Proactive Failure Prediction in Embedded Systems Using Lightweight Anomaly Detection

Ahmed Elsheikh

CSIT Program, Egypt-Japan University of Science and Technology (E-JUST), New Borg El Arab, Alexandria, Egypt

ahmed.elsheikh@ejust.edu.eg

ABSTRACT

Embedded systems often experience abrupt failures that leave little opportunity for corrective action. Conventional monitoring techniques rely on fixed thresholds, which typically react only after critical limits have been exceeded. This work presents **a lightweight, proactive approach for early failure prediction in resource-constrained embedded systems using anomaly detection.**

A hardware-aware runtime simulation is developed to model realistic embedded system behavior, including CPU load variation, thermal dynamics, supply voltage instability, and task execution timing. In addition to raw signals, temporal features capturing rates of change are extracted to emphasize system dynamics and early degradation trends. An Isolation Forest model is **trained exclusively on normal operation data, without using failure labels,** to learn baseline system behavior.

Experimental results show that **the anomaly score begins to rise during the degradation phase, well before the system enters a critical failure state.** This demonstrates the ability of the proposed approach to anticipate failures proactively rather than react to them post hoc. The proposed method is lightweight, interpretable, and suitable for deployment in safety-critical embedded applications such as automotive control units and industrial controllers.

PROBLEM STATEMENT

Embedded systems are widely deployed in safety-critical and industrial environments where ***unexpected failures can lead to system downtime, safety risks, and high maintenance costs***. In many practical 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 methods typically detect failures only after critical operating limits have already been exceeded.

Moreover, **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 approaches.

As a result, existing methods lack the ability to identify degradation trends early enough to enable proactive intervention. There is 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.

System Overview

The proposed prototype consists of **a hardware-aware simulation and a lightweight anomaly detection pipeline designed to enable proactive failure prediction in embedde systems.**

The system models realistic runtime behavior of a resource-constrained embedded device, including CPU load variation, thermal dynamics, supply voltage instability, and task execution timing.

Runtime signals generated by the simulated embedded system are continuously monitored and processed by a feature extraction layer.

In addition to raw measurements, temporal features capturing rates of change are computed to emphasize system dynamics and early degradation trends. These features are then analyzed by a lightweight anomaly detection engine based on Isolation Forest.The anomaly detection model is trained offline using only normal operation data to learn baseline system behavior.

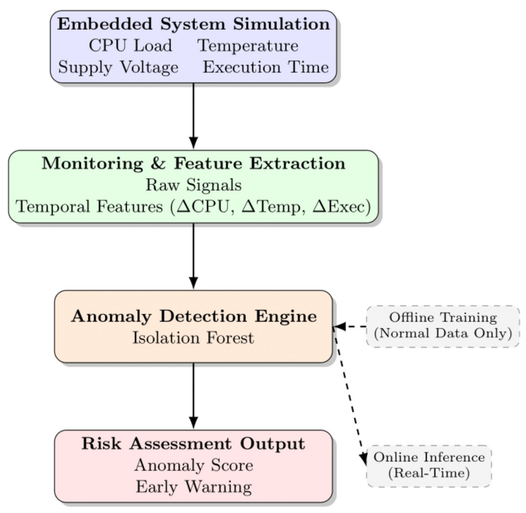

Figure 1. System architecture of the proposed prototype, illustrating runtime simulation, feature extraction, and anomaly detection.

During online inference, the model evaluates incoming system states and produces a continuous anomaly score that reflects deviation from normal behavior. This score can be used to ***trigger early warnings or proactive recovery actions before a critical failure occurs.***

Icon 1. GitHub Repo

Simulation & Data Generation

A controlled, hardware-aware runtime simulation is used to generate realistic ***time-series data*** representing embedded system operation. The simulation captures key system signals, including CPU load, system temperature, supply voltage, and task execution time, sampled periodically to emulate real-time monitoring.

Physical constraints are explicitly modeled, such as thermal inertia, voltage sag under high load, and execution time variability due to scheduling pressure. System behavior evolves across three overlapping operating phases: normal operation, gradual degradation, and failure. The degradation phase includes micro-recovery events, reflecting realistic system attempts to stabilize before failure.

The simulation generates a **time-series dataset of approximately 1,500 samples**, collected at a fixed sampling interval. Each sample contains ***four raw hardware signals*** and ***three temporal features capturing rates of change,*** extracted using smoothed derivatives to emphasize long-term degradation trends rather than transient noise. Failure labels are derived from multi-factor physical criteria and are used exclusively for evaluation and visualization, not during model training.

Anomaly Detection Approach

- An Isolation Forest model is selected due to its low computational complexity and suitability for resource-constrained environments.
- The model is trained offline using only normal operation data, without access to failure labels or degradation boundaries.
- Input features include both raw hardware signals and temporal features capturing system dynamics.
- During online inference, the trained model evaluates incoming system states and produces a continuous anomaly score.
- The approach enables proactive detection by identifying degradation trends before the onset of critical failure.

Results & Discussion

Figure 2 illustrates the evolution of the anomaly score over time. During normal operation, the score remains stable, indicating that the model has successfully learned baseline system behavior. As the system transitions into the degradation phase, the anomaly score begins to rise gradually, despite individual hardware signals still operating within acceptable limits. This behavior demonstrates the model's ability to capture early degradation trends rather than reacting to explicit failure events.

The anomaly score increases during degradation, prior to the onset of critical failure.

Peak anomaly values are observed before and throughout the failure state.

The model responds to system dynamics and temporal trends, not static threshold violations.

This confirms the proactive nature of the proposed failure prediction approach.

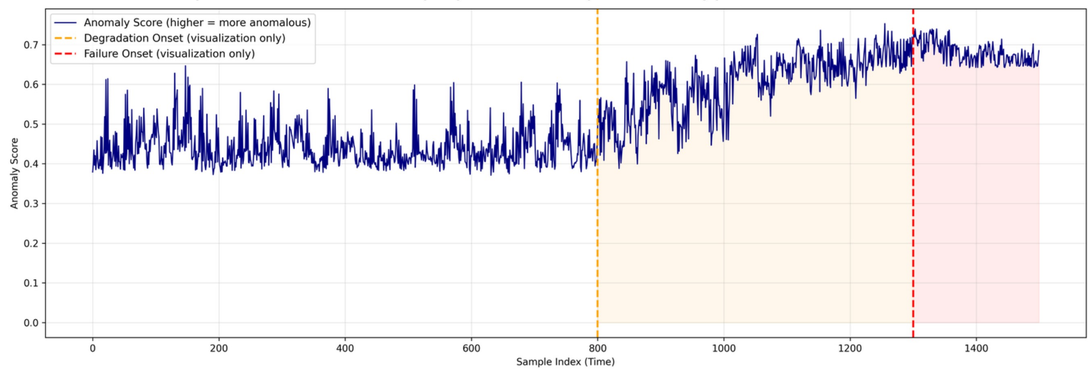

Figure 2. Anomaly score over time. The score begins to rise during the degradation phase, enabling early failure prediction before the onset of critical system failure.

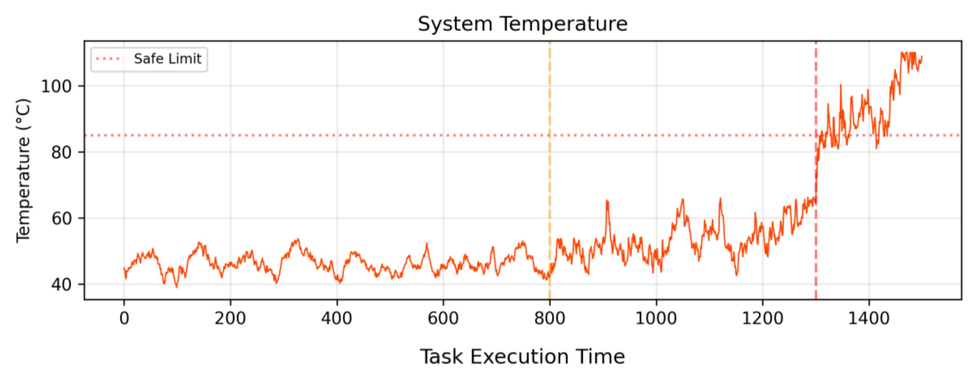

Figure 3. System temperature evolution showing gradual thermal degradation prior to failure.

Conclusion

This work demonstrates a lightweight and proactive approach for early failure prediction in embedded systems using anomaly detection. By combining hardware-aware simulation with temporal feature extraction, the proposed method identifies degradation trends before critical failure occurs. The approach is computationally efficient, does not rely on failure labels, and is well suited for deployment in resource-constrained and safety-critical embedded applications.

JAC-ECC 2025, Alexandria, Egypt, 15-17 December 2025