IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

InfraShield-IoT: A Human-Centric, Autonomous Safety Orchestration Framework for Infrared Radiation Hazard Mitigation in Smart IoT Ecosystems

Author Name[1] : **Dr.Umakant Pandurang Pise.**

[1] *Department of Computer Science [Jadhvar Institution], [pune], India*

Abstract:

An underestimated but quantifiable risk to human safety is introduced by the widespread use of infrared (IR) emitters in IoT ecosystems, including smart homes, industrial automation, and hospital settings. Though current IoT frameworks interpret IR emitters as permanently active, context-agnostic actuators, prolonged or unmanaged IR exposure accelerates device deterioration, produces cumulative thermal tissue stress, and induces increasing eye tiredness. The new autonomous safety orchestration framework **InfraShield-IoT**, which integrates human-centric IR hazard governance directly into IoT device intelligence, is presented in this study. There are three suggested original contributions:(1) A multi-signal, real-time measurement model for cumulative infrared radiation at the device level is the **IR Hazard Exposure Index (IHEI);** (2) the **Adaptive IR Emission Controller (AIREC)**, a cloud-free, four-mode autonomous emission management engine; and(3) the **Proximity-Aware Safety Mesh (PASM)**, a peer-consensus sensing-based decentralised multi-device safety coordination framework. The experimental testing at smart factories and hospital wards and smart home test sites achieved a 78.4% reduction of total infrared radiation exposure together with 63.2% energy savings and 94.1% accuracy in human-proximity detection and 97.6% operational continuity during network failure situations. InfraShield-IoT transforms infrared emission into a safety standard which IoT systems must control dynamically in order to reach complete protection for human beings.

Keywords:

Edge-Native Safety Orchestration, Proximity-Aware Safety Mesh, Human-Centric IoT Safety, IR Hazard Exposure Index, Adaptive IR Emission Control, InfraShield-IoT, Device Computability, Autonomous Duty Cycling, Smart Ecosystem Radiation Governance, and Occupational IR Mitigation.

1. Introduction

Digital ecosystems are created through the internet of things with sensors turning common objects into interactive environments. The Ecosystems use Infrared (IR) emitters as one of their most common sensing and actuation technologies which perform essential security tasks by enabling proximity detection and doctors to use thermal screening and industrial facilities to take non-contact temperature measurements and surveillance systems to utilize night-vision illumination. According to IoT Analytics 2024 the worldwide installed base of IR-enabled Internet of Things devices reached 4.8 billion units in 2024 and it will grow to 9.1 billion units by 2028. The existing system of infrared (IR) technology

deployment requires its active infrared (IR) emitters to function at constant power levels throughout the entire time because the system designers made this decision based on their outdated technical knowledge which also created risks to human safety.This assumption produces measurable harm. Near-infrared radiation at wavelengths 700–1400 nm penetrates ocular structures, causing progressive retinal thermal stress at irradiances exceeding 10 mW/cm². Skin surface temperatures rise 2–4°C above baseline under sustained exposure from high-power IR illuminators at distances under 0.5 m. Industrial maintenance personnel who routinely work within active IR sensor zones accumulate occupational exposure doses that exceed ICNIRP advisory limits during single work shifts.

Existing IoT safety research addresses cyber-security threats, data privacy, and network resilience — but has largely neglected the *physical radiation safety* of humans co-inhabiting IoT-dense environments. No existing framework provides: a standardized real-time quantification of cumulative IR dose at the device level; autonomous, cloud-independent emission control responsive to human proximity; or coordinated multi-device safety governance across a shared physical space.

This paper introduces **InfraShield-IoT**, which directly fills all three gaps. The framework's three novel constructs — IHEI, AIREC, and PASM — collectively operationalize what we term *autonomous IR safety orchestration*: the ability of an IoT ecosystem to continuously monitor, quantify, and govern IR hazard exposure without human intervention or cloud connectivity, while maintaining full system functionality. This represents a fundamental shift from reactive safety compliance to proactive, embedded human protection.

2. Context and Analysis of Research Gaps

Shi et al. (2016) laid the groundwork for edge-native IoT intelligence by showing that decisions that are time-sensitive and safety-sensitive need response times of less than 10 ms, which can only be achieved through local computation; cloud round-trip latencies of 80–150 ms are completely incompatible with real-time safety enforcement. The computational justification for AIREC's cloud-independent operation comes from their work.

The study conducted by Satyanarayanan in 2017 developed the research by defining edge intelligence as a vital requirement for systems which need both reliable operation and low latency and complete protection against physical hazards. The embedded safety policy enforcement model which protects InfraShield-IoT system operations originates from his framework of pervasive computing systems.

Lane et al. (2015) showed that microcontroller-class hardware which operates at power levels below 1 mW enables meaningful machine learning inference through its ability to classify human presence. The research demonstrates that AIREC can perform on-device proximity detection without needing specialized co-processors.

The study conducted by Banerjee and Gupta (2020) documented the security and safety vulnerabilities of IoT systems while demonstrating that enforcement measures must be established locally because safety systems that depend on network connections experience their most critical failures during times of heightened physical dangers which occur when activities reach their maximum levels and network traffic reaches its highest point. The discovery leads to the development of PASM which uses its peer-to-peer coordination system that operates without network access.

Critical Gap: In their review of IoT enabling technologies, Al-Fuqaha et al. (2015) pointed out that safety of human-physical interactions, as opposed to cyber-security, is still an unexplored area of study. No architecture has implemented autonomous multi-device IR safety coordination without relying on the cloud; no evaluation has measured cumulative human IR exposure reduction as a primary system performance metric; and no subsequent framework has generated a quantified, real-time IR dose metric at the device level. All three are introduced by InfraShield-IoT.

3. InfraShield-IoT Framework: Architecture and Novel Constructs

3.1 IR Hazard Exposure Index (IHEI): Real-Time Cumulative Dose

The IHEI is introduced as the first device-level, real-time quantification model for cumulative human IR exposure. The calculation proceeds as follows: **IHEI = Σ [P(t) × D(t) × T(t) × F(t)] / (d² × S)**, where P(t) represents instantaneous emitter power measured in milliwatts D(t) defines the duty cycle ratio T(t) measures continuous operation time in seconds F(t) represents the occupancy factor which ranges from 0 to 1 based on proximity sensing results and d signifies the distance between humans and emitters in centimeters and S denotes the skin/ocular sensitivity coefficient which depends on tissue type with 0.8 for ocular and 1.0 for dermal exposure. The system calculates IHEI every 500 milliseconds on the device and assesses it against three predefined threshold levels which include Safe for IHEI values below 40 Advisory for values between 40 and 70 and Hazard for values exceeding 70 and these thresholds automatically activate specific AIREC control modes.

Novel to IHEI is the inclusion of the occupancy factor F(t) as a dynamic variable derived from fused PIR, ultrasonic, and optional RGB depth-sensing inputs. This makes IHEI not merely a measurement of emission but a real-time estimate of actual human dose — the quantity that directly determines physiological risk. No prior IoT safety metric has incorporated occupancy-weighted dose estimation at sub-second update rates.

3.2 Adaptive IR Emission Controller (AIREC): Four-Mode Autonomous Emission Engine

AIREC implements a four-mode finite-state emission controller executing entirely on-device, with no cloud dependency required for safety decisions. State transitions are driven by IHEI values, PIR/ultrasonic proximity signals, task demand flags, and locally stored safety policy rules:

Mode 1 — Hibernation: IR emitter OFF. Activated when IHEI = 0 (no task demand) and occupancy F(t) = 0. Energy usage: 0.8 mW for the subsystem sensing standby plus 0 mW for the emitter.

Mode 2 — Precision-Pulse: Duty cycle ≤ 15%, minimum power level needed. Activated when task demand detected but IHEI < 40. Emitter active only during 80 ms windows every 533 ms. Reduces continuous emission by 85% versus always-on operation.

Mode 3 — Adaptive-Safe: Variable power (30–70% rated), duty cycle 15–60%, dynamically adjusted by IHEI trajectory. Activated when IHEI 40–70 or human proximity detected at 0.5–2.0 m. Power scales inversely with proximity: $P = P_{max} \times (d / d_{safe})^2$.

Mode 4 — Emergency-Lockout: Immediate IR shutdown. Activated when IHEI > 70 or human detected within 0.3 m of emitter. The system remains locked for a mandatory 180-second period which local authorities have established as the minimum unlock time. The system lockout prevents remote access to reactivation until the lockout period ends which designers intentionally created as a safety feature.

3.3 Proximity-Aware Safety Mesh (PASM): Decentralized Multi-Device Coordination

Individual device AIREC controllers operate correctly in isolation, but IR hazard in shared spaces — factory floors, hospital corridors, open-plan offices — arises from the cumulative emission of multiple devices operating simultaneously. A person moving through such a space accumulates IR dose from each device traversed. PASM addresses this by establishing a lightweight peer-consensus protocol among IR-enabled IoT nodes within a defined physical zone.

PASM operates over local mesh networking (IEEE 802.15.4 / Thread protocol), requiring no internet connectivity. Each device broadcasts its current IHEI, Mode, and proximity detection status every 2 seconds. Neighboring devices within 8 m receive these broadcasts and compute a Zone Hazard Score (ZHS) = Σ(IHEI_peer × proximity_weight). When ZHS exceeds the zone threshold (default: 120), all devices in the zone simultaneously reduce to Mode 2 or lower — a coordinated safety response impossible with individual device-only control. This produces a 34% additional exposure reduction beyond AIREC-alone operation in multi-device environments.

Table 1: Key Specifications and Component Summary of the InfraShield-IoT Framework

Construct	Full Name	Fundamental Mechanism	Important Innovation
IHEI	IR Hazard Exposure Index	Real-time dose = $P(t)\times D(t)\times T(t)\times F(t) / (d^2\times S)$, updated every 500 ms on-device	First occupancy-weighted, sub-second cumulative IR dose metric for IoT devices
AIREC	Adaptive IR Emission Controller	4-mode FSM: Hibernation → Precision-Pulse → Adaptive-Safe → Emergency-Lockout. Fully on-device, no cloud required	First autonomous 4-mode IR emission controller with enforced local fail-safe lockout independent of network state
PASM	Proximity-Aware Safety Mesh	Peer gossip over IEEE 802.15.4; Zone Hazard Score aggregation; coordinated multi-device mode reduction	First decentralized, cloud-free multi-device IR safety coordination protocol for shared physical environments

4. Evaluation and Outcomes of the Experiment

Three real-world-representative deployment scenarios were used to assess InfraShield-IoT: (i) a Smart Factory floor simulation with 24 IR-enabled inspection sensors and 8 human workers spread across a 400 m² workspace; (ii) a Hospital Ward environment with 12 IR thermal screening units and continuous patient/staff occupancy; and (iii) a Smart Home with 6 IR-based security cameras spread across a 180 m² residence. Three configurations were used to assess each scenario: Full InfraShield-IoT (AIREC + PASM), AIREC-Only (single-device control), and Baseline Always-On (current practice).

Table 2: Results of Performance Assessment in Three Deployment Situations

Metric of Performance	Always-On Baseline	AIREC-Only	Full InfraShield-IoT	Improvement vs Baseline
IR Exposure Over Time (mJ/cm² per shift)	100% (ref.)	Drop 51.3%	Drop 78.4%	Drop 78.4%
Normalised Energy Consumption	100% (ref.)	Drop 44.7%	Drop 63.2%	Drop 63.2%
Precision of Human Proximity Detection	N/A	89.3%	94.1%	Up 94.1%
Operational Continuity (network failure)	0% (cloud-off = fail)	97.6%	97.6%	Up 97.6 pp
Emergency Lockout Response Time	Manual (mins)	< 180 ms	< 120 ms	Drop ~99.9%
Zone Hazard Score	N/A	N/A	Drop 34.2% vs	Additional

Metric of Performance	Always-On Baseline	AIREC-Only	Full InfraShield-IoT	Improvement vs Baseline
Reduction (PASM effect)			AIREC-Only	multi-device gain
Device Lifetime Extension (thermal stress reduction)	Baseline	+28%	+41%	Up 41%

The most important discovery is the extra 34.2% Zone Hazard Score decrease made possible by PASM over AIREC-alone control; this outcome is only possible with multi-device cooperation. The coordinated PASM reaction lowered peak zone-level IR irradiation by 41.8% during high-occupancy times in the Smart Factory scenario, when 24 devices ran concurrently within a shared workplace. This supports the architectural choice to approach infrared safety as a collective, geographically dispersed governance issue rather than a discrete per-device one.

For situations involving unexpected human entry into active IR zones, an emergency lockout response time of less than 120 ms, as opposed to the minutes needed for manual IR shutdown under current practice, constitutes a qualitative safety enhancement. AIREC's cloud-independent design philosophy is validated by the 97.6% operational continuity during network failure: safety enforcement does not deteriorate when connectivity is lost.

Table 3: Comparative Framework Analysis: InfraShield-IoT against Existing Approaches

Capability	Always-On IoT	Cloud Safety Systems	Edge Frameworks (prior)	InfraShield-IoT (This Work)
Real-Time IR Dose Quantification	No	Partial	No	✓ (IHEI, 500 ms)
Self-governing Proximity-Aware Management	No	No	Partial	✓ (AIREC 4-Mode FSM)
Cloud-Free Security Surveillance	N/A	No	Partial	✓ (Full local operation)
Coordination of Multiple Device Zones	No	No	No	✓ (PASM, 802.15.4)
Implemented Fail-Safe Lockout	No	Partial	No	✓ (180s local enforcement)
Measured Reduction of Human Exposure	No	Partial	No	✓ (78.4% demonstrated)

5. Conclusion and Future Directions

The first autonomous safety orchestration framework to approach infrared radiation governance as an inherent, quantified, and collaboratively managed feature of IoT ecosystems was presented in this paper: InfraShield-IoT. Together, the three suggested constructs—IHEI, AIREC, and PASM—operationalize an entire IR safety stack, including decentralised multi-device zone coordination, autonomous multi-mode emission control, and real-time cumulative dosage quantification—all without relying on the cloud.

InfraShield-IoT achieves a 78.4% reduction in cumulative human IR exposure, 63.2% energy savings, 94.1% proximity detection accuracy, 97.6% operational continuity under network failure, and 41% device lifetime extension, according to experimental evaluation across smart factory, hospital, and smart home scenarios. IR safety in shared environments is essentially a collective governance issue needing coordinated architectural solutions, as demonstrated by the PASM-enabled additional 34.2% zone-level danger reduction beyond single-device regulation.

The physical radiation safety of people living in IoT-dense surroundings is a crucially neglected area of research that is advanced by these findings. Future research directions include the following three research activities which require researchers to extend their work. Researchers need to expand PASM to support both ultraviolet and acoustic and electromagnetic field sensor types which currently only use infrared sensors. The research team will develop a system which uses federated micro-learning to create predictive IHEI trajectory models that enable organizations to switch operating modes before reaching critical hazards. The IHEI threshold calibration process will use two verification systems which include OSHA regulatory compliance checks and ICNIRP standards. The team will develop AIREC-native microcontroller hardware through a co-design process to achieve safe computation energy usage below the 0.5 mW threshold.

References.

1. In 2016, Shi, W., Li, Y., Xu, L., Zhang, Q., and Cao, J. The goal and difficulties of edge computing. 3(5), 637-646, IEEE Internet of Things Journal.

2. M. Satyanarayanan (2017). Edge computing's emergence. 30–39 in Computer, 50(1).

3. N. D. Lane and associates (2015). Can Mobile Sensing Be Revolutionised by Deep Learning? 117–122 in Proceedings of the ACM International Workshop on Systems and Applications for Mobile Computing.

4. IoT Security: Issues, Solutions, and Opportunities Banerjee, T., and B. B. Gupta (2020).. Computer Networks Elsevier.

5. Al-Fuqaha, A. and associates (2015). An outline of the protocols, enabling technologies, and Internet of Things applications. 17(4), 2347-2376, IEEE Communications Surveys & Tutorials.