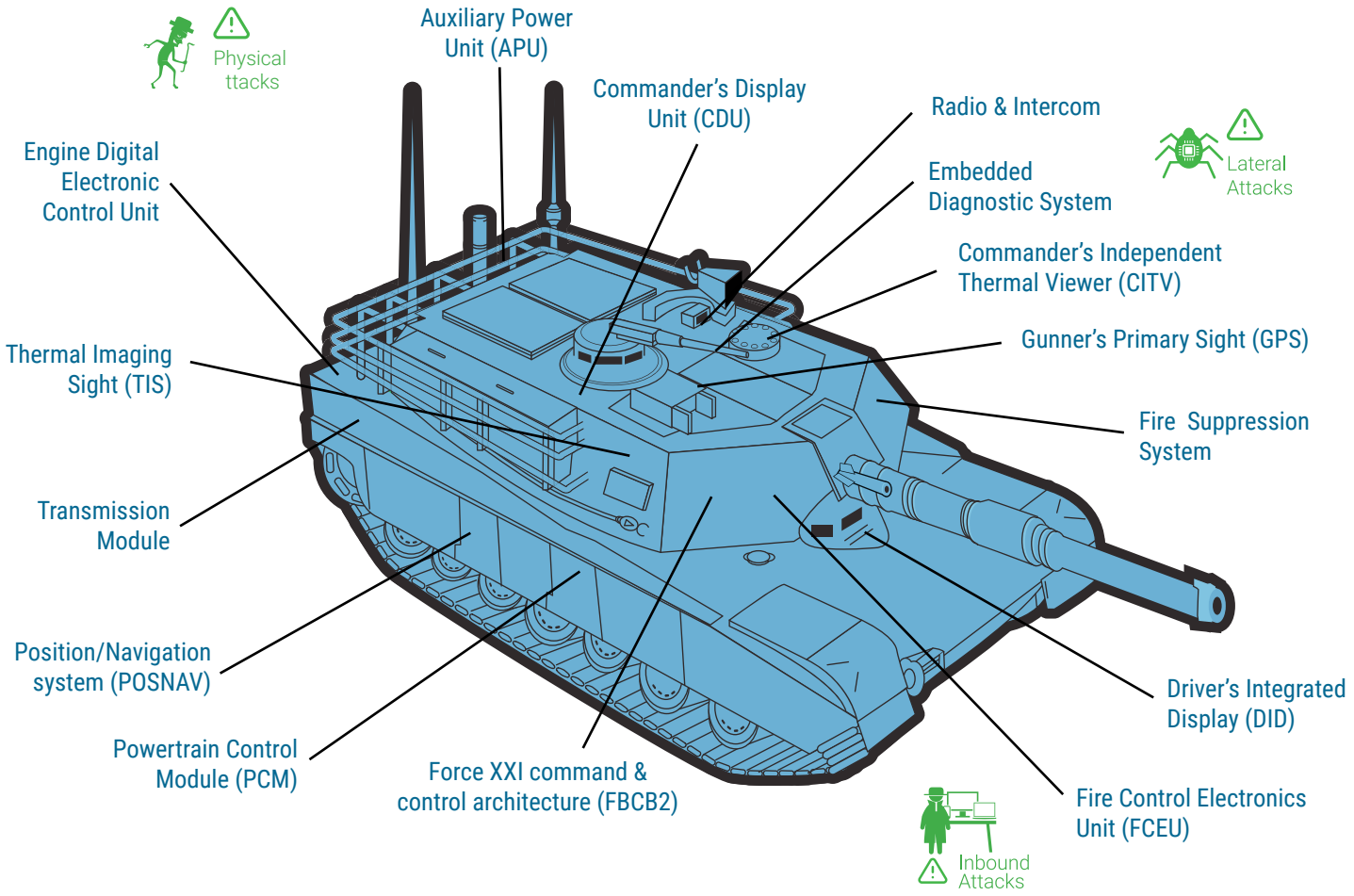
Industry Brief: Military Tank

MOCANA



Ensuring Safety, Reliability and Compliance

Cyber threats have moved from cyber crime to cyber warfare. Fire controls, sighting systems, display units, engine controls, and navigation systems may be vulnerable due to a lack of strong embedded cryptographic controls, including multi-factor authentication, secure boot, secure update, and secure, encrypted communications.

Defense manufacturers must ensure compliance with cybersecurity standards such as NIST 800-53, and FIPS 140-2 while interoperating with a broad ranges of protocols including legacy applications which are often on older deterministic bus networks. On top of that, they must design systems to operate in harsh environmental conditions while consuming a minimum of space and power.

Mocana's Proven Cybersecurity Solution

Used by more than 200 OEMs and defense contractors to protect more than 100 million devices, Mocana's IoT Security Platform is a FIPS 140-2 validated embedded cybersecurity software solution that ensures device trustworthiness and secure communications by giving defense manufacturers, integrators, and the military an easy way to:

- Speed time to market of new weapon systems
- Lower weapon system cybersecurity costs while improving cybersecurity posture
- Protect Intellectual Property
- Tamper-proof on-board computing system firmware & software
- Allow for rapid, secure, remote updating at massive scale

For more information on Mocana's comprehensive IoT Security Platform and how it can help you secure your critical infrastructure, visit our website at mocana.com or send us an email via sales@mocana.com.

A: 20 California Street, 4th floor San Francisco, CA 94111 **W:** www.mocana.com **T:**415-617-0055