BLUESKYTEC

Assured Machine Trust as a Prerequisite for Maritime Information Warfare
A Navy Perspective on Enabling Integrity Across the Modern Battlespace

Submitted by Blueskytec America Inc. | Clinton Groves, CEO

Nontraditional Defense Contractor (NDC) | Small Business Concern (SBC) | U.S. Owned

Maritime operations now depend on machines acting faster than humans can observe, much less intervene. Combat systems, propulsion, navigation, logistics, sensors, and decision aids increasingly exchange data and commands autonomously, across platforms, domains, and classification boundaries. Yet the trust model underpinning these machine-to-machine interactions remains fundamentally unchanged. Systems still assume the authenticity and integrity of the signals they receive. This assumption has become the primary source of operational risk.

Cybersecurity, zero trust architectures, and information warfare initiatives have significantly improved visibility, detection, and response. What they have not done is remove the underlying risk that a machine can be deceived at the moment of execution. In contested maritime environments, that gap is no longer acceptable. When machines act on false, corrupted, or spoofed signals, the consequences manifest not as data loss, but as mission failure, asset compromise, and potential loss of life.

The Navy requires a different foundation. Not better monitoring after the fact, but deterministic assurance before a machine acts.

1. THE UNADDRESSED PROBLEM BENEATH EVERY THEME

The AFCEA Maritime Operations and Information Warfare Summit rightly focuses on zero trust, C5ISR modernization, cyber resilience, digital engineering, and data-driven operations. For each of these efforts to operate effectively, there is a presumption that systems exchange information securely and reliably in degraded, denied, or deceptive conditions. What is rarely stated explicitly is that all of these initiatives depend on a prerequisite that has never been fully solved. Verifiable trust in machine-to-machine communications at operational speed.

Zero trust architectures govern who or what should communicate. Cyber tools detect when something has gone wrong. Digital engineering ensures systems are designed correctly. However, none of these prevent a machine from executing a malicious or malformed command if that command appears valid within existing protocols, timing and topology.

To address this issue, we must look beyond software and related solutions. To answer this need, we must operate within physics.

Signals arrive at machines as voltage, light, or RF energy. Even as they traverse control solutions and enter the transport layer they are beneath the reach of modern conventional cyber. By the time software inspects them, the opportunity for harm already exists. The Navy, in fact the entire

Department of War and our global economy, has lived with this risk because, until recently, there was no practical way to eliminate it without the introduction of unacceptable latency, complexity, or operational burden. That constraint no longer holds.

2. REFRAMING ZERO TRUST FOR THE MACHINE AGE

Zero trust is often described as “never trust, always verify.” In practice, verification typically occurs at the user, device, or session level, mediated by software and policy engines. This works for human-driven IT systems. It is insufficient for operational systems where machines exchange thousands of commands per second.

True zero trust for machine operations requires verification at the signal level and transport layers, in real time, and without negotiation. Every command, every data exchange, must prove itself authentic and expected before it reaches a system’s point of execution. Session controls are insufficient. Patterns of operational behaviors are only valuable for post event analysis.

Keyspace Technology (KST) introduces the missing layer of real-time trust enforcement. Rather than monitoring traffic patterns or enforcing trust through certificates and sessions, KST enforces integrity deterministically at the physical and data-link layers. It validates that a signal originates from an authorized machine, conforms to expected behavior, and has not been altered in transit. If it cannot prove those conditions, the signal never reaches execution. From an operational perspective, this transforms zero trust from a policy aspiration into a physical control.

3. IMPLICATIONS FOR MARITIME C5ISR AND IW

Modern maritime C5ISR systems rely on distributed sensors, edge processing, autonomous coordination, and rapid dissemination of machine-generated intelligence. These systems are resilient only insofar as their internal communications are trustworthy. By enforcing machine trust at wire speed, KST removes entire classes of attack and failure from the C5ISR risk equation. False targeting data cannot propagate. Corrupted timing signals cannot cascade. Compromised subsystems cannot issue commands outside their authorized behavior envelope.

This has direct information warfare implications. An adversary’s ability to manipulate, spoof, or poison machine interactions becomes sharply constrained. Deception efforts that rely on protocol compliance, but semantic corruption fail by default. In effect, the Navy regains positive control of its machines, even in environments where networks are contested and visibility is limited.

4. ENABLING THE TACTICAL EDGE WITHOUT FRAGILITY

Edge systems are where trust breaks first. Limited bandwidth, intermittent connectivity, and the need for autonomous action make conventional security controls impractical. As a result, edge platforms often operate with relaxed assumptions of trust and deferred validation.

KST was designed for precisely these conditions. It does not require continuous connectivity, centralized key management, or dynamic negotiation. Trust is established at manufacture or

provisioning and enforced locally, independent of external services. This allows edge systems to operate with confidence rather than hope. Machines can act autonomously without expanding the attack surface. Operators can delegate authority without surrendering control. For maritime operations, this means unmanned systems, auxiliary platforms, and distributed sensors can integrate into the force without becoming liabilities.

5. DIGITAL ENGINEERING WITH OPERATIONAL INTEGRITY

Digital engineering promises traceability from design through sustainment. What it cannot guarantee today is that the behavior of a system in the field matches its modeled intent when under adversarial pressure.

By enforcing machine behavior at runtime, KST closes that loop. The same constraints defined during system design become enforceable conditions during operation. Deviations are not logged for later analysis; they are prevented outright.

This shifts digital engineering from documentation and assurance to active enforcement, aligning design intent with operational reality.

6. PROVEN, NOT THEORETICAL

These claims are not speculative. KST has been demonstrated within Navy contexts under operationally relevant conditions over a multi-year examination (MSTIC 22-02-A-002). It does not replace existing cyber or network investments but complements them by removing a foundational risk they were never designed to address.

Importantly, KST achieves these objectives without imposing new operational burdens. No rekeying cycles, no cloud dependencies, no continuous tuning. The system enforces integrity silently and continuously, as infrastructure should.

7. CLOSING

It is now possible in the context of machine level integrations to remove risk, not simply manage it. We have all become adept at managing cyber risk. Those skills will remain necessary. However, management is not elimination, and in machine-driven warfare, residual risk compounds faster than humans can respond.

Assured machine trust is no longer an aspirational goal, often believed impossible to achieve. It is an operational requirement.

By enforcing trust at the moment of action, KST enables the Navy to pursue zero trust, information warfare dominance, and maritime superiority on firmer ground. It removes a long-accepted failure mode that no longer needs to be tolerated or accepted. This shift is not about cybersecurity. It is about control.