FWSEC
Firmware protection

INTEGRASYS
Building success from innovation

CAPEX or SaaS

RESILIENT FIRMWARE SECURITY TOOL TO FIGHT AGAINST CYBER-ATTACKS

Successful protection of data centers, and remote assets.
Ideal for major Telco Providers and MoDs.

www.integrasys-space.com

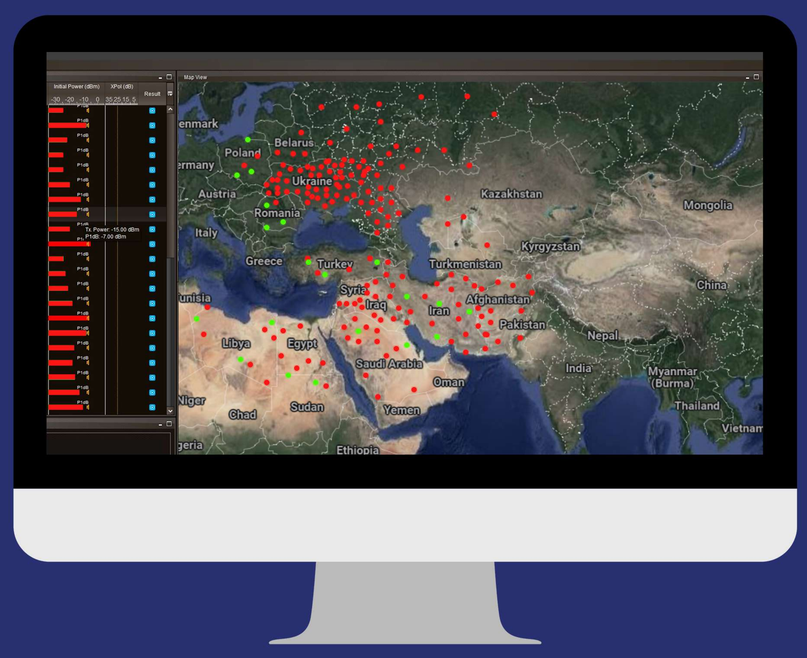
INTEGRASYS GROUP: USA, Australia, Indonesia, UAE, Spain, and Luxembourg
info.sales@integrasys-sa.com

FWSEC
Firmware protection

INTEGRASYS
Building success from innovation

Competitive Advantage

- Inmediate detection and reporting of malicious tampering attempts
- Scale up the threat towards the full system through the network infrastructure
- Configurable check-points of the firmware integrity based on user-defined policies
- Hard copy of the signature FW locally



Features

- Based on three main pillars: a firmware management server, a TPM module at the sensor platform, and an external tamper-proof private blockchain.
- The system is prepared to go back to a safe state with a digital coded footprint.
- The main layers of the system are: state-of-the-art link-level, network-level, and application-level security complemented with additional blockchain-based and multi-link out-of-channel functions
- Centralized interface to manage certificates and signatures remotely

Benefits

- Resilient protection of the devices against unauthorised changes
- Easy to be integrated with other cybersecurity products
- The security approach of the FWSEC solution allows for configurable checkpoints
- The sensors firmware includes a firmware management agent which implements -in cooperation when needed with a counterpart
- Faster recovery of the hacked assets

Company Awards