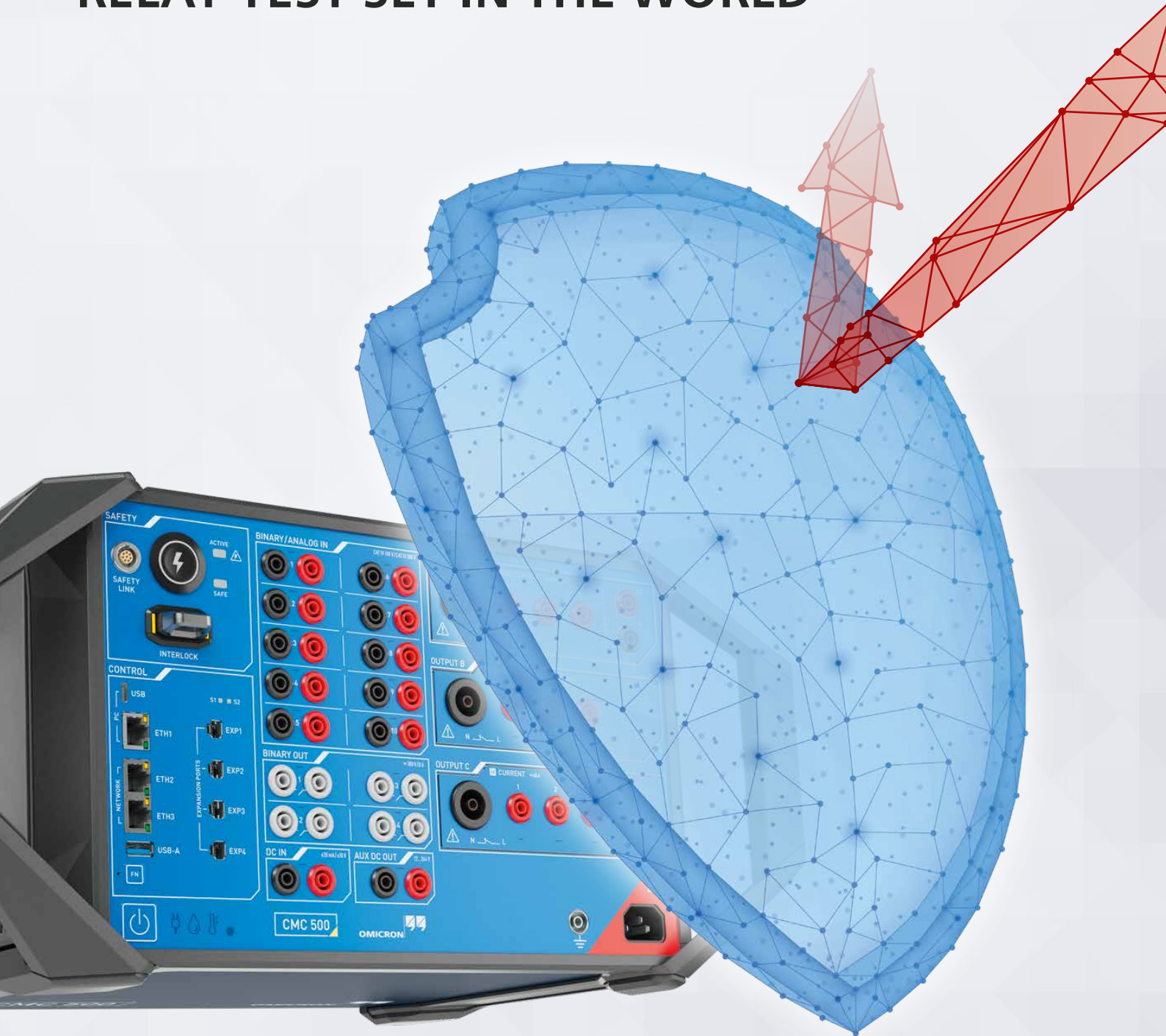
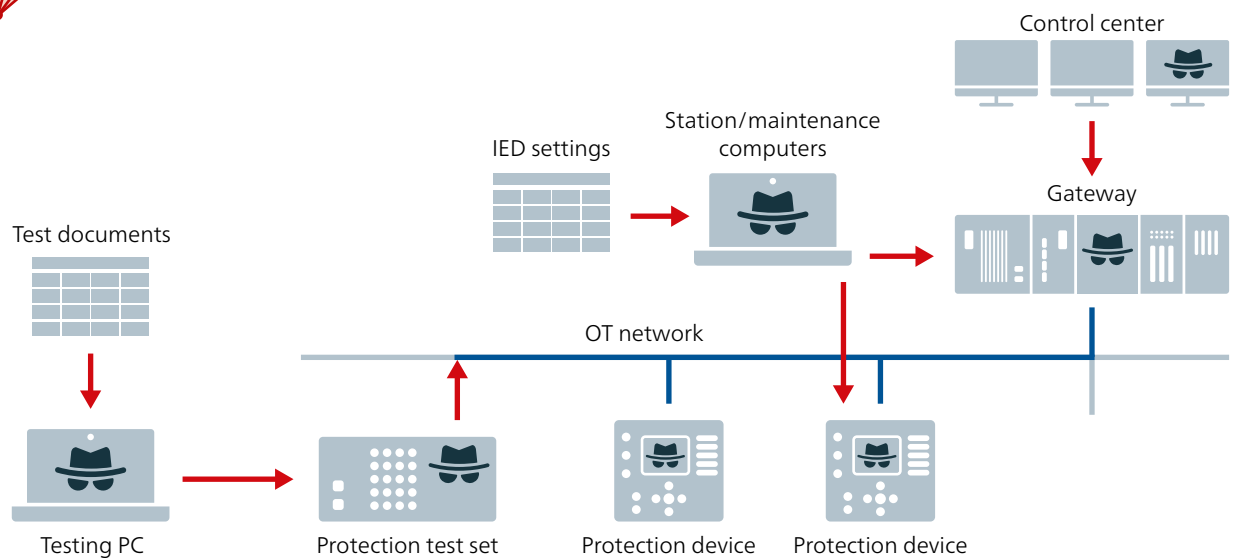


CMC 500

THE FIRST CYBER-HARDENED PROTECTION
RELAY TEST SET IN THE WORLD





If protection is inadequate, there are several ways for attackers to gain access to the station bus of critical infrastructures.

You need to take a holistic approach if you want to provide substations with effective protection against cyber-attacks. Cybersecure protection relay test sets are an essential element that should be featured in every security concept. Find out why this is and discover the extensive measures we've implemented to establish a new cybersecurity standard for protection testing.

A cyber-attack on critical infrastructure isn't just something that happens in books – and plenty of real cases exist to prove it. The most well-known incident occurred in Ukraine in 2016, when attackers exploited the connection to a control center. Since then, the necessity of protecting critical infrastructure has been stipulated through various legal requirements. For example, the NIS2 Directive (network and information security) lays out the framework for improving cybersecurity in the EU.

A comprehensive threat analysis covering as many attack vectors and vulnerabilities as possible, forms

the basis for hardening substations. As shown in a study by the Ponemon Institute, known vulnerabilities were exploited in 100% of the attacks they examined. Eliminating all vulnerabilities poses a real challenge for utilities, as there are many attack vectors, such as:

- › The connection to the control center and remote maintenance channels
- › Station and maintenance computers
- › The firmware and settings files for the protection devices themselves
- › Test sets used in the substations

While the awareness of cyber threats has grown, a closer look makes it clear that there's a lack of more specific solutions.

In terms of protection testing, the protection relay test set and the test laptop represent attack vectors that can be exploited. A secure test set has the advantage of addressing both of these attack paths. Until now, ▶

«Referring to a product as having cybersecurity by design requires more than employing measures at hardware and software levels. **Analyzing potential attack vectors begins with an entire company and encompasses all its processes.»**

cybersecure protection relay test sets weren't available in the market – but our new CMC 500 offers a solution.

Test sets can be an attack vector

We've addressed this issue by developing the CMC 500, the world's first cyber-hardened protection relay test set. But what kind of measures were required? And what do we mean by cybersecurity? Like a threat analysis for critical infrastructure, the first step was identifying potential attack vectors in test sets and addressing them step by step. The years of experience we've gained with StationGuard – our intrusion detection system (IDS) tailored to the energy sector – proved extremely helpful. A holistic approach was required to develop the CMC 500 for maximum cybersecurity. So, our company took the necessary steps in our processes, production, software, and hardware. These combined measures more than lived up to the concept of cybersecurity by design.

Secure test hardware

At the hardware level, the CMC 500 features an ISO/IEC-11889-compliant trusted platform module (TPM 2.0). This cryptoprocessor establishes the basis for several security measures, as a range of keys and certificates can be securely stored on it. This ensures communication is reliably encrypted and allows the test set to be uniquely identified – just like with a fingerprint. Attacks such as machine-in-the-middle attacks can thereby be prevented.

Likewise, checks can be carried out during the boot process using secure boot and measured boot, which check the firmware authenticity and prevent the device from starting up if these checks fail. All communication can also be protected on an additional level by setting a password.

Secure test software

Hardened hardware cannot serve its purpose without the proper test software. Therefore, we also developed our software with a clear set of guidelines. Our Secure Software Development Life Cycle (SSDLC) process was already introduced during StationGuard's development. It ensures high quality standards and code security, laying out our approach to potential vulnerabilities and their disclosure. Transparency is one of the essential cornerstones ensuring the cybersecurity of our products.

To find out more about how we handle vulnerabilities, please visit omicronenergy.com/product-security.

Secure production and repair

We don't simply rely on selected suppliers and trusted partners for production and repair, we carry out the most crucial steps ourselves. That's why only a few of our employees are authorized to set up the CMC 500's certificates and keys. The process is structured without interruption to prevent any manipulation while it's carried out. Based on a hardware security module (HSM), our internally developed software

services also ensure that keys cannot be stolen. Any attempt to physically access a key in the HSM results in its destruction. Housing the modules in our secure server room is the final stage of our comprehensive security measures.

Secure processes throughout the entire company

Whether it's hardware or software development, production, or repair, people are at the heart of all these processes. Raising awareness about data and IT security is one of the most important factors in making life for cyber criminals more difficult. In addition to ensuring that our employees are properly trained, they must demonstrate their knowledge and skills regularly as part of internal phishing simulations and ISO/IEC 27001 audits.

Redefining cybersecurity

Referring to a product as having cybersecurity by design requires more than employing measures at hardware and software levels. Analyzing potential attack vectors begins with an entire company and encompasses all its processes. This is the precise route we've taken with the CMC 500. Additionally, we support our product throughout its entire life cycle with corresponding measures, such as vulnerability management. This is why we offer a solution unlike any other for addressing the test set attack vector: our CMC 500, the first cyber-hardened protection relay test set on the market. ■

«This cryptoprocessor establishes the basis for several security measures, as a range of keys and certificates can be securely stored on it.»

Find out more
about the new
CMC 500!



 omicron.energy/new-cmc

