
KAGES
Kenneth Angus Global Energy Services

KAGES
Kenneth Angus Global Energy Services

# 'ROTECTING THE NATION'S MOST STRATEGIC ASSETS

Custom Cyber Intelligence • Cybersecurity • Electronic Warfare Countermeasures for Oil & Gas Asset

KAGES
Kenneth Angus Global Energy Services

# THE QUIET RISK TO NATIONAL VALUE

Oil & Gas Assets are not ordinary infrastructure. They are the country's most strategic economic assets and a weakness in security has a high risk of financial impact.

- **Exposed Control Systems:** Internet-facing Supervisory Control and Data Acquisition (SCADA), aging Operational Technology (OT), and unprotected Radio Frequency channels leave critical processes exposed. Most wells still rely on classic radio and SCADA systems that mainstream tools cannot fully defend.
- **One Oil Set-Up ≠ Another**: Each asset was engineered differently at different times. So every system is unique. Generic OT tools and major cybersecurity providers lack visibility into the original RF and control architecture that only engineering-rooted knowledge can reveal.
- **Accountability Gap:** When disruption occurs—especially via RF channel attacks that standard providers cannot stop—questions turn to those responsible. Foresight and platform-specific defense are the only reliable protection of value and reputation.

KAGES
Kenneth Angus Global Energy Services

# TAILORED PROTECTION FOR EACH ASSET

**No two platforms share the same engineering DNA. Effective defense must start from that reality.**

- **Platform-Specific Mapping:** Deep analysis of the original control architecture, RF communications, protocols and implementation choices unique to each facility—including classic SCADA radio and modern IIoT links.
- **Engineering-Informed Controls:** Countermeasures designed with the same technical language used by the engineers who built the systems—addressing gaps that pure software OT tools leave open.
- **Layered Cyber + Electronic Warfare Defense:** Integrated cyber intelligence, OT hardening and electronic warfare resilience that covers the RF channel itself—where major providers offer only detection or none at all.
- **Continuous Adaptation:** Ongoing refinement as threats evolve—without forcing one-size-fits-all software onto the five technology generations of wells still operating today.
- **System Warning:** Hackers take longer to get into KAGES systems with warning of attacks in real time. Able to locate source of attacks.

KAGES
Kenneth Angus Global Energy Services

# CYBERSECURITY

## TYPICAL CYBER FIRMS

- Software-centric expertise; limited RF channel protection
- Generic OT detection; no full protection of the RF channel
- Limited insight into original RF and control engineering.
- One framework applied across five generations of wells.
- Strong on IT; weak on RF jamming, spoofing and process reality

## KAGES APPROACH

- Engineering-rooted design that addresses RF channel gaps.
- Platform-by-platform customisation by engineers.
- Deep knowledge of how systems were built to extract value.
- Countermeasures matched to actual RF and control implementation.
- Integrated cyber + EW that protects what others cannot

KAGES
Kenneth Angus Global Energy Services

# THE VALUE OF WORKING WITH KAGES

- Reduced Operational Exposure: Protection calibrated to the real architecture and RF communications of each platform. No theoretical models or generic software.
- Continuity of Production: Measures that respect process safety and uptime, optimise client costs and close the RF and engineering gaps that generic tools leave open.
- Demonstrable Stewardship: Clear evidence of proactive, asset-specific defense that closes gaps left by major providers and withstands scrutiny.
- Partnership, Not Package: Integral, customised engineering solutions developed alongside the knowledge of each facility, maximising security and operational results. Standardising the operability and removing bottlenecks when operating the cyber security system.

# KAGES SYSTEM DIFFERENTIATORS

- KAGES can protect the assets that protect the Nation.
- KAGES full understand it requires more than standard tools and generic Outdated Technology (OT) platforms to protect from Cyber attacks.
- It requires partners who understand how each asset was constructed to understand how to protect it.
- KAGES can close the Radio Frequency and Engineering security gaps other Cyber Security firms cannot.

Admin@KAGES-LLC.com | +44 7837 517 327 | www.kages-LLC