Jiayu Energy Technology Co., Ltd PV Microinverter RED DA Cybersecurity Test Report

Jiayu Energy Technology Co., Ltd
Unit 1, Building 3, No.3 Nanshan Road, Songshan Lake Park. Dongguan City. 523000 GUANGDONG P.R. CHINA

Attn: Pachi Hu, jet@jydet.com

REPORT NUMBER
CPRW-ESH-P25061990

COMPLIED BY
BUREAU VERITAS LCIE CHINA COMPANY LIMITED

ISSUE DATE
July 6, 2025

PAGES
16

DOCUMENT CONTROL NUMBER
RPTMIN-EN18031-Rev.01 (April 01, 2025)

Shaping a World of Trust

List of Revisions

REV.	DATE	REVISION DETAILS	AUTHOR	QA / REVIEW
1.0	July 6, 2025	Initial Release	Atlas Huang	Lukas Su

Issuing Office: Bureau Veritas LCIE China Company Limited

Disclaimer

Bureau Veritas LCIE China Company Limited Location

SHANGHAI

Building 4, No. 518, Xin Zhuan Road,
CaoHeJing SongJiang High-Teck Park,
Shanghai P.R.C. (201612)

Tel.: +86 21 6195 7000
Fax: +86 21 6195 7001
E-mail: BVLCIEMKT@bureauveritas.com

Table of Contents

List of Figures

List of Tables

1. Device Under Test

1.1. Testing Sponsor

Jiayu Energy Technology Co., Ltd

Unit 1, Building 3, No.3 Nanshan Road, Songshan Lake Park. Dongguan City. 523000 GUANGDONG P.R. CHINA

Contact: Pachi Hu

jet@jydet.com

1.2. Configuration Details

Date of the Statement:	July 6, 2025
DUT Name:	PV Microinverter
Brand / Trademark:	
Software / Firmware Version:	0147

1.3. Testing Participants

Report Prepared and Checked By:

Atlas Huang

Technical Reviewer

Lukas Su

Signature: Atlas Huang

Signature: Lukas Su

1.4. Product Images

The product under the testing is shown below.

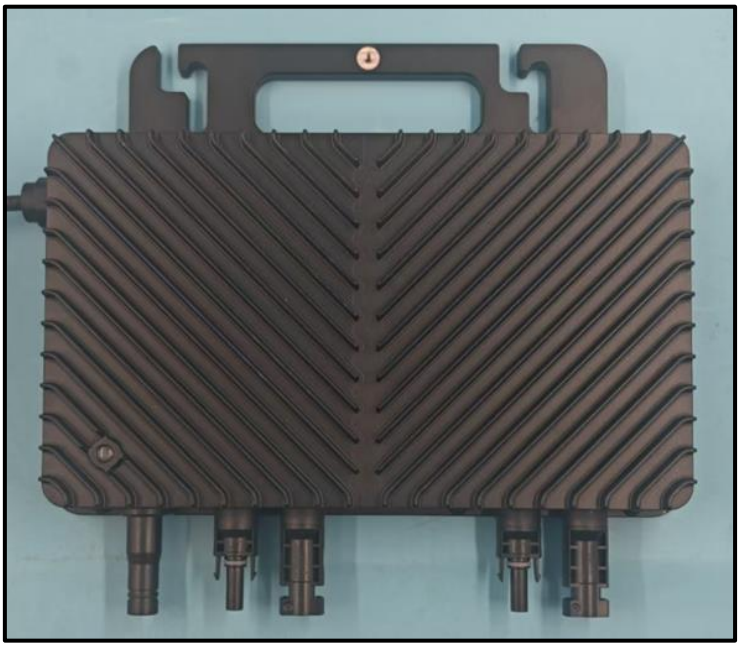

Figure 1 – Images of PV Microinverter

1.5. Workstation Setup

Table 1 – List of All Components Used in the Testing

Hardware Components Used in the Testing Included:
a. VA Computer Running Kali Linux 2024.4
Software Components Used in the Testing Included:
a. Wireshark v4.4.5 b. Burp Suite Community Edition 2025.1.4 c. Nmap v7.95-3 d. Hping3 v3.a2.ds2 e. Scapy v2.6.1 f. Tcpdump v4.99.5 g. Openssl v3.4.1 h. Braktooth Sniffer v1.0 i. SniffLE v1.10.0 j. LTESniffer v2.1.0
Vendor Supplied Components Used in the Testing Included:
k. None

1.6. Scope of Application

Table 2 – List of Models

PV Microinverter			
01	JMI-800		

The testers checked the consistency following the same cybersecurity baseline policy between the models based on the above list, and they used the same software system version and system architecture. The laboratory is only responsible for the results of the samples currently under test.

2. Introduction

2.1. Background

The client, Jiayu Energy Technology Co., Ltd, has produced a line of wireless equipment under the brand of JET. The PV Microinverter is falling into the scope as the description of (EU) 2022/30 Article 3(3) Points (d) and (e). The report is specific to the JMI-800.

This report is intended to document that Bureau Veritas LCIE China Company Limited has conducted testing against the RED DA Certification using the most current tools, technology, and methods as well as using skilled security testers to identify as many security issues as possible within the scope of the engagement at the time of testing. The laboratory is only responsible for the results of the samples currently under test.

2.2. Purpose

The purpose of this testing is to demonstrate conformity of PV Microinverter against requirements of the EN 18031 Series Standard.

2.3. Scope

The product assessed in this report is the PV Microinverter, JMI-800. The scope of testing is based on the following definition of (EU) 2022/30 Supplementing Directive 2014/53/EU of Radio Equipment and EN 18031 Series Standard.

2.4. Terms and Conditions

This report is governed by, and incorporates by reference, the Conditions of Testing as posted at the date of issuance of this report at http://www.bureauveritas.com/home/about-us/our-business/cps/about-us/terms-conditions/ and is intended for your exclusive use. Any copying or replication of this report to or for any other person or entity, or use of our name or trademark, is permitted only with our prior written permission. This report sets forth our findings solely with respect to the test samples identified herein. The results set forth in this report are not indicative or representative of the quality or characteristics of the lot from which a test sample was taken or any similar or identical product unless specifically and expressly noted. Our report includes all of the tests requested by you and the results thereof based upon the information that you provided to us. Measurement uncertainty is only provided upon request for accredited tests. Statements of conformity are based on simple acceptance criteria without taking measurement uncertainty into account, unless otherwise requested in writing. You have 60 days from the date of issuance of this report to notify us of any material error or omission caused by our negligence or if you require measurement uncertainty; provided, however, that such notice shall be in writing and shall specifically address the issue you wish to raise. A failure to raise such an issue within the prescribed time shall constitute your unqualified acceptance of the completeness of this report, the tests conducted and the correctness of the report contents.

2.5. Definitions, Acronyms and Abbreviations

Table 3 – Explanation of All Abbreviations

ACM	Access Control Mechanism
API	Application Programming Interface
AU	Assessment Unit
AUM	Authentication Mechanism
CCK	Confidential Cryptographic Key(s)
CRY	Cryptography
CSP	Confidential Security Parameter
CWE	Common Weakness Enumeration
DHCP	Dynamic Host Configuration Protocol
DN	Decision Node
DoS	Denial of Service
DT	Decision Tree
E	Evidence
E.Info	Evidence Information
E.Just	Evidence Justification
GEC	General Equipment Capabilities
IC	Implementation Category
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
OS	Operating System
MitM	Man-in-the Middle
NNM	Network Monitoring Mechanism
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RLM	Resilience Mechanism
SCM	Secure Communication Mechanism
SDO	Standards Developing Organization
SQL	Structured Query Language
SSM	Secure Storage Mechanism
SSP	Sensitive Security Parameter
SUM	Secure Update Mechanism
TCM	Traffic Control Mechanism
USB	Universal Serial Bus
WLAN	Wireless Local Area Network

2.6. References

[1] European Union, “DIRECTIVE 2014/53/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC”, May 2014. Available: https://eur-lex.europa.eu/eli/dir/2014/53/oj/eng

[2] European Union, “COMMISSION DELEGATED REGULATION (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive”, Jan. 2022.
Available: https://eur-lex.europa.eu/eli/reg_del/2022/30/oj/eng

[3] European Union, “Commission Implementing Decision (EU) 2025/138 of 28 January 2025 amending Implementing Decision (EU) 2022/2191 as regards harmonised standards in support of the essential requirements of Directive 2014/53/EU of the European Parliament and of the Council that relate to cybersecurity, for the categories and classes of radio equipment specified in Delegated Regulation (EU) 2022/30”, Jan. 2025.
Available: https://eur-lex.europa.eu/eli/dec_impl/2025/138/oj/eng

[4] CEN/CENELEC, “EN 18031-1: 2024 - Common security requirements for radio equipment - Part 1: Internet connected radio equipment”, Aug. 2024.
Available:
https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:76896,2307986&cs=10961A016B31D121BA238BD7FFFB318D0

[5] CEN/CENELEC, “EN 18031-2: 2024 - Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment”, Aug. 2024.
Available:
https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:76897,2307986&cs=16C47BC0A68DBB7B14E25CA31F6D95707

[6] CEN/CENELEC, “EN 18031-3: 2024 - Common security requirements for radio equipment - Part 3: Internet connected radio equipment processing virtual money or monetary value”, Aug. 2024.
Available:
https://standards.cencenelec.eu/dyn/www/f?p=CEN:110:0::::FSP_PROJECT,FSP_ORG_ID:76898,2307986&cs=11A431AC3F4210326404F1B9726536F84

3. Test Approach

This section describes the methodology used to perform each requirement of EN 18031 Series Standard as well as the rationale behind the security mechanisms.

3.1. Methodology

The assessments are conducted by examining the documented assessment cases, not all assessment cases might be provided for every mechanism:

Table 4 – Category of Assessment

Conceptual Assessment	Examine if the provided documentation and rationale provide the required evidence (for example the rationale why a mechanism is not applicable for a specific network interface).
Functional Completeness Assessment	Examine and test if the provided documentation is complete (for example use network scanners to verify that all external interfaces are properly identified, documented and assessed)
Functional Sufficiency Assessment	Examine and test if the implementation is adequate (for example run fuzzing tools on a network interface to check if it is resilient to attacks with malformed data).

3.2. Threat Modelling and Security Risk Assessment

STRIDE is an example of a classification scheme, useful for system decomposition, for characterizing identified threats according to the kinds of exploit that are used by the attacker. The STRIDE acronym is formed from the first letter of each of the following threat categories:

Table 5 – STRIDE Model

Threat	Desired Property	Description
Spoofing	Authenticity	Illegally accessing assets by pretending you are someone else (credentials, network address)
Tampering	Integrity	Prevent malicious modification of data (including system configuration)
Repudiation	Non-repudiability	Ability to proof an action between two parties took place (and do not allow repetition)
Information Disclosure	Confidentiality	Do not disclose any information to unauthorized users (personal data, system configuration)
Denial of Service	Availability	Making a system or data unavailable to authorized users by overloading the system
Elevation of Privilege	Authorization	An unprivileged user gains privileged access and could compromise the entire system

Each security property has primary mitigation techniques to address the threats that could be identified by a risk management process.

Table 6 – List of Mitigations for Security Threats

Mitigation Technique	Description
Identify	Process of recognizing the attributes that identify the object.
Protect	The ability to limit or contain the impact of a potential cybersecurity event. • Prevent: Measures that avoid or preclude a cybersecurity event. • Limit: Measures intended to reduce the impact of a cybersecurity event.
Detect	Security controls are intended to detect a cybersecurity event.
Respond	Appropriate activities to execute regarding a detected cybersecurity event.
Recover	Appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

3.3. Assignment of Verdict

In order to assess the security features of a connected device, the laboratory has developed the test plan according to EN 18031 Series Standard for classifying the results during the assessment conducted.

Table 7 – Explanation of Verdict Assigned

Classification	Description
PASS	The verdict PASS for the assessment case is assigned if: **Conceptual Assessment:** • At least one path through the decision tree ends with “PASS”; and • No Path though the decision tree ends with “FAIL”; and • The information provided is correct justifications for all paths through the decision tree. **Functional Completeness Assessment:** • All security assets and network assets found are documented. **Functional Sufficiency Assessment:** • There is no evidence that the mechanism documented is not implemented.
FAIL	The verdict FAIL for the assessment case is assigned if: **Conceptual Assessment:** • A path though the decision tree ends with “FAIL”; or • A justification provided is not correct or missing for a path though the decision tree. **Functional Completeness Assessment:** • A security asset or network asset is found which is not documented. **Functional Sufficiency Assessment:** • There is evidence that the mechanism documented is not implemented.
NOT APPLICABLE (N/A)	The verdict NOT APPLICABLE (N/A) for the assessment case is assigned if: **Conceptual Assessment:** • The assessment case is assigned otherwise. **Functional Completeness Assessment:** • The assessment case is assigned otherwise. **Functional Sufficiency Assessment:** • The assessment case is assigned otherwise.

The testers shall conduct the assessment and conclude the result considering the cybersecurity risk analysis based on the intended user group and usage scenarios of the product.

4. Test Result Summary

Introduction

The client, Jiayu Energy Technology Co., Ltd, has produced a line of wireless equipment under the brand of JET. The PV Microinverter is falling into the scope as the description of (EU) 2022/30 Article 3(3) Points (d) and (e). The report is specific to the JMI-800.

This report is intended to document that Bureau Veritas LCIE China Company Limited has conducted testing against the RED DA Certification using the most current tools, technology, and methods as well as using skilled security testers to identify as many security issues as possible within the scope of the engagement at the time of testing. The laboratory is only responsible for the results of the samples currently under test.

Scope of Review

Article 3(3), Point (d): Any radio equipment that can communicate over the internet, whether it communicates directly or via any other equipment (Internet-connected Radio Equipment).

Article 3(3), Point (e): Any of the following radio equipment, if that radio equipment is capable of processing, within the meaning of Article 4(2) of Regulation (EU) 2016/679, personal data, as defined in Article 4(1) of Regulation (EU) 2016/679, or traffic data and location data, as defined in Article 2, points (b) and (c), of Directive 2002/58/EC.

Article 3(3), Point (f): Any internet- connected radio equipment, if that equipment enables the holder or user to transfer money, monetary value or virtual currency as defined in Article 2, point (d), of Directive (EU) 2019/713.

Table 8 – PV Microinverter Corresponding to Regulations

Scope	Standard	Involved
Article 3(3), Point (d)	EN 18031-1: 2024	☑
Article 3(3), Point (e)	EN 18031-2: 2024	☑
Article 3(3), Point (f)	EN 18031-3: 2024	

Results

Overall, Jiayu Energy Technology Co., Ltd has provided a reasonable level of security appropriate for the mechanisms to protect the assets of the device. Further, the PV Microinverter has met all of the applicable requirements in all of the applicable clauses of the EN 18031 Standard Series based on a cybersecurity risk analysis and considering the intended user group and usage scenarios of the product.

Table 9 – EN 18031 Series Summary of Results

Provision	Description	Verdict
ACM – Access Control Mechanism		
ACM-1	Applicability of Access Control Mechanisms	**PASS**
ACM-2	Appropriate Access Control Mechanisms	**PASS**
ACM-3	Default Access Control for Children in Toys	**N/A**
ACM-4	Default Access Control to Children's Privacy Assets for Toys and Childcare Equipment	**N/A**
ACM-5	Parental / Guardian Access Controls for Children in Toys	**N/A**
ACM-6	Parental / Guardian Access Controls for Other Entities' Access to Managed Children's Privacy Assets in Toys	**N/A**
AUM – Authentication Mechanism		
AUM-1-1	Requirement Network Interface	**PASS**
AUM-1-2	Requirement User Interface	**PASS**
AUM-2-1	Requirement One Factor Authentication	**PASS**
AUM-2-2	Requirement Two Factor Authentication	**N/A**
AUM-3	Authenticator Validation	**PASS**
AUM-4	Changing Authenticators	**PASS**
AUM-5-1	Requirement for Factory Default Passwords	**PASS**
AUM-5-2	Requirement for Non-factory Default Passwords	**PASS**
AUM-6	Brute Force Protection	**PASS**
SUM – Secure Update Mechanism		
SUM-1	Applicability of Update Mechanisms	**PASS**
SUM-2	Secure Updates	**PASS**
SUM-3	Automated Updates	**PASS**
SSM – Secure Storage Mechanism		
SSM-1	Applicability of Secure Storage Mechanisms	**PASS**
SSM-2	Appropriate Integrity Protection for Secure Storage Mechanisms	**PASS**
SSM-3	Appropriate Confidentiality Protection for Secure Storage Mechanisms	**PASS**
SCM – Secure Communication Mechanism		
SCM-1	Applicability of Secure Communication Mechanisms	**PASS**
SCM-2	Appropriate Integrity and Authenticity Protection for Secure Communication Mechanisms	**PASS**
SCM-3	Appropriate Confidentiality Protection for Secure Communication Mechanisms	**PASS**
SCM-4	Appropriate Replay Protection for Secure Communication Mechanisms	**PASS**
RLM – Resilience Mechanism		
RLM-1	Applicability and Appropriateness of Resilience Mechanisms	**PASS**

NMM – Network Monitoring Mechanism		
NMM-1	Applicability and Appropriateness of Network Monitoring Mechanisms	**N/A**
TCM – Traffic Control Mechanism		
TCM-1	Applicability of and Appropriate Traffic Control Mechanisms	**N/A**
LGM – Logging Mechanism		
LGM-1	Applicability of Logging Mechanisms	**PASS**
LGM-2	Persistent Storage of Log Data	**N/A**
LGM-3	Minimum Number of Persistently Stored Events	**N/A**
LGM-4	Time-Related Information of Persistently Stored Log Data	**N/A**
DLM – Deletion Mechanism		
DLM-1	Applicability of Deletion Mechanisms	**PASS**
UNM – User Notification Mechanism		
UNM-1	Applicability of User Notification Mechanisms	**PASS**
UNM-2	Appropriate User Notification Content	**PASS**
CCK – Confidential Cryptographic Keys		
CCK-1	Appropriate CCKs	**PASS**
CCK-2	CCK Generation Mechanisms	**PASS**
CCK-3	Preventing Static Default Values for Preinstalled CCKs	**PASS**
GEC – General Equipment Capabilities		
GEC-1	Up-To-Date Software and Hardware with No Publicly Known Exploitable Vulnerabilities	**PASS**
GEC-2	Limit Exposure of Services Via Related Network Interfaces	**PASS**
GEC-3	Configuration Of Optional Services and The Related Exposed Network Interfaces	**PASS**
GEC-4	Documentation Of Exposed Network Interfaces and Exposed Services via Network Interfaces	**PASS**
GEC-5	No Unnecessary External Interfaces	**PASS**
GEC-6	Input Validation	**PASS**
GEC-7	Documentation of External Sensing Capabilities	**N/A**
GEC-8	Equipment Integrity	**N/A**
CRY - Cryptographic		
CRY-1	Best Practice Cryptography	**PASS**

********** **END OF REPORT** **********