Whitepaper: Advancing ICS Cybersecurity with the NX-914 Adaptive Logic Array

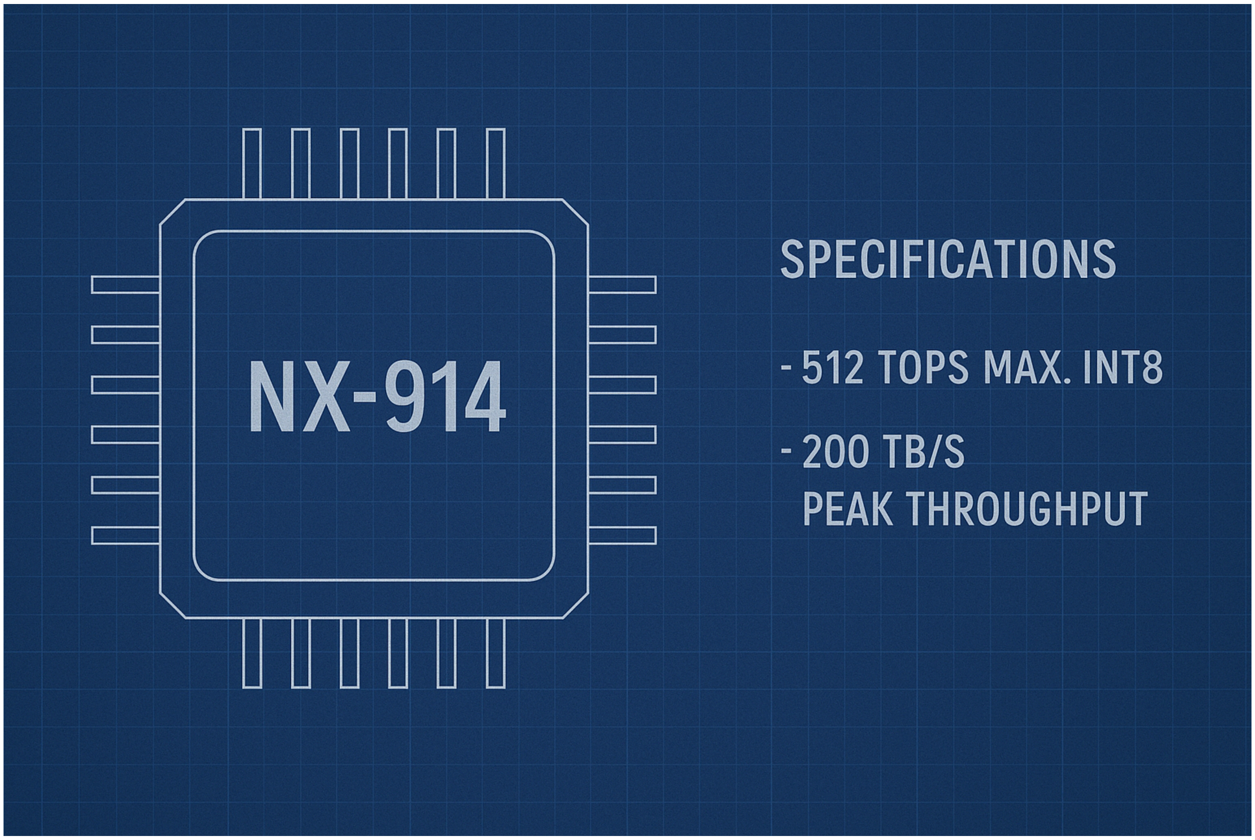
By Robin Egas, Co-Founder and COO, ICS Guard Technologies

Executive Summary

As cyber threats against industrial control systems (ICS) continue to grow in sophistication and scale, the need for secure, intelligent, and adaptable hardware components is more pressing than ever. The NX-914 Adaptive Logic Array, developed by ICS Guard Technologies, represents a transformative approach to cybersecurity in critical infrastructure environments. Designed specifically for edge deployment in operational technology (OT) networks, the NX-914 offers real-time threat mitigation, AI-driven anomaly detection, and dynamic reconfigurability—all in a low-latency, power-efficient integrated circuit.

Introduction

Modern industrial control environments—from power plants and water treatment facilities to manufacturing lines and logistics hubs—face increasing vulnerability to cyber attacks. Many of these systems still operate on legacy infrastructure and lack the computing resources necessary for modern AI-driven security solutions. The NX-914 is engineered to close this gap by embedding intelligence directly at the hardware level, where latency is minimal and detection capabilities are immediate.



SPECIFICATIONS

- 512 TOPS MAX. INT8
- 200 TB/S
  PEAK THROUGHPUT

Technical Overview of the NX-914

The NX-914 Adaptive Logic Array is a secure edge AI chip with the following key specifications:

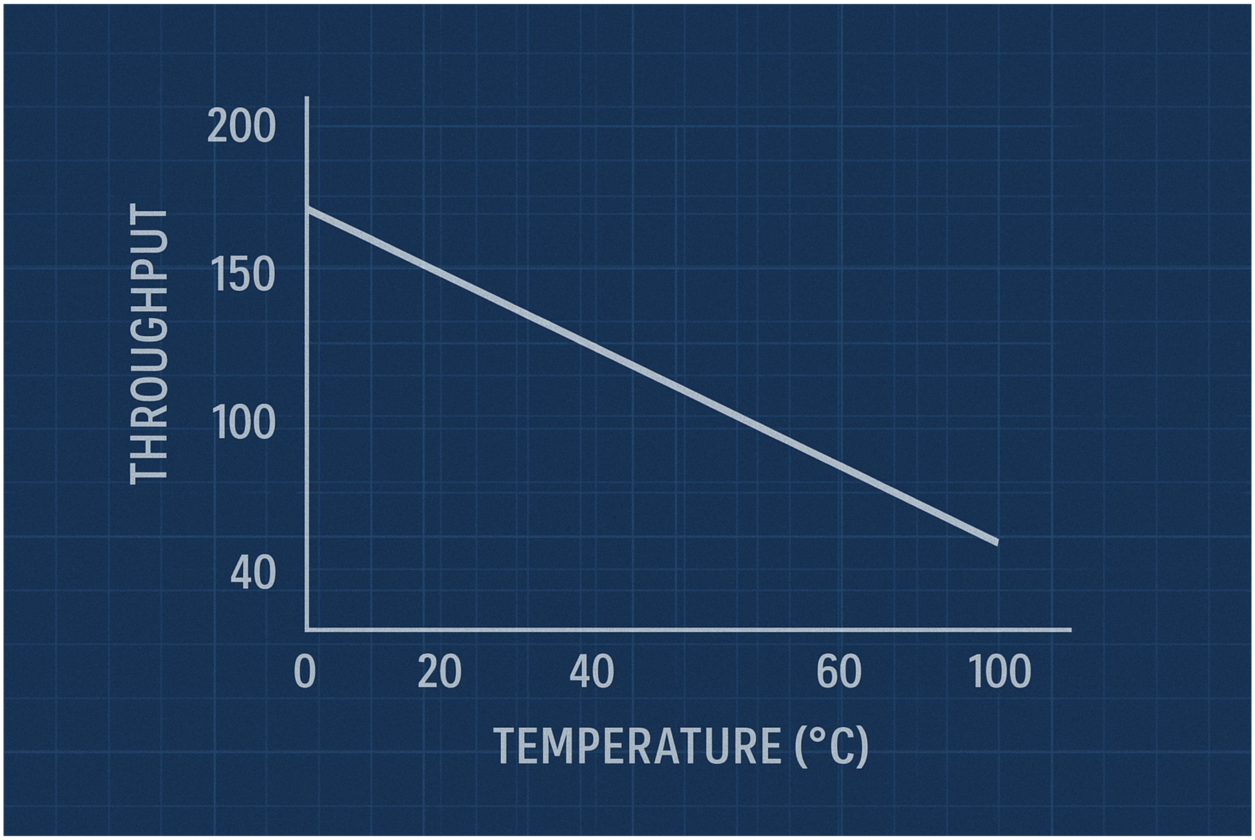
- **Tensor-Aware Reconfigurable Logic (TARL):** The core of the NX-914 is its ability to dynamically rewire its logic gates in response to real-time data input, optimizing processing pathways for emerging attack patterns or environmental changes.

- **Secure Boot & Cryptographic Isolation:** The chip includes a hardware-anchored root of trust and encrypted firmware zones, preventing unauthorized firmware modifications or tampering.

- **Low-Power AI Accelerator:** Designed to run complex machine learning inference models with ultra-low latency, consuming less than 1.2W in full operational mode.

- **Integrated Side-Channel Monitoring:** Built-in sensors detect unusual power usage or electromagnetic emissions, identifying side-channel attacks without the need for external tools.

- **Field Programmability with Hardware Lockout:** The NX-914 supports on-site reprogramming under secure conditions, but can be locked permanently once deployed to high-security environments.


200
150
100
40
THROUGHPUT
0
20
40
60
100
TEMPERATURE (°C)

Applications in ICS Cybersecurity

1. Real-Time Anomaly Detection at the Edge
By embedding the NX-914 directly into PLCs, RTUs, or network gateways, organizations can enable real-time anomaly detection without routing data back to centralized systems. This reduces response time and limits exposure windows for potential intrusions.

2. Network Behavior Profiling
The chip can profile baseline network behavior over time and flag anomalies indicative of lateral movement, command injection, or data exfiltration—common attack vectors in ICS breaches.

3. Adaptive Threat Response
Utilizing its reconfigurable logic, the NX-914 can dynamically shift between defense postures based on threat intelligence—effectively creating a “moving target” architecture that increases attacker workload and complexity.

4. Legacy System Hardening
Even legacy devices without embedded security can benefit from NX-914 retrofitting, allowing critical infrastructure operators to gain AI-powered defenses without overhauling entire systems.

Deployment Architecture

ICS Guard Technologies offers a modular deployment model:

- **NX-914 Embedded Module**: For OEM integration into new ICS hardware.
- **NX-914 Secure Adapter Unit**: A standalone retrofit device that sits between ICS endpoints and the network layer.
- **NX-914 Management Console**: A secure, role-based access platform for updating firmware, monitoring chip activity, and integrating with SIEMs and SOCs.

Each deployment type includes firmware signed by ICS Guard’s root certificate authority, ensuring traceable authenticity.

Compliance and Certification Roadmap

The NX-914 architecture is aligned with NIST SP 800-82 Rev. 3 guidance and is currently undergoing testing for FIPS 140-3 validation and IEC 62443-4-2 conformance. These certifications will ensure broad interoperability with U.S. federal and international cybersecurity frameworks.

Future Outlook

As threat actors increasingly target the operational core of national infrastructure, the fusion of AI and hardware-level protection will become essential. ICS Guard Technologies envisions the NX-914 as the foundational element in next-generation ICS security stacks—bridging operational continuity with uncompromising defense.

Our roadmap includes development of the NX-918, which will expand on the NX-914's capabilities by introducing secure federated learning, allowing devices to share learned threat models without exposing raw data.

Conclusion

The NX-914 Adaptive Logic Array provides a critical leap forward in ICS security. By embedding smart defense mechanisms directly into hardware, organizations can defend vital infrastructure with speed, intelligence, and adaptability. ICS Guard Technologies is committed to protecting operational systems at the speed of innovation.

Robin Egas
Co-Founder and Chief Operating Officer
ICS Guard Technologies

ICSGUARD