Whitepaper

Cybersecurity of the RBX1 and MBX1 Platforms

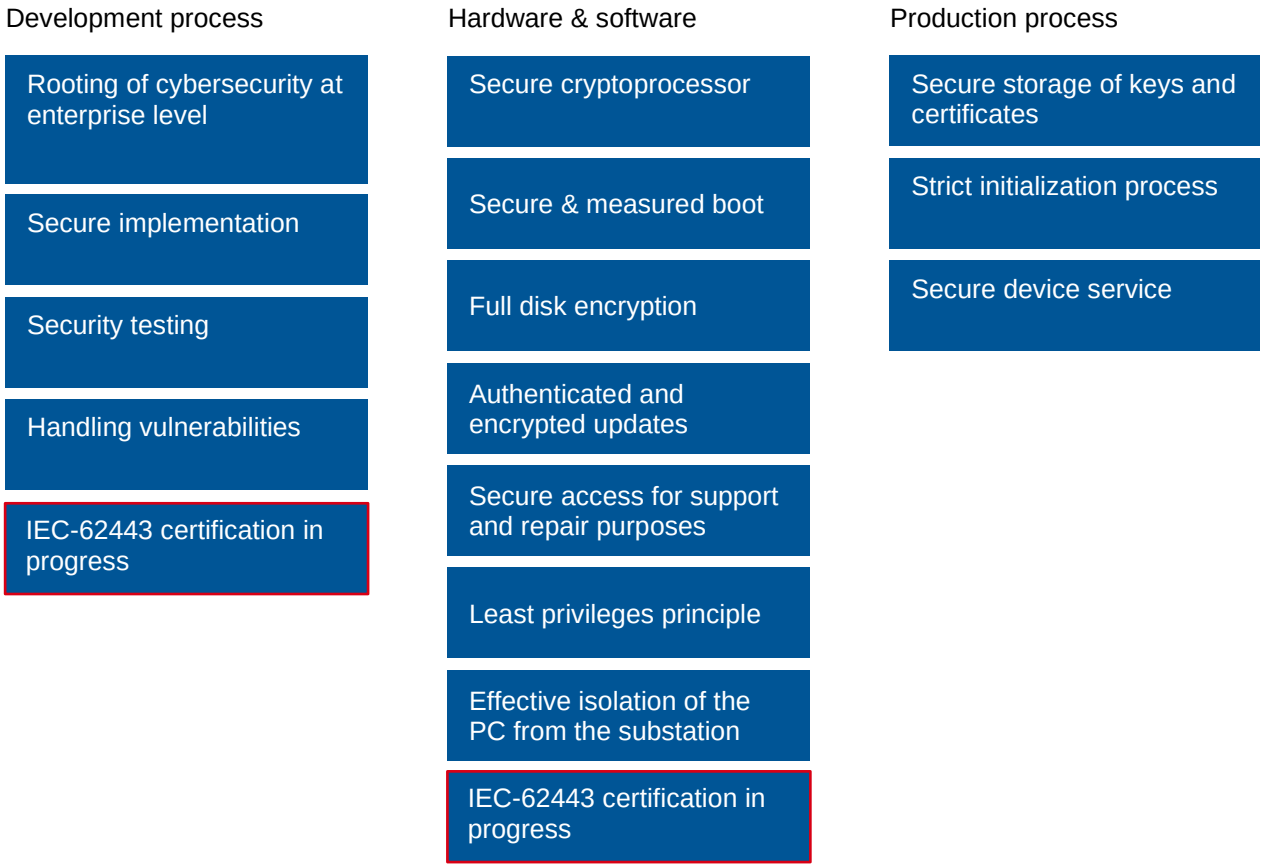
Contents

Cybersecurity of the RBX1 and MBX1 Platforms 3
Measures at hardware and software level 3
1 Secure cryptoprocessor 3
2 Secure boot and measured boot 4
3 Full disk encryption 4
4 Authenticated and encrypted firmware updates 4
5 Secure access for support and repair purposes 4
6 Execution of all processes with least privileges 4
7 Effective isolation of the Windows PC from the substation 4
Measures in the software development process 5
8 Rooting of cybersecurity at enterprise level 5
9 Secure implementation 5
10 Security testing 5
11 Handling vulnerabilities 5
Measures in the production process 6
12 Secure storage of keys and certificates 6
13 Strict initialization process 6
14 Secure device service 6
Satisfying the most stringent security requirements 6

Cybersecurity of the RBX1 and MBX1 Platforms

The RBX1 and MBX1 hardware platforms were both developed on the basis of an integrated approach to security and satisfy the most stringent demands in terms of cybersecurity and integrity. Appropriate security measures were implemented at the hardware, software, and process levels to harden the development process, the products themselves, and the production process against cyber threats. Both platforms, as well as the development process – the Secure Software Development Life Cycle (SSDLC) – are currently undergoing certification to IEC 62443.

Cybersecurity measures for the RBX1 and MBX1



This whitepaper examines the individual cybersecurity measures introduced into the design and ongoing development of the RBX1 and MBX1.

Measures at hardware and software level

State-of-the-art hardware components and a specially hardened embedded software are used to protect the RBX1 and MBX1 devices.

1 Secure cryptoprocessor

Both devices feature a separate Trusted Platform Module (TPM2.0) chip conforming to ISO/IEC-11889. The chip will securely generate and store cryptographic certificates and supports secure boot (see Section 2). Certain certificates are stored on this chip during the secure production process (see Section 13). The chip also generates unique keys that are used to encrypt the data on the device (see Section 3).

2 Secure boot and measured boot

RBX1 and MBX1 use a modern UEFI (Unified Extensible Firmware Interface) specially designed for OMICRON. The interface supports secure boot. Secure boot and measured boot mechanisms implement the boot processes of the devices. This prevents unknown software or code from being executed on a device. Every step in the boot process checks the signature of the next phase of the process before that phase is executed to ensure that RBX1 and MBX1 only load and execute software that has been signed by OMICRON. Furthermore, the secure boot function monitors the hardware and software used by the devices. If a change is detected, all the data on the device remain encrypted and the device will not start.

3 Full disk encryption

All critical data on the RBX1 and MBX1 are encrypted and can only be decrypted by the device to which they are assigned. The key used to encrypt the data is generated in the cryptochip in the RBX1 and MBX1 (see Section 1). Neither a third party nor OMICRON can decrypt the data, even if the hard disk is installed in a different MBX1 or RBX1. If the devices detect any manipulation of the hard disk contents during the boot process, they will not start. If, for example, the encryption code of a device has been compromised, this will have no effect on the customer data on another device. A new key record can only be generated by a factory reset, which requires physical access to the device.

4 Authenticated and encrypted firmware updates

Firmware upgrades for the RBX1 and MBX1 are signed using an OMICRON certificate (SHA512). This guarantees the authenticity and integrity of the firmware update file. To prevent reverse engineering, the firmware update files are also encrypted using the AES-256-CBC encryption mechanism. The keys required for decryption and signature checking of the firmware update file are securely stored on the cryptoprocessor (TPM 2.0) chip.

5 Secure access for support and repair purposes

Firmware and hardware do not contain default passwords or other backdoors. Access to the RBX1 and MBX1 for maintenance purposes can only be temporarily granted (the session is automatically terminated following a restart) and requires physical access by pressing the Reset button on the rear of the device. A challenge-response procedure instead of a password is used to grant access. The OMICRON employee has to correctly solve a cryptographic problem to obtain one-off access to the device. This problem can only be solved using the OMICRON key infrastructure (see Section 12). There are therefore no default passwords or general keys that might fall into the wrong hands.

6 Execution of all processes with least privileges

All critical functions on the RBX1 and MBX1 are distributed over various processes. Each individual process runs with the lowest level of privileges required for its tasks on the Least Privileges principle. No process has administrator or root privileges.

7 Effective isolation of the Windows PC from the substation

A Windows PC (or several PCs) running StationScout, IEDScout, or StationGuard and connected to the RBX1 or MBX1 only performs visualization and user interface functions. All other functions are carried out by the secure firmware inside the device. The RBX1/MBX1 does not transfer any data between the network ports of the substation and those of the controller. In all compatible software applications, communication with the device is authenticated and encrypted using TLS 1.3. StationScout and StationGuard only accept connections to devices that can provide the relevant security certificate. Both devices are also able to isolate the control PC and the substation network at protocol and operating system levels. A potentially infected Windows PC therefore remains effectively isolated from the substation network.

Measures in the software development process

OMICRON has created a secure software environment for the development of its software and firmware. This ensures a consistently high standard with respect to cybersecurity in the development process. Besides security training, secure implementation and cybersecurity quality assurance, the process also covers the detection and handling of potential threats and vulnerabilities associated with a specific product. The Secure Software Development Life Cycle (SSDLC) is based on a number of proven standards, such as IEC 62443-4-1, ISO 27000, and NIST 800-30r1. SSDLC ensures that various security measures are not ignored during the development process. It describes each phase of the process, as well as the standardized security measures and best practices that are used.

8 Rooting of cybersecurity at enterprise level

The SSDLC also ensures that every software development at OMICRON complies with the relevant cybersecurity standards. The process starts with an analysis of the usage context of the product and a definition of the cybersecurity requirements, together with in-depth risk modeling. Secure implementation is based on established standards and is continually verified by security testing. All the steps in the development process are documented and checked again at the end to ensure the required security level is achieved.

9 Secure implementation

Security checks are carried out throughout the implementation phase to minimize security issues. This involves extending preventive measures, such as adherence to the guidelines for secure program code, by close examination of the code in separate review loops. The twelve security principles that must currently be observed, include, for example, reducing the attack surface by minimizing the number of open interfaces, the aforementioned principle of least privileges, and the fixing of identified vulnerabilities across the entire code base.

10 Security testing

Besides monitoring the implementation, the SSDLC also controls security testing. It checks whether the specified requirements and the desired level of cybersecurity have been achieved. Standard practice in this respect involves checking the program code, dynamic and static application security testing, monitoring of application security, and software composition analysis. The latter involves the automated scrutiny of the components and vulnerabilities of every line of code on a weekly basis. Identified vulnerabilities then have to be analyzed and fixed by the development team. On the RBX1 and MBX1 platforms, penetration tests are also employed to identify any hidden security vulnerabilities.

11 Handling vulnerabilities

At OMICRON, every type of security vulnerability that affects our products is taken extremely seriously, which is why we welcome any feedback that will help us improve product security. OMICRON has therefore introduced a systematic workflow for the submission, handling, and disclosure of security vulnerabilities. Further details about the OMICRON Product Security Vulnerability Handling and Disclosure Workflow can be found at https://www.omicronenergy.com/security.

Measures in the production process

Besides the software development process, the workflows during the production of the RBX1 and MBX1 hardware and its initialization have also been examined and adapted accordingly.

12 Secure storage of keys and certificates

The secure handling of keys and certificates forms the backbone of all the remaining security measures. The secure development process and the certificates and keys in our products are generated and managed via a secure infrastructure. This key infrastructure is based on HSMs (Hardware Security Modules), which are located in secure server rooms. The HSMs prevent the keys from being extracted. OMICRON's private keys have been generated in this hardware and cannot be extracted, which means that not even OMICRON employees have access to them. All associated keys and signatures, e.g., of firmware updates, are generated directly by the hardware using a special service. Only a very small number of users are authorized to use this signature service, and even they only have access to the services that are essential for their needs. The solution even goes as far as to cause the HSM to self-destruct if an attempt is made to force it open.

13 Strict initialization process

The devices are initialized in an uninterrupted process step that only specifically authorized employees are permitted to carry out. During this process, the cryptographic certificates and keys are securely stored on the TPM2.0 chip. The relevant employees have received targeted training on the subject of security threats and have an extremely well-developed awareness of all aspects of data security in the workplace and in their dealings with external persons.

14 Secure device service

The device is reset before any repair work begins. This ensures that it no longer contains any customer data or other security-relevant information. Once the device has been repaired, the secure initialization process is repeated, at the end of which the OMICRON engineers lose their access rights. Renewed access will only be possible when the customer issues its challenge file again (see Section 5).

Satisfying the most stringent security requirements

All the measures implemented on the RBX1 and MBX1 platforms and in the StationScout and StationGuard applications are re-evaluated at predefined intervals as part of a process of continuous improvement. This ensures that all products will continue to satisfy the most stringent requirements in terms of cybersecurity and integrity.

OMICRON works passionately on pioneering ideas to make energy systems safer and more reliable. With our innovative solutions, we are facing up to the present and future challenges in our sector. We are totally committed to supporting our customers: We take their needs seriously, offer them exceptional on-site support, and share our expertise and experience.

The OMICRON Group develops innovative technologies for all areas of electrical power systems. At the heart of its activities are the electrical testing of medium and high-voltage equipment, protection tests, the testing of digital substations, and cybersecurity. Customers around the world put their faith in our user-friendly solutions and value their accuracy, speed, and quality.

We have been active in the electrical power industry since 1984 and can boast many years of in-depth experience in the sector. Approximately 900 employees at 26 sites support customers in more than 160 countries. Our Technical Support Team is on call 24/7.

You can find more information, an overview of the available literature as well as detailed contact information for our worldwide offices on our website.

www.omicronenergy.com