# RISC-V and openHarmnoy empower a "Dual Security" system of energy usage and privacy in future smart homes and smart cities

Xuegang Jiang,[1] Yuechuan Tao,[2] Haoliang Li,[2] Zehao Wang,[1] Yuxi Jiang,[1] Guokui Qin,[1] Chun Zou,[3] Di Wang,[1] and Zhaoyang Dong[2,*]
[1]RVOH Open-Source International Laboratory, Shenzhen 518071, China
[2]Department of Electrical Engineering, City University of Hong Kong, Hong Kong SAR, China
[3]xFusion Digital Technologies Co., Ltd., Zhengzhou 450046, China
*Correspondence: zydong@cityu.edu.hk
Received: October 29, 2025; Accepted: November 20, 2025; Published Online: November 26, 2025; https://doi.org/10.59717/j.xinn-energy.2026.100126

Citation: Jiang X., Tao Y., Li H., et al. (2026). RISC-V and openHarmnoy empower a "Dual Security" system of energy usage and privacy in future smart homes and smart cities. *The Innovation Energy* **3**:100126.



The increasing occurrence of energy-related safety accidents worldwide—with gas leaks and explosions serving as a stark, well-documented example—has driven urgent calls for advanced safety solutions across the entire energy ecosystem. This growing threat to energy usage security, which causes significant fatalities and property damage, highlights the critical need for more reliable and sophisticated safety systems. Apart from physical usage security, cyber security has emerged as an equally pressing concern in the era of smart energy systems. As energy infrastructure becomes interconnected (e.g., smart gas detectors linking to home hubs, or municipal energy grids sharing real-time data), sensitive information such as energy consumption patterns, device operational status, and even control signals becomes vulnerable to data breaches, malicious hacks, or unauthorized access. A cyber attack on these systems could disrupt energy supply, falsify safety alerts, or even trigger physical hazards indirectly—creating a "double threat" that single-dimensional safety solutions can no longer address. In this context, the integration of cutting-edge technologies, such as RISC-V architecture and OpenHarmnoy, is helping to develop a "dual security" framework and redefine the landscape of energy securitty monitoring and management systems.

## RISC-V ARCHITECTURE: A NEW ERA OF OPEN-SOURCE COMPUTING

RISC-V is an open-source processor architecture based on the principles of Reduced Instruction Set Computing (RISC).[1] Unlike traditional proprietary processor designs, RISC-V provides a flexible, customizable, and modular platform that is freely available for modification and distribution. This positions RISC-V uniquely to address the "dual security" demands of modern energy systems: safeguarding both physical energy operations and the digital data they generate.

For physical energy security, RISC-V's modularity enables hardware customization tailored to real-time safety needs. Developers can integrate specialized instruction sets for energy-specific risk detection—such as low-latency modules for gas leak sensing, voltage fluctuation monitoring, or thermal anomaly tracking—without unnecessary computational overhead. This precision ensures microcontroller units (MCUs) in smart meters, pipeline sensors, or grid controllers process critical safety data (e.g., pressure spikes, current surges) with minimal latency, triggering rapid responses like automatic shutdowns or alerts to prevent physical hazards.

For cyber security, RISC-V's open-source nature eliminates "black-box" vulnerabilities inherent in proprietary architectures, where hidden backdoors or undisclosed flaws can expose energy systems to hacks. Its transparent codebase allows global communities to audit, identify, and patch vulnerabilities collaboratively—critical for protecting sensitive energy data (e.g., consumption patterns, device control signals) from breaches. Additionally, modularity lets developers embed hardware-level security features: encrypted data pipelines, secure boot protocols, or access-control instructions can be directly integrated into RISC-V chips, creating a "root of trust" at the processor level. This prevents malicious actors from falsifying sensor data (e.g., masking a gas leak) or hijacking control systems (e.g., remotely disabling safety valves)—risks that plague interconnected energy ecosystems reliant on generic, closed architectures.

## OPENHARMNOY: A UNIFIED PLATFORM FOR IOT AND SMART DEVICES

OpenHarmnoy,[2] developed by Huawei, is an open-source, distributed operating system designed to support a wide variety of devices, from smartphones to smart appliances and IoT systems.

Its key feature is its ability to seamlessly integrate with multiple types of devices, enabling them to work together in a unified ecosystem. OpenHarmnoy aims to address the growing complexity of smart devices by offering a single, consistent operating platform that supports cross-device communication and collaboration.

OpenHarmnoy's distributed computing framework breaks silos between energy devices, enabling real-time coordinated safety responses across the ecosystem. Unlike traditional OSes limited to single-device/type communication, it connects heterogeneous hardware—such as RISC-V-powered gas sensors, smart meters, thermal monitors, and control hubs—into a unified safety network. For instance, if a gas sensor detects a leak, it instantly triggers cross-device actions: shutting the gas valve, disabling electrical appliances (to prevent ignition), adjusting ventilation, and alerting users and municipal platforms. In smart cities, it can reroute power if electrical sensors spot grid anomalies, while alerting gas pipeline controllers to boost monitoring and avoid cascading risks. Its modular design also ensures scalability: developers adapt apps to residential, industrial, or municipal scenarios without rebuilding systems, fitting small homes to large urban grids.

For cyber security, OpenHarmnoy embeds distributed security as a core feature to protect sensitive data in connected energy systems. It uses a "trusted device chain": every device (e.g., smart meter, gas detector) undergoes strict identity authentication before joining, blocking unauthorized or compromised hardware. Device-to-device data transmission is end-to-end encrypted, shielding sensitive data (e.g., energy use, user habits, control signals) from breaches or tampering. Fine-grained permission management lets admins restrict access: a home gas sensor, for example, shares leak alerts with hubs/platforms but only sends anonymized usage data to providers, balancing function and privacy.

## THE RISC-V + OPENHARMNOY COMBINATION IN ENERGY SAFETY SYSTEMS

The integration of RISC-V and OpenHarmnoy transforms energy safety systems—spanning gas, electricity, and thermal infrastructure—into a holistic framework for dual security (physical hazard prevention and digital data protection). Rather than simply integrating these technologies into existing systems, their combination lays the groundwork for an entirely new paradigm in energy security—one where the system itself evolves and adapts autonomously, learning from its own data and external threats. Their synergy unites hardware and software safeguards in ways neither could achieve alone, with gas safety serving as a clear example of how this collaboration works.

These systems—from AI-powered gas detectors to electrical load monitors—leverage the unique synergy between hardware-level precision and software-driven intelligence. RISC-V's customized processing enables real-time analysis of energy data (e.g., gas concentrations, electrical spikes) while embedding hardware-level checks to prevent tampering with hazard signals. OpenHarmnoy builds on this foundation by creating a unified, distributed framework that not only integrates devices across various domains but also allows for continuous, autonomous decision-making in response to evolving threats. This network security extends beyond traditional encryption, incorporating advanced features like anomaly detection and adaptive security protocols, which can autonomously update device behaviors based on real-time conditions, thereby preemptively neutralizing new types of cyber attacks.

A concise example illustrates this: When a RISC-V-enabled gas detector spots a leak, it first validates data via hardware-level checks to rule out

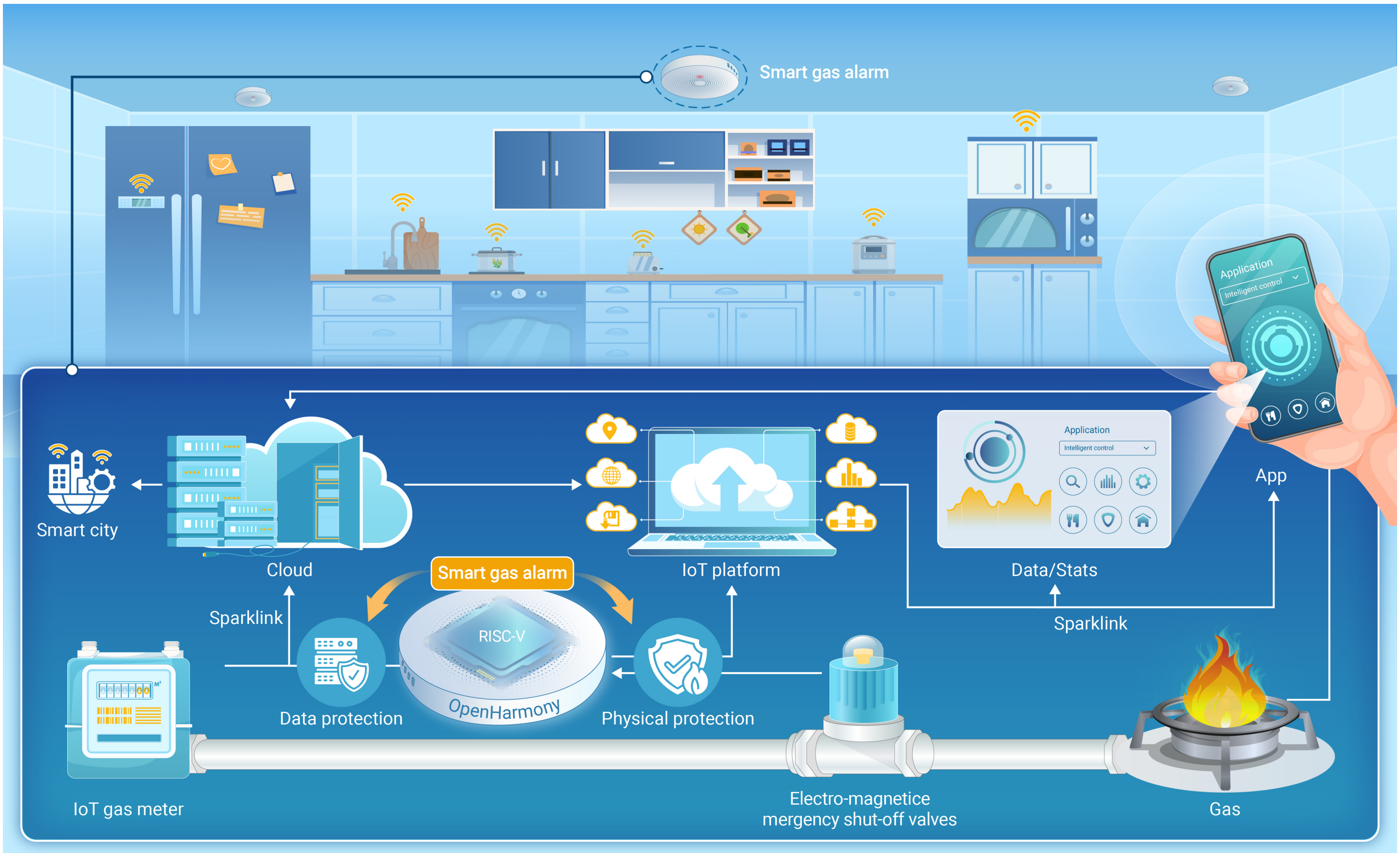


**Figure 1. Framework of "Dual Security" System for Energy Usage.**

tampering. It then sends an encrypted alert to OpenHarmnoy, which triggers coordinated actions—shutting the gas valve (physical safety), disabling nearby appliances (ignition prevention), and sending a password-protected alert to the user (digital privacy). This approach is far more than a reactive safety mechanism; it is part of a broader strategy to create a 'cognitive' safety system that not only reacts to real-time threats but also anticipates them by analyzing data from diverse sources, adjusting the system's behavior accordingly.

This combination delivers three focused dual-security benefits:

- Security-Aligned Customization: RISC-V's microcontrollers embed "root-of-trust" features (e.g., secure boot) for physical safety functions, aligned with OpenHarmnoy's software security protocols.
- Trusted Integration: OpenHarmnoy's distributed framework authenticates all devices, blocking fake commands that could compromise physical safety.
- Scalable Protection: As systems grow (from homes to commercial sites), RISC-V adds secure sensors and OpenHarmnoy extends encrypted channels—keeping both physical and digital security intact.

## FUTURE POTENTIAL

The global gas alarm market is experiencing significant growth. For example, gas alarm has a forecast of a market value of USD 9.8 billion by 2029.[3] This growth is driven by an increasing focus on safety, stricter regulations, and technological advancements. The combination of RISC-V and OpenHarmnoy is positioned to play a key role in this market expansion by providing innovative, scalable, and cost-effective solutions.

In addition to residential applications, RISC-V and OpenHarmnoy-driven energy safety systems have the potential to revolutionize industries such as smart home, IoT, industrial facilities, and even public transportation systems.

The versatility of these technologies makes them ideal for addressing the diverse needs of various sectors, from energy management to risk mitigation. Furthermore, as AI and machine learning technologies continue to advance, these systems will become even smarter, capable of predicting potential energy-related hazards before they occur. Predictive maintenance, powered by AI, will allow gas systems to be monitored continuously, ensuring that any signs of failure are addressed proactively.

## CONCLUSION

The convergence of RISC-V and OpenHarmnoy in the development of energy safety systems is a significant step forward in the pursuit of safer homes and workplaces. By leveraging open-source hardware and software, developers can create customized, efficient, and scalable systems that enhance safety and reliability. As the demand for smart safety solutions grows, RISC-V and OpenHarmnoy will play an increasingly important role in shaping the future of energy security, offering a path to a more secure and connected world. This integration not only highlights the potential of open-source technologies in driving innovation but also sets the stage for the next generation of smart, interconnected devices that will form the backbone of tomorrow's safety ecosystems.

## REFERENCES


1. Gao Y., Cui E., Li T., et al. (2024). A review of big data applications based on risc-v. *CCPQT* 2:316–320. DOI:10.1109/CCPQT60491.2023.00025
2. Weng V.N.S. (2020). HARMONY OS's FEATURES AND CHALLENGES. https://www.researchgate.net/publication/341849888_HARMONY_OS's_FEATURES_AND_CHALLENGES.
3. Grand View Research. (2024). Gas Sensor Market (2025 - 2030). *Market Analysis Report.* https://www.grandviewresearch.com/industry-analysis/gas-sensors-market.


## FUNDING AND ACKNOWLEDGMENTS


This work is supported by JC STEM Lab of Future Energy Systems (2025-0039), Global STEM Professorship (GSP313), and a Startup Grant of City University of Hong Kong.


## DECLARATION OF INTERESTS

The authors declare no competing interests.