Proactive Failure Prediction in Embedded Systems Using Lightweight Anomaly Detection

Team Information

Team Name: — (Individual Project)

Team Member: Ahmed Elsheikh

Affiliation: Program of Computer Science | Egypt–Japan University of Science and Technology (E-JUST), Egypt

Contact Information: Email: ahmed.elsheikh@ejust.edu.eg

Problem Statement

Embedded systems are widely deployed in safety-critical and industrial environments where unexpected failures can lead to system downtime, safety risks, and increased maintenance costs. In many real-world deployments, system health monitoring relies on fixed thresholds applied to individual signals such as temperature, CPU utilization, or execution time. While simple to implement, these threshold-based approaches typically detect failures only after critical operating limits have already been exceeded.

In practice, failures in embedded systems rarely occur instantaneously. They are often preceded by gradual performance degradation caused by sustained workload, thermal stress, power instability, or scheduling delays. These early warning signs are subtle and may remain within nominal limits, making them difficult to detect using conventional monitoring techniques. As a result, existing methods lack the ability to identify degradation trends early enough to enable proactive intervention. There is therefore a need for a lightweight and realistic approach that can detect abnormal system behavior before a critical failure occurs, while remaining suitable for resource-constrained embedded platforms.

Objectives

- To develop a hardware-aware simulation that realistically models embedded system runtime behavior under normal operation, degradation, and failure conditions.
- To generate representative time-series data capturing both raw hardware signals and temporal degradation patterns.
- To design a lightweight anomaly detection pipeline suitable for resource-constrained embedded platforms.
- To train an anomaly detection model exclusively on normal operation data, without relying on failure labels.
- To demonstrate proactive failure prediction by detecting degradation trends before the onset of critical system failure.

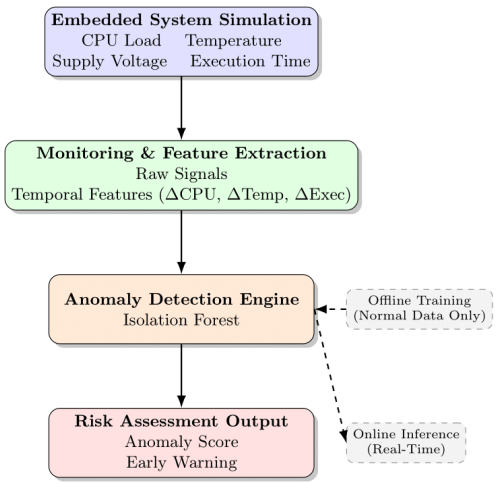
Proposed Solution

The proposed solution introduces a lightweight anomaly detection framework for proactive failure prediction in embedded systems. A hardware-aware runtime simulation is used to generate realistic time-series data reflecting normal operation, degradation, and failure behavior.

Raw signals and temporal features capturing rates of change are extracted and analyzed using an Isolation Forest model trained exclusively on normal operation data. During online inference, the model produces an anomaly score that reflects deviation from learned normal behavior, enabling early detection of degradation trends.

System Design

The proposed system is designed as a modular pipeline that enables proactive failure prediction through continuous monitoring and anomaly detection. The design consists of three main layers: system behavior simulation, monitoring and feature extraction, and anomaly-based decision making.



At the first layer, a hardware-aware runtime simulation models realistic embedded system behavior, including CPU load variation, thermal dynamics, supply voltage instability, and task execution timing. This layer serves as a controlled environment for generating representative operational data.

The second layer performs online monitoring and feature extraction. Raw hardware signals are collected periodically, and temporal features capturing rates of change are computed to highlight system dynamics and early degradation trends.

At the final layer, a lightweight anomaly detection engine based on Isolation Forest analyzes the extracted features. The model is trained offline using only normal operation data and deployed for online inference to produce a continuous anomaly score. This score represents the system's deviation from learned normal behavior and can be used to trigger early warnings or proactive recovery actions.

Methodology

The project is conducted through a sequence of well-defined phases, starting from system modeling and ending with performance evaluation.

First, a hardware-aware runtime simulation is designed to model realistic embedded system behavior under normal operation, degradation, and failure conditions. This phase focuses on capturing key physical and computational constraints such as thermal inertia, voltage instability, and task execution variability.

Next, the simulation is used to generate time-series data, which is periodically sampled to emulate real-time system monitoring. Both raw hardware signals and temporal features capturing rates of change are extracted to represent system dynamics and early degradation trends.

In the third phase, a lightweight anomaly detection model based on Isolation Forest is implemented using Python and scikit-learn. The model is trained offline using only normal operation data to learn baseline behavior, without relying on failure labels.

Finally, the trained model is evaluated on the full operational timeline. Anomaly scores are analyzed and visualized to assess the model's ability to detect degradation trends prior to critical failure.

Tools and Software

1. Python
2. NumPy and Pandas for data generation and processing
3. scikit-learn for anomaly detection
4. Matplotlib for visualization
5. Jolib for model export

Table 1. Dataset Description

Item	Description
Data Type	Time-series
Number of Samples	~1500
Sampling Strategy	Periodic sampling
Raw Features	CPU Load, System Temperature, Supply Voltage, Task Execution Time
Temporal Features	ΔCPU Load, ΔTemperature, ΔExecution Time
Operating Phases	Normal Operation, Gradual Degradation, Failure
Failure Labels	Used for evaluation and visualization only
Data Source	Hardware-aware runtime simulation

Expected Results

- The anomaly detection model is expected to maintain a stable anomaly score during normal system operation, indicating successful learning of baseline behavior.
- As the system transitions into the degradation phase, the anomaly score is expected to rise gradually, reflecting early deviation from normal operating conditions.
- This increase is expected to occur before individual hardware signals exceed critical thresholds, demonstrating proactive rather than reactive detection.
- During failure conditions, the anomaly score is expected to remain consistently high, confirming severe system deviation.

Overall, the results are expected to validate that combining hardware-aware simulation with temporal feature extraction enables early identification of degradation trends in embedded systems.

Challenges and Mitigation

Challenge 1: Limited availability of labeled failure data

Failures in embedded systems are rare and often poorly labeled, making supervised learning impractical.

Mitigation: An unsupervised anomaly detection approach is adopted, with the model trained exclusively on normal operation data.

Challenge 2: Unrealistic or overly simplified system behavior in simulations

Synthetic data can lack physical realism if not carefully designed.

Mitigation: A hardware-aware simulation is developed that incorporates physical constraints such as thermal inertia, voltage sag, and execution-time variability, along with micro-recovery events.

Challenge 3: Late detection using threshold-based monitoring

Fixed thresholds often react only after critical limits are exceeded.

Mitigation: Temporal features capturing rates of change are used to identify degradation trends before threshold violations occur.

Challenge 4: Suitability for resource-constrained embedded platforms

Complex models may be infeasible for embedded deployment.

Mitigation: A lightweight Isolation Forest model is selected due to its low computational complexity and efficient inference.

References

Susto, G. A., Beghi, A., & De Luca, C. (2015).
A predictive maintenance system for industrial machinery based on machine learning. *IEEE Transactions on Industrial Informatics, 11*(3), 804–814.
https://doi.org/10.1109/TII.2014.2349359

Zonta, T., da Costa, C. A., da Rosa Righi, R., de Lima, M. J., da Trindade, E. S., & Li, G. P. (2020).
Predictive maintenance in the Industry 4.0: A systematic literature review. *Computers & Industrial Engineering, 150*, 106889.
https://doi.org/10.1016/j.cie.2020.106889