

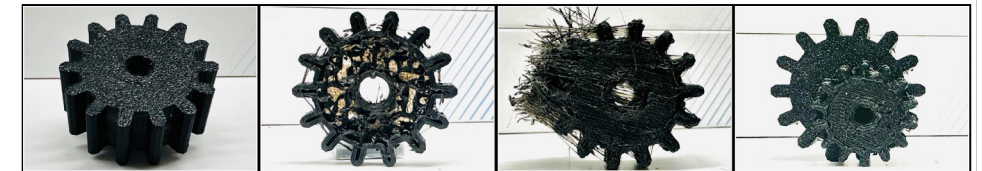
Metric	Benign		Attack	
	Value	(%)	Value	(%)
Precision	0.9801	98.01%	0.9055	90.55%
Recall	0.9499	94.99%	0.9614	96.14%
F1-score	0.9648	96.48%	0.9326	93.26%
Overall Accuracy		0.9537 (95.37%)		
Macro Avg F1-score		0.9487 (94.87%)		
Weighted Avg F1-score		0.9541 (95.41%)		
AUROC (AUC)		0.9870 (98.70%)		
Threshold (MSE)		0.0019		



(a) Benign. (b) Cavity Ins. (c) Noise Inj. (d) Dimension Inj.



(e) Benign Extrusion (f) Under-Extrusion (g) Over-Extrusion



(a) Benign. (b) Cavity Ins. (c) Noise Inj. (d) Dimension Inj.



(e) Benign Extrusion (f) Under-Extrusion (g) Over-Extrusion



CONCLUSION

- Quality of AM parts → RG4
 - Anomaly identification → RG2
 - Data safety → RG2 and RG3
 - Teaching and workforce → EWD1 and EWD2
- 