

CERTIFICATE

for a System with Cybersecurity Requirements as per
IEC 62443-4-1 : 2018
IEC 62443-4-2 : 2019

In accordance with TÜV NORD CERT procedures, it is hereby certified that

Bachmann electronic GmbH
Kreuzäckerweg 33
AT-6800 Feldkirch
Austria



meets the requirements of the standards listed above with the following development:

Processor Modules:

MC206/MC212/MC220, MC205/MC210, MX207/MX213/MX220 and MH212/MH230

Certificate Registration No. 44 331 24070502

Audit Report No. 3538 7270

Valid from 2025-04-11

Valid until 2028-04-10

Initial certification 2025



Certification Body
at TÜV NORD CERT GmbH

Essen, 2025-04-11

This certification was conducted in accordance with the TÜV NORD CERT auditing and certification procedures and is subject to regular surveillance audits.

ANNEX

Annex 1, page 1 of 3

to Certificate Registration No. 44 331 24070502

- Remarks:** To perform an assessment of a complete cybersecurity-related system, all relevant requirements of the IEC 62443 series of standards must be applied to the overall system in which the assessed Processor Modules are to be integrated for the required security levels.
- The assessed Processor Modules are designed as a “generic component” that requires an application software, not developed by Bachmann electronic GmbH, to operate in the final application. For an IEC 62443 conformity statement of the final application, it is required to assess the Controller component including the application software.
- The Security Levels as documented in this Annex can only be fulfilled if software version M-Base V4.75R or a later version is used.
- *)** The achievable Security Level depends on the communication interface and the communication path under consideration (please refer to the appendix of the Security Manual for further details)
 - **)** The specified achievable Security Level requires compensating countermeasures to be implemented on the Processor Modules on application programming level.
 - ***)** The specified achievable Security Level requires compensating countermeasures to be implemented externally of the assessed Processor Modules.
- For further information related to the fulfilment of the Security-Levels listed in this Annex, please also refer to the “M-Base M200 User Manual”, the “Security Manual” and referenced documentation that is provided in its latest available version.



Certification Body
at TÜV NORD CERT GmbH

Essen, 2025-04-11

ANNEX

Annex 1, page 2 of 3

to Certificate Registration No. 44 331 24070502

The assessed component including its user documentation is compliant with the following Security-Levels:

FR 1: Identification and authentication control:

CR 1.1: Human user identification and authentication	SL 2 ⁾
CR 1.2: Software process and device identification	SL 2 ⁾
CR 1.3: Account management	SL 2
CR 1.4: Identifier management	SL 2
CR 1.5: Authenticator management	SL 2
EDR 1.6: Wireless access management	n/a
CR 1.7: Strength of password-based authentication	SL 2
CR 1.8: Public key infrastructure certificates	SL 2 ⁾
CR 1.9: Strength of public key authentication	SL 2 ⁾
CR 1.10: Authenticator feedback	SL 2
CR 1.11: Unsuccessful login attempts	SL 2
CR 1.12: System use notification	n/a
CR 1.13: Access via untrusted networks	n/a
CR 1.14: Strength of symmetric key-based authentication	SL 2

FR 2: Use control:

CR 2.1: Authorization enforcement	SL 2 ⁾
CR 2.2: Wireless use control	n/a
CR 2.3: Use control for portable and mobile devices	n/a
EDR 2.4: Mobile code	n/a
CR 2.5: Session lock	SL 2 ⁾
CR 2.6: Remote session termination	SL 2
CR 2.7: Concurrent session control	SL 2
CR 2.8: Auditable events	SL 2
CR 2.9: Audit storage capacity	SL 2
CR 2.10: Response to audit processing failures	SL 2
CR 2.11: Timestamps	SL 2
CR 2.12: Non-repudiation	SL 2
EDR 2.13: Use of physical diagnostic and test interfaces	SL 2


Certification Body
at TÜV NORD CERT GmbH

Essen, 2025-04-11

ANNEX

Annex 1, page 3 of 3

to Certificate Registration No. 44 331 24070502

FR 3: System integrity:

CR 3.1: Communication integrity	SL 2
EDR 3.2: Malicious code protection	SL 2
CR 3.3: Security functionality verification	SL 2 ^{***})
CR 3.4: Software and information integrity	SL 2 ^{**}) or ^{***})
CR 3.5: Input validation	SL 2
CR 3.6: Deterministic output	SL 2
CR 3.7: Error handling	SL 2 ^{**})
CR 3.8: Session integrity	SL 2
CR 3.9: Protection of audit information	SL 2
EDR 3.10: Support for updates	SL 1
EDR 3.11: Physical tamper resistance and detection	SL 1
EDR 3.12: Provisioning product supplier roots of trust	SL 1
EDR 3.13: Provisioning asset owner roots of trust (VxWorks7 only)	SL 2 ^{**})
EDR 3.14: Integrity of the boot process	SL 1

FR 4: Data confidentiality:

CR 4.1: Information confidentiality	SL 2
CR 4.2: Information persistence	SL 2
CR 4.3: Use of cryptography	SL 2

FR 5: Restricted data flow:

CR 5.1: Network segmentation	SL 2
CR 5.2: Zone boundary protection	n/a
CR 5.3: General purpose person-to-person communication restrictions	n/a
CR 5.4: Application partitioning	n/a

FR 6: Timely response to events:

CR 6.1: Audit log accessibility	SL 2
CR 6.2: Continuous monitoring	SL 2

FR 7: Resource availability:

CR 7.1: Denial of service protection	SL 2
CR 7.2: Resource management	SL 2 ^{**})
CR 7.3: Control system backup	SL 2 ^{***})
CR 7.4: Control system recovery and reconstitution	SL 2 ^{**})
CR 7.5: Emergency power	n/a
CR 7.6: Network and security configuration settings	SL 2
CR 7.7: Least functionality	SL 2
CR 7.8: Control system component inventory	SL 2



Certification Body
at TÜV NORD CERT GmbH

Essen, 2025-04-11