BLUESKYTEC

Keyspace Technology

Don’t simply detect failures, prevent them.

Machines act faster than both humans and conventional security. When they behave badly, nothing can intervene.

The problem is simple. For decades, connected systems have lacked a practical way to prove a signal is trustworthy before machines act upon it. Without a solution, we have been forced to police machine-to-machine (M2M) communications with tools that are unable to operate both where and at the speed they exist; forcing us to react to failures, not prevent them.

KST (Keyspace Technology) changes the risk framework by inverting the solution.

Rather than chasing vulnerabilities, KST verifies every signal in real time, before that signal becomes trusted data, before a decision is made and before any machine executes. If a signal is not legitimate, it never reaches the system to cause harm.

Instead of continuing to assume signals are safe, KST proves it.

FEEDS THE RIGHT DECISIONS, STOPS THE WRONG ACTIONS	If messages are outside of compliance, they simply do not become data, decisions or actions.
WORKS INSTANTLY, NOT STATISTICALLY	Either the signal is proven valid, or it is blocked. KST does not analyze behavior, build profiles, or guess intent over time. It makes a clear decision at the exact moment of execution.
OPERATES BELOW CONVENTIONAL CYBERSECURITY	Operating below the software and network stacks as a FPGA logic-based trust anchor. It functions even when those layers are compromised, disconnected, or overwhelmed.
IMPROVES CONVENTIONAL CYBERSECURITY	Preventing invalid signals before they reach the application layer reduces alerts, shrinks the attack surface, and lowers response burden. Existing cyber tools have a clearer image of real threats.
APPLIES ANYWHERE	Whether a signal is destined for a database or a command to a weapons systems—or it travels over ethernet, radio, serial, satellite, or fiber—KST enforces integrity before action.
PROVEN, NOT THEORETICAL	U.S. Navy demonstrated wire-speed signal integrity can be achieved without slowing systems or disrupting operations.

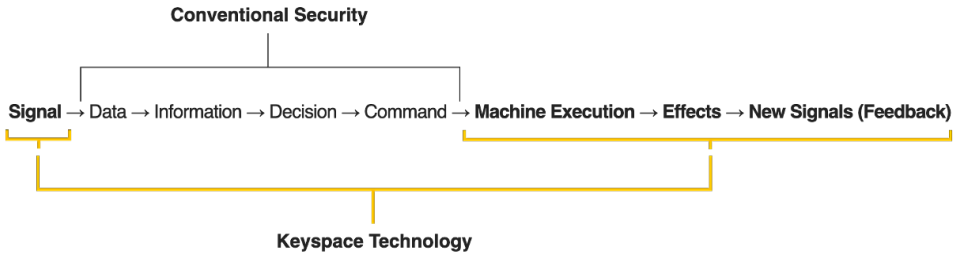
Blueskytec America Inc. | engage@blueskytec.us | +1 (980) 446 4220 | DUNS: 117751967

BLUESKYTEC

All modern systems act on machine-to-machine (M2M) communications before legitimacy is proven—this assumption of trust creates systemic operational risk.

Conventional security validates access, identity, routing, encryption, session integrity, and policy compliance within physical, software and network layers. These controls help ensure low-level messages are delivered correctly and originate from authenticated systems.

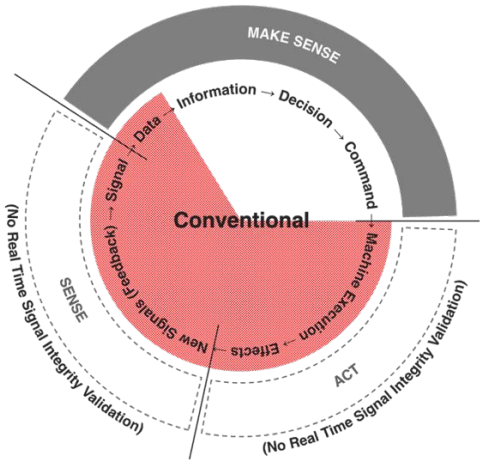
However, a properly routed, encrypted, authenticated, and policy-compliant signal can still contain an unauthorized, unsafe, replayed, or manipulated instruction. The assumption that transport integrity implies trust and execution legitimacy creates a critical gap between communication and action. KST (Keyspace Technology) closes that gap.



Operating as a hardware-enforced trust anchor across OSI Layers 1–4 and ISA-95 Levels 0–5, KST verifies message legitimacy in real time before signals become trusted data, decisions, or the commands and machine actions that turn our modern world. Unauthorized, malformed, replayed, and cross-domain injected signals are rejected before execution occurs.

WHY THIS MATTERS

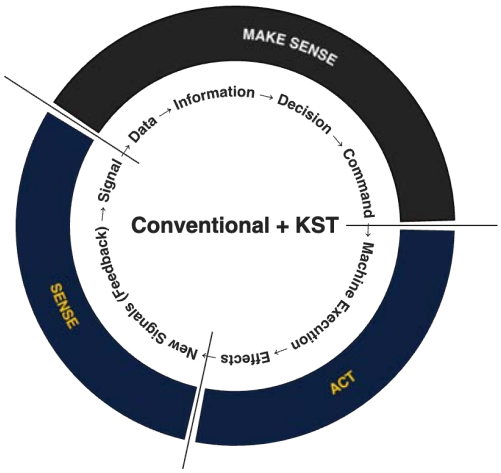
Military, industrial, autonomous, and AI-enabled systems now operate at machine speed across increasingly connected and contested environments. As these systems accelerate beyond the pace of human intervention and conventional cyber response, the ability to verify legitimacy before execution becomes foundational to mission assurance, operational continuity, resilient modernization, and operational trust.



Conventional security legitimizes access at the system, network and application layers

- Identity & Access Management — user and device identity assurance
- Configuration & Patch Control — vulnerability reduction over time
- Session Encryption & Transport Security — channel confidentiality
- Detection & Response — anomaly monitoring and incident containment

Controls do not ensure that inputs or outputs are trustworthy



KST proves M2M integrity, before they become data or action

- Authenticity — cryptographic origin validation
- Integrity — structural and cryptographic tamper resistance
- Freshness — replay resistance at discreet signal or packet level
- Authorization — rule/policy conformity before execution

Ensures inputs and outputs of human decisions are trustworthy