Project SHIELD: **S**mart **H**ardware **I**nspection for **E**arly **L**atency **D**etection

In 2018 and 2019, the Boeing 737 MAX crashes revealed a critical vulnerability in modern embedded systems: the catastrophic consequences of undetected sensor degradation. A single faulty angle-of-attack (AoA) sensor activated the MCAS flight control system erroneously, ultimately leading to fatal crashes. Similar failures have occurred in domains such as autonomous vehicles and medical devices, where sensor drift, delay, or calibration loss caused dangerous misjudgments. These incidents underscore an urgent need for systems capable of detecting sensor degradation before it results in failure.

Sensors are foundational to embedded systems, enabling accurate monitoring, feedback control, and autonomous behavior across aerospace, robotics, industrial automation, and healthcare. As embedded systems grow increasingly autonomous and safety-critical, the reliability of sensor data becomes mission-critical. Yet, most current systems depend on post-failure detection, threshold-triggered alerts, or costly redundancy—none of which provide early warnings necessary for preemptive mitigation. This research introduces **SHIELD: Smart Hardware Inspection for Early Latency Detection**, a novel framework that proactively monitors sensor behavior to forecast failures before they occur.

Motivation and Background

SHIELD is inspired by early-stage diagnostics in medicine, such as detecting cancer via blood biomarkers before symptoms arise. In a similar spirit, SHIELD continuously monitors statistical and temporal patterns in sensor outputs to detect early signs of degradation—bias drift, latency, elevated noise, or signal saturation—before system integrity is compromised. This allows operators to take preventive action such as mission reconfiguration, failover, recalibration, or maintenance scheduling.

The Problem SHIELD Solves

In many safety-critical applications, sensors represent a single point of failure. For example:

- A drifting IMU in a UAV can destabilize flight.
- A miscalibrated flow sensor in an infusion pump may overdose a patient.
- A stuck pressure sensor in aerospace systems can misguide control logic.

- Such failures often emerge gradually, yet no on-device mechanism currently exists to forecast their degradation in real time.

Limitations of existing approaches:

- **Redundancy** increases cost and power consumption, especially in SWaP-constrained platforms.
- **Threshold-based detection** is reactive and often too late.
- Scheduled replacements cause unnecessary downtime or miss failures between intervals.
- **Cloud-based** diagnostics are infeasible for real-time embedded systems.

SHIELD directly addresses these limitations with an on-device, lightweight, proactive monitoring framework.

Literature Review

Traditional Fault Detection and Isolation (FDI) relies on observer-based residuals (e.g., Kalman Filters, Unknown Input Observers) and parity relations (Isermann, 2006; Chen & Patton, 1999). While useful for abrupt faults, they lack sensitivity to slow-developing degradations. Prognostics and Health Management (PHM) extends detection to estimate Remaining Useful Life (RUL), but it largely focuses on mechanical systems or batteries (Saha & Goebel, 2009; Saxena et al., 2008), with little attention to embedded sensors.

Recent anomaly detection techniques utilize deep learning models—LSTMs, autoencoders (Hundman et al., 2018; Zhang et al., 2019)—for time-series analysis. However, these methods are computationally intensive and designed for cloud environments, not real-time embedded devices. SHIELD fills this critical gap by offering a predictive, embeddable, general-purpose solution compatible with constrained hardware.

Observer-based FDI (Kalman/Unknown-Input Observers, parity relations [Isermann 2006; Chen & Patton 1999]) detects abrupt faults but is insensitive to slow drifts. Prognostics & Health Management (PHM) work has centred on batteries and rotating machinery [Saha & Goebel 2009; Saxena et al. 2008]. Cloud-scale deep models (LSTM, autoencoders [Hundman et al. 2018]) capture gradual change but demand >10 MB and >10 MFLOPs—unfit for microcontrollers. Early edge-PHM studies (e.g., Banbury et al., Micronets 2021) compress models but rely on purely data-driven

features. SHIELD's novelty is a hybrid residual-plus-TinyRNN approach that keeps model size ≈5 k parameters (<64 kB flash, <0.5 MFLOPs).

Research Objectives

SHIELD addresses these gaps by providing a generalizable, proactive, and embeddable solution for sensor degradation forecasting.

This research aims to design and validate a system that predicts sensor failure using real-time behavioral analysis of sensor outputs.

Research Question

Can a hybrid residual + tiny-RNN framework running on constrained MCUs predict sensor failure ≥20 s ahead of functional loss with <1 % false-positive rate?

Hypothesis

Combining model-based residuals with a resource-efficient IRNN (or 8-cell quantised LSTM) will detect bias drift, latency growth, and noise-floor elevation early enough to enable preventive action, all within 64 kB flash and 5 kB RAM on a Cortex-M4 @ 80 MHz.

Methodology Overview

SHIELD is implemented as a three-tier architecture:

1. Output Monitoring and Residual Analysis

Estimates expected sensor behavior using physical models or observers (e.g., Kalman Filters, UIO). The residual between actual and expected values surfaces early anomalies (noise elevation, bias drift, saturation, latency).

2. Temporal Forecasting Module

Residuals and features are input into a resource-efficient recurrent model (e.g., IRNN or quantized LSTM). Trained offline on real or simulated degradation profiles, the model predicts time-to-failure (TTF) or outputs a degradation score. Inference is performed on embedded platforms (e.g., STM32, Raspberry Pi) via TinyML toolchains.

3. Failure Prediction and Decision Layer

Issues early warnings based on degradation thresholds. Enables sensor failover, recalibration, or alerts—before functional failure occurs.

Validation Plan

- Data — NASA PCoE turbofan (public), new 50 h HIL corpus of pressure & IMU drift (to be released MIT-licensed).
- Metrics — AUROC, prediction horizon @95 % recall, inference latency, energy/byte (Power Profiler Kit II).
- Baselines — static thresholds, KF-CUSUM, 128-unit LSTM autoencoder (desktop), Micronets edge-PHM model.
- Safety & Certifiability — code generation targets MISRA-C; roadmap for DAL B (DO-178C) and ASIL C (ISO 26262) qualification.

Definition of Sensor Failure & Detection Horizon

SHIELD covers hard loss, stuck-at faults, bias drift, rising latency, saturation, dropout, calibration shift, EMI-induced noise. Target horizons range from 20 s (high-speed UAV) to 12 h (industrial process), enabling fail-over, safe-mode, or scheduled maintenance.

SHIELD defines sensor failure broadly as any deviation that renders the sensor's output inaccurate, unsafe, or untrustworthy—including:

- Complete signal loss
- Constant outputs (stuck-at faults)
- Gradual bias drift
- Increased latency
- Saturation and signal clipping
- Intermittent dropouts
- Calibration loss
- Measurement interference
- Both hard failures and soft degradations are within SHIELD’s scope.

Detection Horizon and Preventive Action

SHIELD targets a proactive detection horizon—from seconds to hours before failure—depending on degradation severity. Even a 10–20 second early warning in high-speed platforms (e.g., UAVs or autonomous vehicles) can enable emergency maneuvers or system failover. Longer-term forecasts allow scheduled maintenance, minimizing unplanned downtime and improving safety margins.

Scope Considerations: Sensor vs. System-Level Monitoring

SHIELD focuses on sensor-centric degradation analysis but acknowledges that some failures propagate system-wide. Future iterations may extend the architecture to incorporate system-level anomaly correlation for holistic diagnostics. The modular design supports both approaches.

SHIELD is engineered to detect failures early enough to allow for meaningful intervention. For degradation processes such as bias drift, noise floor elevation, or increased latency, SHIELD can identify changes minutes, hours, or even days before complete failure. This detection horizon allows for actions like sensor recalibration, mission reconfiguration, switching to backup sensors, or triggering safe-mode protocols. Even a 10–20 second warning in high-speed systems can be operationally significant.

Commercial and Industrial Potential

SHIELD's embeddability, modularity, and generalizability position it for adoption across multiple sectors:

- Aerospace (Boeing, Honeywell): AoA, pitot, IMU, and pressure sensors
- Autonomous UAVs (DJI, Skydio): IMU/GPS degradation monitoring
- Industrial Automation (FANUC, KUKA): torque, force, and vibration sensors
- Medical Devices (Medtronic, GE): biosensors, flow and pressure sensors

Deployment modes include SDKs, firmware modules, or hardware-assisted dev kits. Its compatibility with TinyML and off-the-shelf microcontrollers ensures accessibility for OEMs and integrators.

Conclusion and Impact

SHIELD pioneers an edge-AI prognostic layer that forecasts sensor degradation with MCU-level resources, bridging the gap between heavyweight cloud analytics and coarse threshold alarms. By delivering actionable warnings well before failure, SHIELD promises to slash unscheduled downtime, lower redundancy costs, and raise safety margins across aerospace, autonomous systems, industry, and healthcare.