Israel Electric

# SOPHIC ZONE™

## ADVANCED OT VALIDATION PLATFORM BASED ON NEAR-REAL-TIME SIMULATION AND HARDWARE IN THE LOOP ABILITIES TO CORROBORATE OPERATIONAL AND CYBER STURDINESS

In critical infrastructure, industry, manufacturing, or any other domain with large operational systems, implementing or modifying any new technology, components, configuration, process, or software can be risky. Whether they are being deployed instead of, on top of, or in parallel to what is already in place, they can have an unexpected impact on the running of the existing systems, introducing faults, causing disruption, or even bringing operations to a halt.
Sophic Zone™ is a non-intrusive, non-destructive breakthrough solution that enables you to emulate, simulate and validate the operational processes of your ICS/ OT/ SCADA systems on a day-to-day basis. Cost-effectively, quickly and flexibly building a digital model of your operating system as a whole, Zone enables you to test the impact of planned changes in a near-real-time digital test environment before they go live. It also incorporates a complete cyber security scan of the system to ensure that changes won't introduce new vulnerabilities, enabling you to keep your systems working safely and securely.

**What you get**

**OT**

- Simulate and emulate your ICS, including IT and OT near-real-time operational processes, in a safe, dedicated staging environment.
- Test technologies, tools and systems on all your operating systems in different configurations, before roll out.
- Receive a detailed report, including achievements, vulnerabilities, impacts and recommendations.
- Prioritize recommended actions to significantly increase system sturdiness.
- Apply fixes and re-run tests to validate operating systems and recommendation results.

**Cyber**

- Test and validate the cyber sturdiness of your organization based on your processes and operational model, in a safe, dedicated environment.
- Run attack scenarios, based on real-life cyberattacks, to expose vulnerabilities in your operational systems.
- Analyze how long your systems, processes and services would be able to keep running in the event of a cyberattack.

Israel Electric

**How you use it**

- Lifecycle gateways: Go/ No-go to next project/ progress stage.
- Vulnerability mitigation: Eliminate superfluous risks, plan mitigation steps and validate them before deployment.
- Post-recovery: Simulate incidents post-attack/ post-compromise to validate your recovery processes.
- Changes: Assess the impact of any modifications to your system as a result of external and internal changes, validating them before deployment in your production system.

**What makes us different**

**Fully-integrated, end-to-end ICS**
Sophic Zone™ enables you to establish various simulative, dynamic CI system environments, rapidly and efficiently. Comprising CI models and physical equipment, Sophic Zone™ enables the user to run operational events and processes in near real time, alongside cyberattack simulations, to achieve a risk analysis of sustainable operation.

**Integrity mechanism**
A built-in integrity mechanism of software-based and real hardware-based (HIL) elements enables precise operation and cyber validation that can not be achieved by software-based components.

**Adaptability**
Implementation of customer-specific operational procedures and event management protocols, and a selection of mechanisms from a pre-prepared, best practice procedures library.

**Random scenarios and event procedure**
Randomly running different scenarios and events on the CI model enables the discovery of unknown logic, data paths, and vulnerabilities

**Cyberattack portfolio**
Based on complete and updated MITRE OT vulnerability models, Zone adds ICS-specific threats to its cyberattack portfolio, mimicking the mindset and actions of potential adversaries.

**Advanced risk assessment methodology**
Using a unique risk assessment methodology, Sophic Zone™ estimates risk on the fly, based on customer criticality input and best practices in the industry.

**Continuous validation of ICS cyber sturdiness**
Sophic Zone™ covers the entire system life cycle, including architecture, deployment plan, processes, procedures, and policy validation, providing reports on vulnerabilities, risk assessment, mitigation, and deployment recommendations.

About Sophic
The Sophic suite of cyber security solutions has been created and proven by the Israel Electric Corporation - one of Israel's leading critical infrastructure organizations solely responsible for supplying electricity to the whole country. Operating in a very challenging geopolitical environment, we are also one of the most targeted organizations in the world, having experienced our first cyberattack 25 years ago. This dubious distinction has driven our engineers, together with cyber security specialists from elite units in the Israel Defense Forces, to leverage the most cutting-edge technology to ensure we stay one step ahead of the threats we face.

Contact us to learn more how our solutions can benefit your organization:
**iecmarketing@iec.co.il | +972-072-3433813**