ASME IDETC-CIE 2026
INTERNATIONAL DESIGN ENGINEERING TECHNICAL CONFERENCES
& COMPUTERS AND INFORMATION IN ENGINEERING CONFERENCE

LIGHTWEIGHT MULTIMODAL FUSION FOR REAL-TIME CYBERSECURITY OF OPTICAL AND THERMAL IN-SITU MONITORING SIGNALS IN METAL ADDITIVE MANUFACTURING

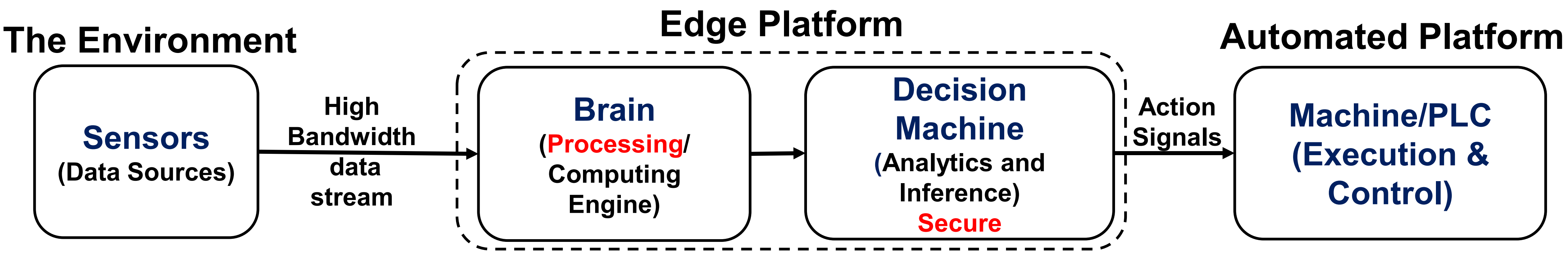
Nishant Chinnasami[1], Rye Stahle-Smith[1], Zaki Bushiri[1], Mumin Adhami[2], Austin R. J. Downey[2], Lang Yang[2] and **Rasha Karakchi[1]**

Department of Computer Science and Engineering[1]
Department of Mechanical Engineering[2]

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Edge-Class Computing Platforms in Manufacturing Systems

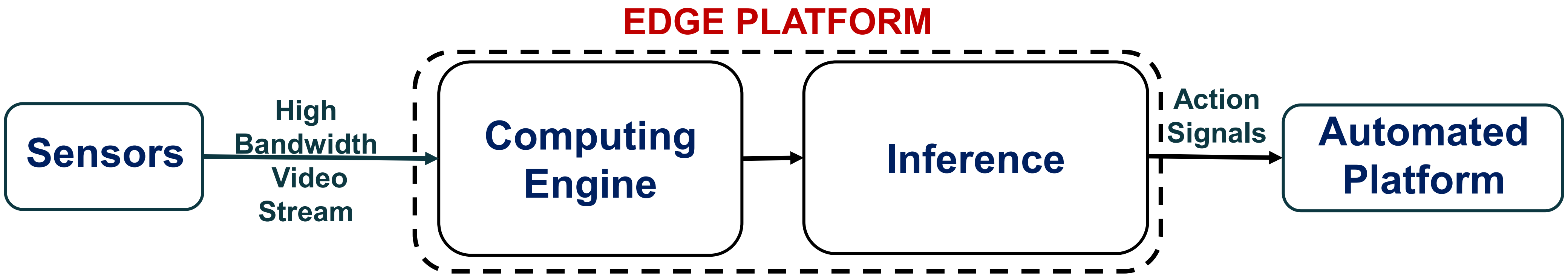
Edge Platforms: Acquire, Process and Secure High-Bandwidth Sensor Streams



Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Edge Platform

Edge platform consists of two main components:
Computing Engine and Inference/Analysis Engine



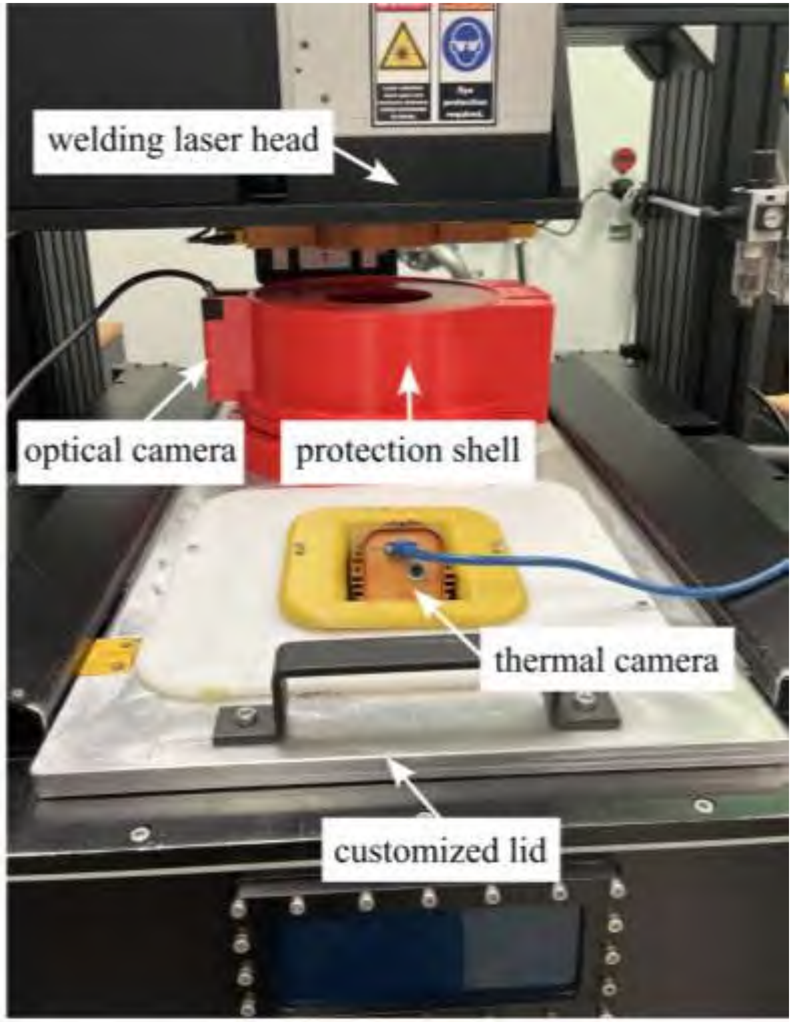
Edge Makes Decision Locally & Enable Real-Time Protection

EXAMPLE: BATTERY TAB LASER WELDING

- **In-Situ Thermal Camera**
- Monitors the weld region during laser welding

- **Process Monitoring**
- Captures melt-pool behavior, heat distribution and cooling response

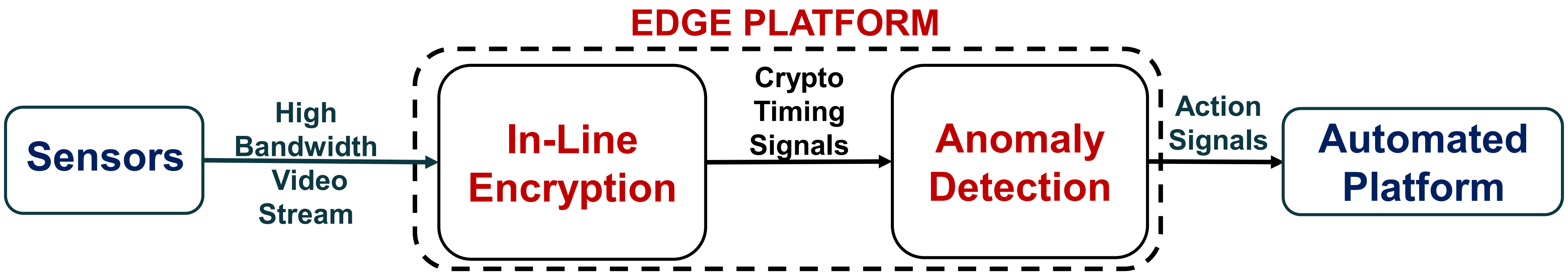
- **Quality Assessment**
- Thermal features can support weld-quality classification



Experimental setup for in-situ optical and thermal monitoring of battery-tab laser welding (Hoang et al.)

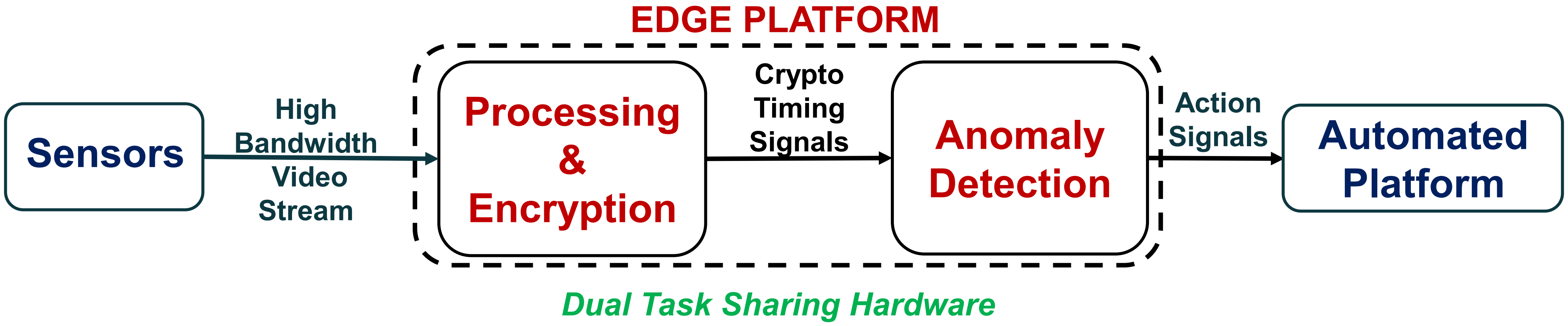
Edge Platform for Monitoring and Security: Advantage

Performing encryption and anomaly detection directly at the edge **reduces latency, preserves data privacy, and enables rapid mitigation of defects** before the next layer printed



Edge Platform for Monitoring and Security: Disadvantage

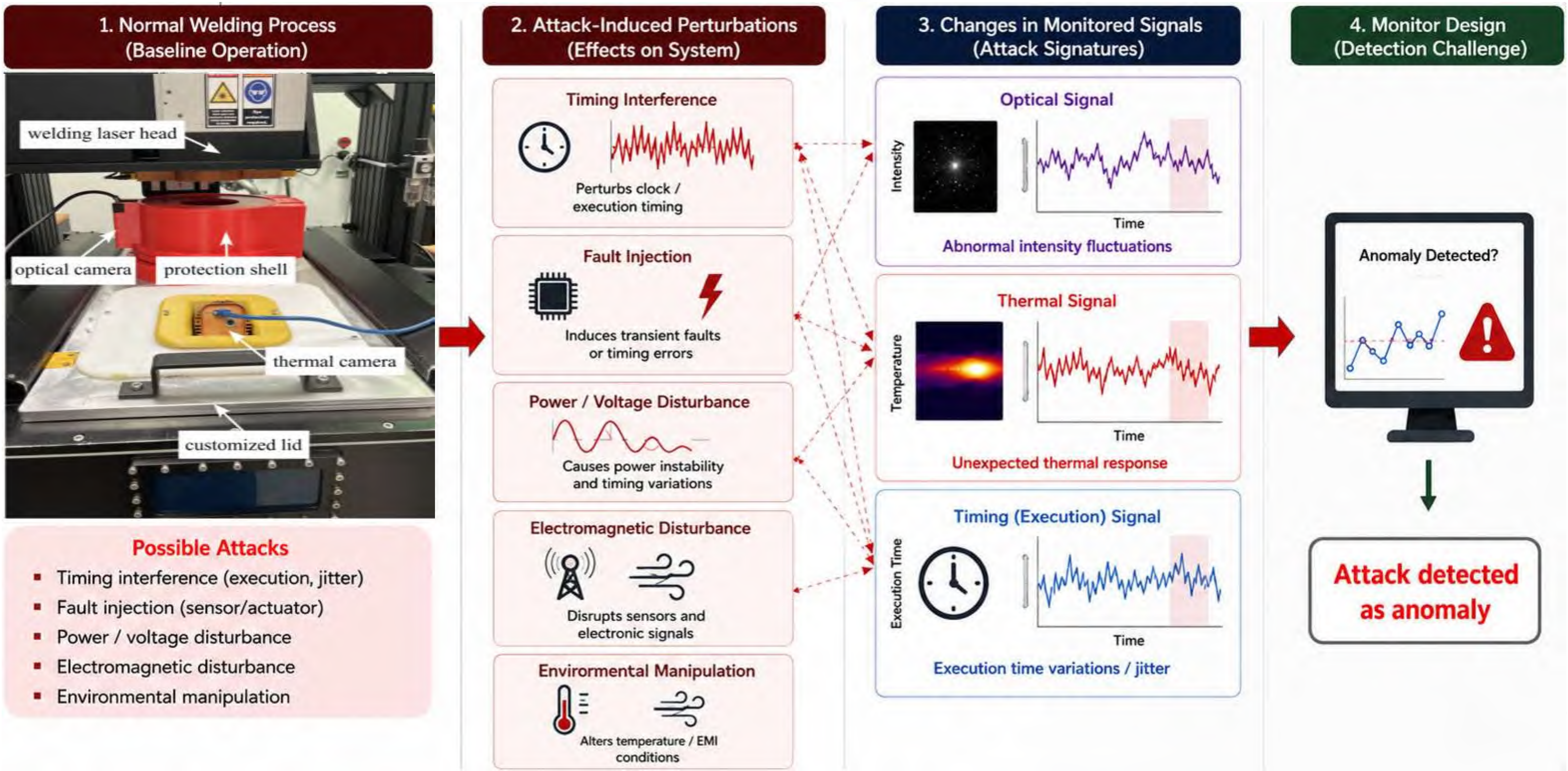
Embedding security into process monitoring create a key challenge:
Normal process variations and cyber manipulation can produce indistinguishable signatures in monitored signals.



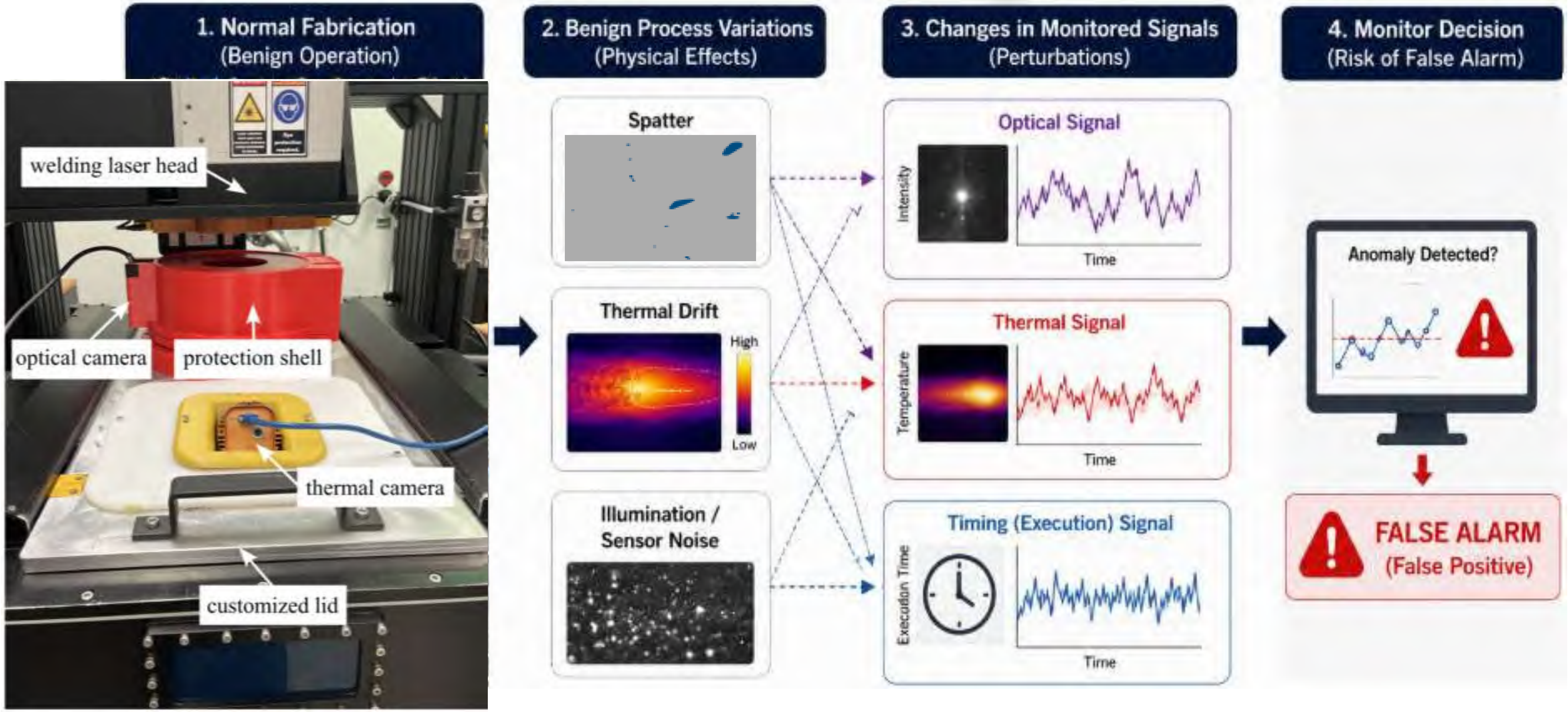
Shared Edge Hardware Creates a Noise-vs.-Attack Detection Challenge

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Attack/Malicious Manipulation Scenario



Normal Process Variation (Noise) in Manufacturing



Normal process variations can perturb monitored signals and be misclassified as anomalies

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Prior Work

Prior work is effective but either resource-intensive or too dependent on timing, creating ambiguity between normal process variations and attacks.

Approach	Method	Strength / Purpose	Main Limitation
Traditional Methods (Protection)	Constant-time implementation	Prevents timing leakage	Performance & implementation overhead
	Shielding	Protects against physical/EM interference	Added cost & hardware complexity
	Hardware redundancy	Detects/tolerates injected faults	High area & power overhead
Timing-Only Monitoring	Runtime timing analysis	Lightweight & real-time	Cannot distinguish process variations from attacks

Research Gap: Lightweight monitoring is needed that can distinguish **benign process variations** from **malicious perturbations**.

What We Propose:

Multimodal Process-Aware Monitoring

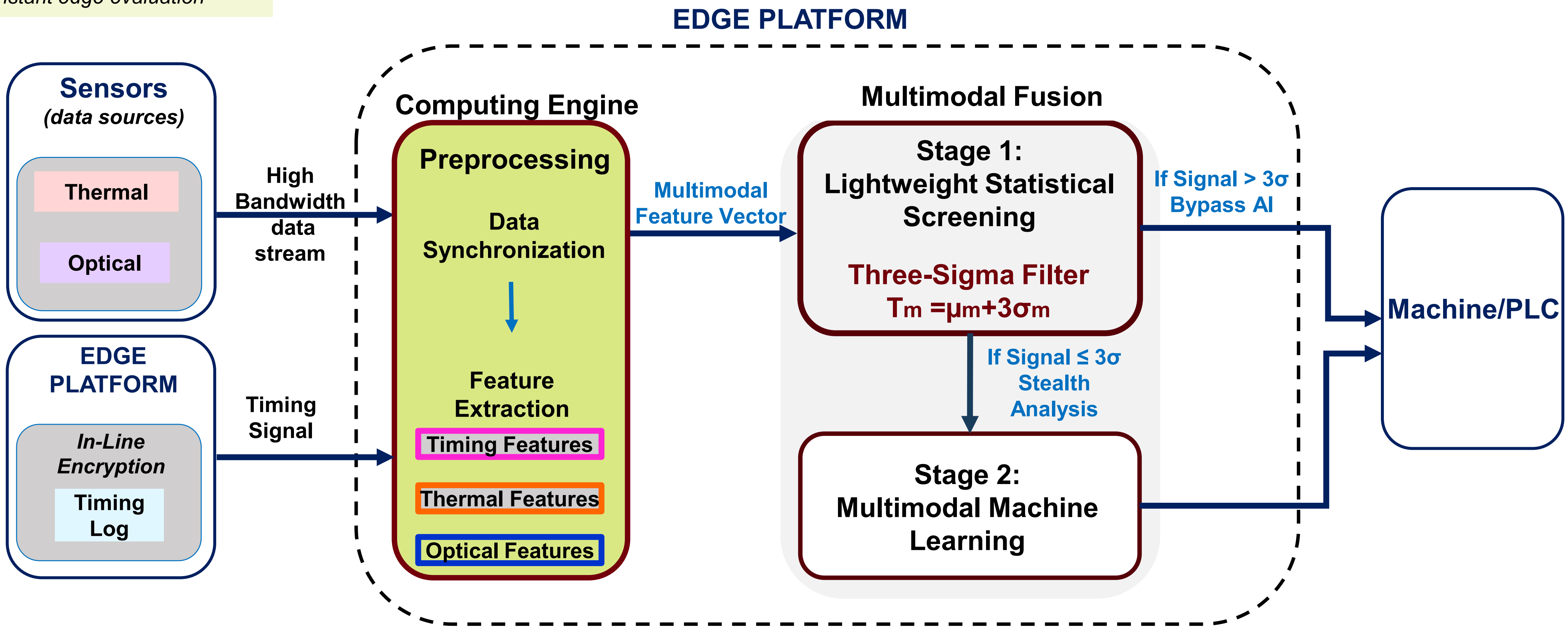
Feature	Our Approach
Multimodal sensing	Timing + Optical + Thermal
Process awareness	Captures physical process context
Detection	Statistical + lightweight ML
Edge deployment	Low-latency, deterministic monitoring
Goal	Distinguish benign process variations from malicious attacks

Move beyond timing-only monitoring by incorporating physical process context.

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Proposed Multimodal Process-Aware Monitoring Framework

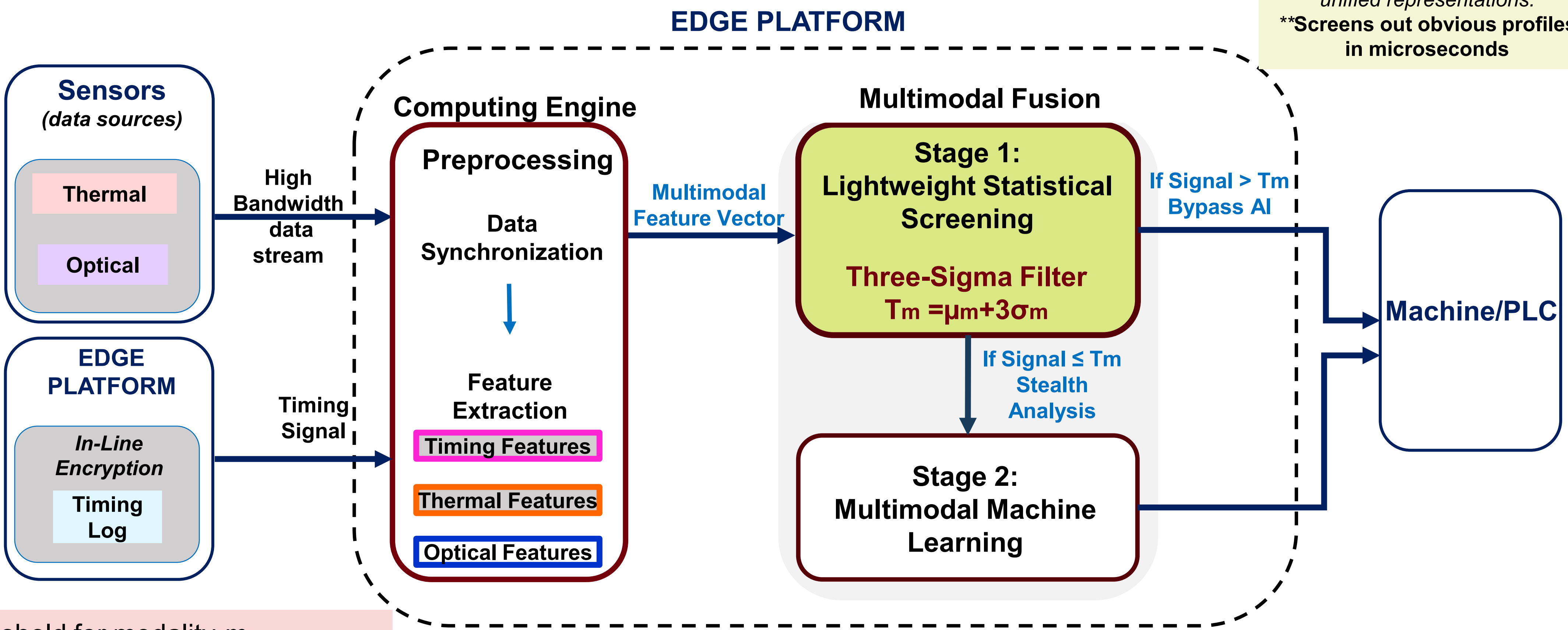
Aligns inputs using shared microsecond timestamps, and compresses them into a lightweight three-element feature vector suitable for instant edge evaluation



Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Proposed Multimodal Process-Aware Monitoring Framework

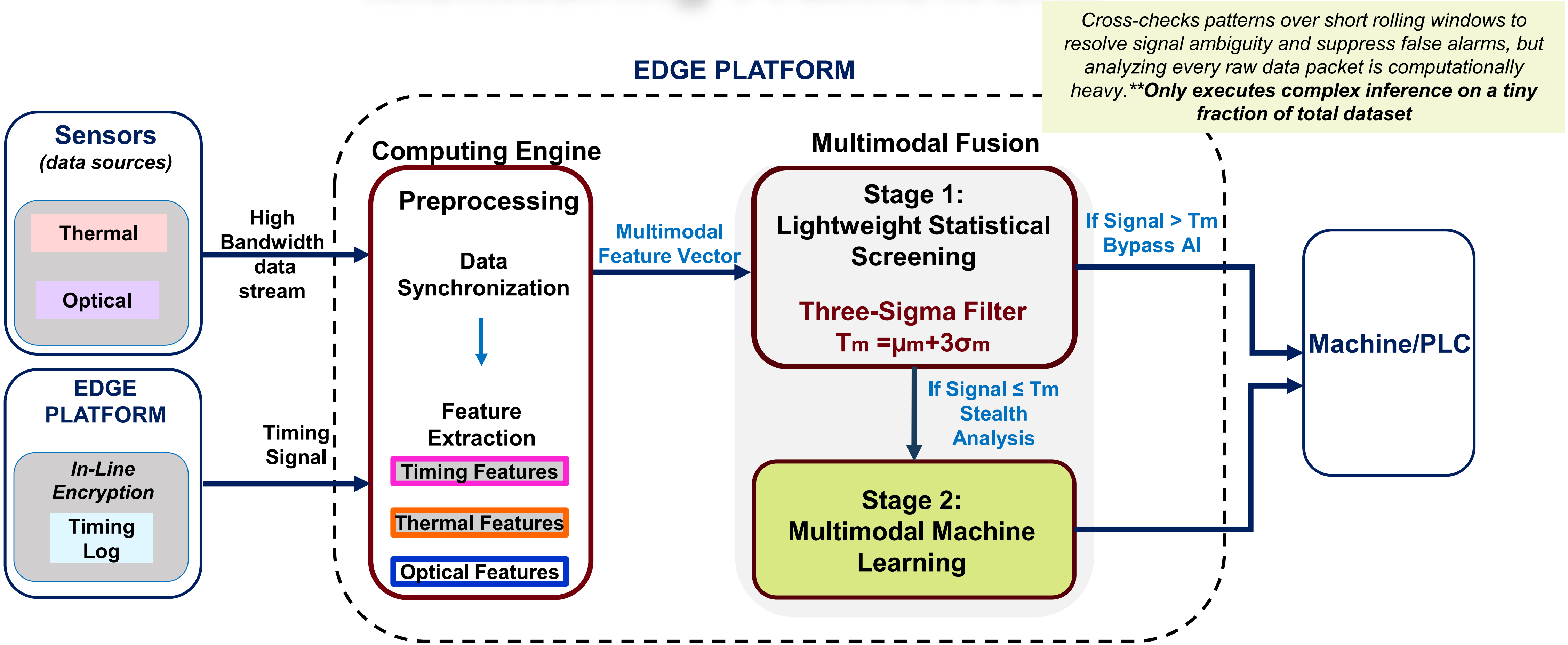
Combines timing, thermal and optical features to form rich unified representations.
****Screens out obvious profiles in microseconds**



T_m – Threshold for modality *m*
μ_m – Mean value for modality *m*
σ_m – Standard deviation for modality *m*
m – Modality index (time, therm, etc.)

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Proposed Multimodal Process-Aware Monitoring Framework



Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Evaluation

- **Objective**
  - Compare timing-only and multimodal monitoring for distinguishing normal process variability from malicious anomalies.
- **Dataset**
  - 12 manufacturing datasets containing synchronized timing, thermal, and optical measurements.
  - Datasets span different materials, welding conditions, and data volumes.
  - Data collected under controlled fabrication conditions.
- **Data Modalities**
  - **Timing:** execution-time / timing traces from the embedded platform.
  - **Thermal:** infrared measurements of the melt-pool / process region.
  - **Optical:** process images capturing melt-pool and surface behavior.
- **Dataset Categories**
  - Normal process operation
  - Benign process variations
    (e.g., spatter, thermal fluctuations, illumination/sensor noise)
  - Malicious / attack-induced perturbations

Evaluation Dataset

12 datasets spanning different materials, weld conditions, and data volumes were used to evaluate accuracy, latency, and throughput.

Dataset Group	Examples	Size Range
Welding	Tab Welding, Laser Welds, Weld 01/02	0.54–100.59 MB
Steel	Steel No Glass 1/2, Thermal Test Weld Steel 1/2	3.48–115.47 MB
Aluminum	Thermal Test Weld Aluminum	125.17 MB
Battery	Battery Tab Weld	52.60 MB
Other Tests	Test Weld Recording, Filter Weld 2	0.54–96.62 MB

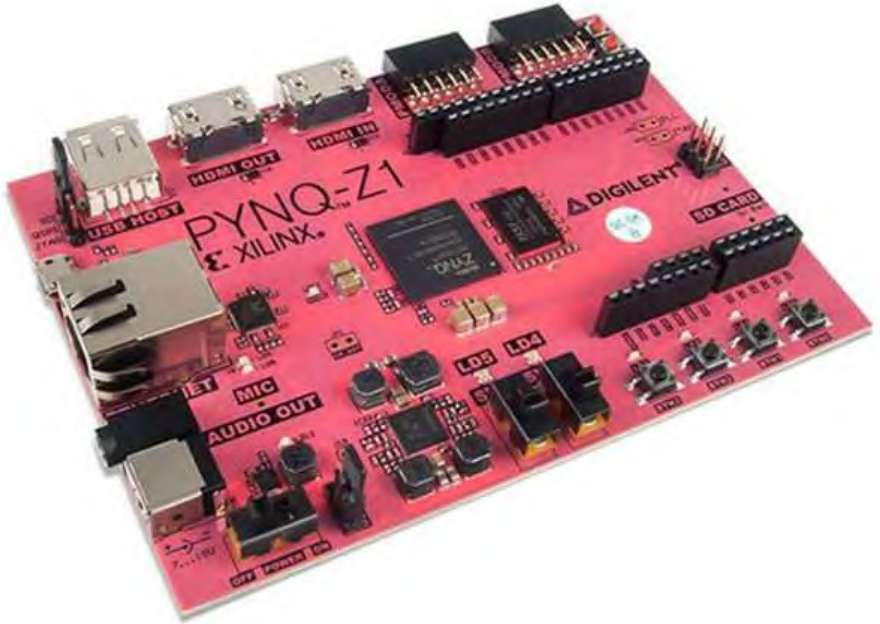
Experimental datasets provided by the ARTS Laboratory, University of South Carolina.
In-Situ Monitoring of Powder Bed Fusion Additive Manufacturing dataset repository
github.com/ARTS-Laboratory/In-situ-monitoring-of-powder-bed-fusion-additive-manufacturing

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Hardware Deployment Specification

Processor & Hardware Architecture

- Target Platform: PYNQ-Z2 edge development board.
- Evaluation CPU: Embedded ARM Cortex-A9 processor.
- Hardware Fabric: Programmable Logic (FPGA) fabric co-processor.
- Clock Frequency: Constrained at a stable 100 MHz.
- Total LUTs: 53,200
- Total FFs: 106,400
- Total BRAMs: 4.9 Mbits
- Total DSP Slices: 220 MAC



Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Evaluation on Traditional Embedded CPU

-36% Latency Reduction

Metric	Timing-Only	Full Hybrid (Optical + Thermal + Timing)
Accuracy	~99.9%	~99.9%
Inference Latency	**~1.42 ms**	**~0.91 ms**
Throughput	Dataset-dependent	Comparable / slightly higher
Multimodal Context	No	Yes
Process-Aware Detection	Limited	Improved

Timing-only: CPU must run heavy ML inference on **100% of packets** to check for leaks.
Full Hybrid: Stage 1 gatekeeper: Uses fast, constant-time statistics across all channels.
Short-circuit evaluation: Massive anomalies bypass Stage 2 (ML) instantly, saving CPU cycles.

Confusion Matrix Comparison

The hybrid fusion model eliminates false negatives across all evaluated datasets, improving anomaly sensitivity, but introduces a higher false-positive rate in some cases.

Metric	Timing-Only	Full Hybrid (O + T + Time)	Observation
False Negatives (FN)	43	**0**	No missed anomalies
False Positives (FP)	23	**58**	More conservative detection
True Negatives (TN)	High	**Higher**	Strong normal-case recognition
True Positives (TP)	High	**High**	Maintains strong attack detection

Localized Thermal Drift Anomalies

94% of Excess FPs Confined to Only 2 Datasets

Dataset	Timing-Only FP	Hybrid FP
Thermal Test Weld Steel 1	2	23
Thermal Test Weld Steel 2	1	15

- Thermal welding signals naturally vary because of temperature changes and cooling cycles.
- Stage 1 quickly detects deviations across data channels.
- In volatile thermal-steel data, normal shifts may be flagged as anomalies, causing false positives before ML analysis

Hardware Deployment Results

Metric	Result	Significance
FPGA LUT Utilization	155 LUTs (0.29%)	Very compact hardware footprint
Flip-Flop Utilization	129 FFs (0.12%)	Minimal logic overhead
FPGA Clock	100 MHz	Deterministic operation
FPGA Latency	10 ns/block	1 block/cycle
HW Throughput	1600 MB/s	Theoretical high-throughput processing
Measured ARM Inference	897–933 μs/block	Software/I/O overhead
Memory Usage	9.60–9.79 MB	Low and stable
Power	0.141 W total	Low power for continuous edge operation
Dynamic Power	0.036 W	Low processing overhead

The system performs real-time edge inference in under **1 ms per block** while using less than **10 MB of memory**. FPGA processing reaches **1600 MB/s**, far exceeding ARM throughput.

Edge Runtime Performance

Metric	Result
Inference Latency	897–933 µs/block
Total Processing Time per Dataset	24.98–25.79 s
ARM Throughput	0.04–9.27 MB/s
FPGA Throughput	1600 MB/s
Memory Usage	9.60–9.79 MB

- The system performs real-time edge inference in under **1 ms per block** while using less than **10 MB of memory**.
- FPGA processing reaches **1600 MB/s**, far exceeding ARM throughput.

Conclusion

❖ **Multimodal monitoring improves process awareness**

Combined **timing, optical, and thermal signals** provide richer process context than timing-only monitoring.

❖ **Lightweight fusion enables real-time edge monitoring**

The hybrid approach maintained **~99.9% accuracy** while reducing inference latency from **1.42 ms to 0.91 ms (~36%)**.

❖ **Physical context improves anomaly sensitivity**

The hybrid detector reduced **false negatives from 43 to 0 but** increased false positives in some thermally variable datasets.

Cybersecurity monitoring in manufacturing should consider both cyber signals and physical process behavior.

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA

Future Work

- **Reduce false positives** under sustained thermal/process variation.
- **Expand multimodal datasets** and process conditions.
- **Further optimize edge implementation** for practical real-time deployment

Thank You!

Author Information

Name: Dr. Rasha Karakchi

Email: karakchi@cec.sc.edu

GitHub: github.com/Karakchi-Research

Molinaroli College of Engineering and Computing
UNIVERSITY OF SOUTH CAROLINA