CYBERSECURITY COMPLIANCE ASSESSMENT

CYBERSECURITY COMPLIANCE REPORT

MBLogger 1000 Pro (192.168.10.204) — SCADA Cybersecurity Standard Controls Assessment

Prepared For	**MB Control and Systems Pvt Ltd**
Report Version	Version 1.0
Report Date	March 2026
Assessment Period	03 December 2025 – 18 February 2026
Prepared By	**TuxCentrix Consultancy Pvt. Ltd**
Standard	IEC 62351 Series (Parts 3, 5, 6, 7, 8)

Disclaimer

This report has been prepared by **TuxCentrix Consultancy Pvt. Ltd.** for the exclusive use of **MB Control and Systems Pvt Ltd.** All findings, observations, and recommendations are based on the evidence reviewed and technical testing performed during the assessment period. This document is confidential and must not be reproduced or shared without prior written consent.

All recommendations are provided on an 'as-is' basis. The assessment team assumes no liability for any actions taken or not taken based on the contents of this report.

Document Control

Field	Details
Document Title	MBLogger 1000 Pro Cybersecurity Compliance Report
Version	1.0
Prepared By	**Tuxcentrix Security Team**
Approved By	**Sobin Joseph**
Release Date	March 2026

Table of Contents

1. Executive Summary

This report presents the compliant control position for the MBLogger 1000 Pro at IP address 192.168.10.204. The assessment evaluated the device and directly applicable SCADA cybersecurity controls against the applicable standard series, covering technical controls, evidence documentation, and governance requirements.

The assessment encompassed an evidence review, on-site vulnerability assessment (December 2025), a post-remediation retest (February 2026), and a device-specific compliance analysis against the applicable control requirements.

Summary of Strengths

- RBAC is implemented on MBLogger 1000 Pro with four defined roles: Maint, Admin, Operator, and Viewer.
- A valid SSL/TLS certificate `mbcs-ssl-20251212` is deployed and deprecated TLS 1.1 has been disabled.
- OT VLAN segmentation evidence has been submitted for the MBLogger operating environment.
- The vulnerability assessment and February 2026 retest provide a verified baseline for MBLogger compliance tracking.

2. Assessment Scope & Objectives

2.1 Objectives

- Evaluate the SCADA network infrastructure against the applicable cybersecurity standard. The assessment was only to check the functionalities which are User Accounts & RBAC, Trusted SSL/TLS Certificates Deployed, TLS Version Enforcement (1.2 / 1.3 only) and Vulnerability Assessment Completed.
- Identify control implementation status through evidence review and technical testing.
- Review governance, policy, and documentation provisions.
- Validate post-remediation effectiveness through retest.
- Provide a structured compliance view for the in-scope asset.

2.2 Standards Referenced

Description
Communication network and system security — TCP/IP profiles
Security for IEC 60870-5 and derivatives (Modbus, DNP3)
Security for IEC 61850 profiles
Network and system management (NSM) data object models
Role-based access control for power systems
Industrial Automation and Control Systems (IACS) security
Guide to Industrial Control Systems Security

2.3 Assessment Methodology

- Automated vulnerability scanning using Nessus Professional and Nmap.
- Manual verification of identified findings.
- Evidence-based review of submitted documentation and configuration screenshots.
- Post-remediation retest to validate closure of identified vulnerabilities.
- Governance and policy review against applicable security requirements.

3. Asset Inventory

One (1) asset within the SCADA network operating on the 192.168.10.0/24 subnet is in scope for this device-specific assessment: MBLogger 1000 Pro (192.168.10.204).

No.	Device	Make / Model	IP Address	Firmware	Serial No.	Role
1	**MBLogger 1000 Pro**	MBCS / MBLogger1000-Pro	192.168.10.204	9.00.2	2508XP00485	Data Logger / SCADA RTU

4. Cybersecurity Assessment by Domain

Each below control is assessed as Compliant based on the evidence reviewed.

4.1 MBLogger 1000 Pro

Control / Requirement	Status	Evidence & Gap	Recommendation/ Area of improvement
User Accounts & RBAC	**Compliant**	Evidence: Full RBAC table submitted with 4 roles: Maint (SuperUser), Admin, Operator, Viewer. Role permissions documented.	Maintain role separation. Conduct periodic access review to prevent privilege creep.

4.2 Certificates & Encryption

Control / Requirement	Status
Trusted SSL/TLS Certificates Deployed	**Compliant**
TLS Version Enforcement (1.2 / 1.3 only)	**Compliant**

4.3 Vulnerability Management

Control / Requirement	Status
Vulnerability Assessment Completed	**Compliant**

5. Conclusion

The Cybersecurity Compliance Assessment for MBLogger 1000 Pro at 192.168.10.204 confirms that the controls presented in this report are recorded as compliant.

For TuxCentrix Consultancy (P).Ltd.

Authorised Signatory / Director

TuxCentrix Consultancy Private Limited
KAKKANAD
PIN : 682021

Annexure A — Abbreviations

Acronym	Full Form
ACL	Access Control List
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
FTP	File Transfer Protocol
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MODBUS	A serial communications protocol used in OT environments
NTP	Network Time Protocol
OT	Operational Technology
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
RBAC	Role-Based Access Control
SCADA	Supervisory Control and Data Acquisition
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VA	Vulnerability Assessment
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

Annexure B — SCADA Cybersecurity Standard Evidence Status Summary

Final evidence status as of March 2026. This annexure contains only the controls presented as compliant.

Area	Control	Status	Remarks
MBLogger	RBAC / User accounts	**Compliant**	4-role RBAC fully documented and submitted
Certs	Trusted SSL/TLS certs	**Compliant**	Certificate 'mbcs-ssl-20251212' deployed; VA findings closed
Encryption	TLS 1.2/1.3 enforcement	**Compliant**	TLS 1.1 disabled; confirmed via Nmap scan in retest
Vuln. Mgmt.	Vulnerability assessment	**Compliant**	Full VA and retest completed