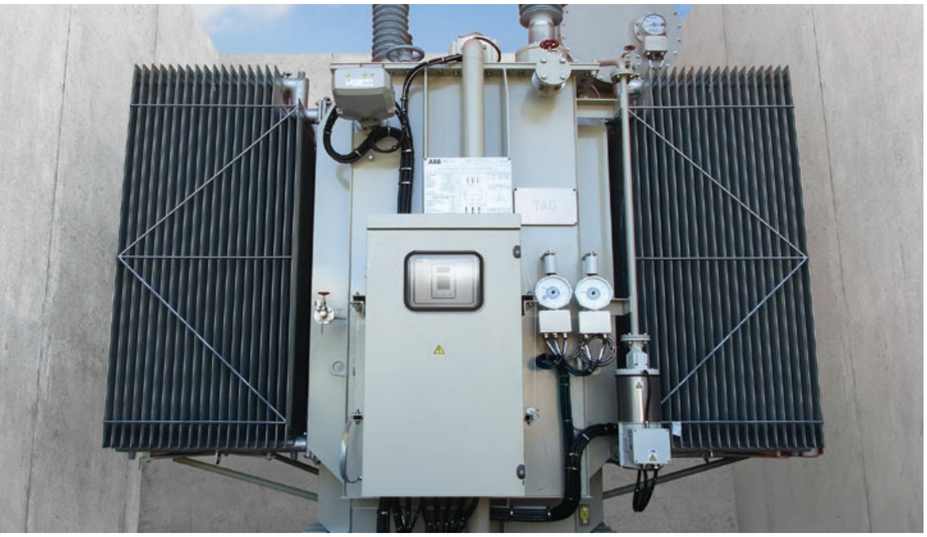
ABB TRANSFORMERS

Cyber security robustness testing

Hardening and validating CoreTec™ 4



Utilities and industries face intensifying cyber security risks. In order to increase stability, security, and robustness in its solutions, ABB has formally established cyber security robustness testing as part of the product development process.

Digital monitoring of key parameters helps operators protect their transformer investments. CoreTec™ 4 is a modular monitoring platform that collects, aggregates and analyzes critical data to assure a transformer continuously delivers optimal performance. The development of the CoreTec™ 4 included a strong focus on cyber security, an important phase of our product development process, including design, implementation, testing, release and life-cycle support. ABB is following a rigorous product development process – key activities in this process are security and robustness testing. As a result, ABB has established an independent Device Security Assurance Center (DSAC) ensuring a strong commitment towards hardening and validating.

Examples of applied test tools:

- Achilles satellite
- Mu-8000
- Defensics
- Burp Suite Professional

The test center performs a comprehensive suite of tests, including port scanning, network flooding, vulnerability and protocol fuzzing – aligning with internationally recognized cyber security standards such as IEC 62443. This is done by using a variety of best in class testing platforms as the examples listed above, as well as other complementary testing tools.

Testing is performed by highly trained specialists in close collaboration with the suppliers of the test platforms. For example, ABB testing specialists receive instruction, support and accreditation directly from the test platform suppliers. The CoreTec™ 4 has been continuously tested in different configurations with an explicit focus on operational performance. In order to evaluate product performance as precisely as possible, they are tested without additional protection such as firewalls. As a formally established practice, results from the independent DSAC testing are returned to the respective development group for resolution.

ABB relentlessly pursues a continuous improvement process, able to quickly adapt to the changing cyber security environment.

Examples of performed tests

Vulnerability scanning: Used to check for known flaws, identifying services with known vulnerabilities and testing with known exploits.

Protocol fuzzing: Uses targeted manipulation of the protocol fields beyond the specification to test for weaknesses in the protocol implementation.

Network flooding: Floods the products with too many packets with different specified rates.

ABB is the first accredited vendor lab to perform Achilles L1 and L2 ISA Secure Communication Robustness testing, an element of EDSA certification.

ABB
Transformer Services
(TRES)

www.abb.com/transformerservice

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.