kaspersky

Security Maturity Certificate

Certificate holder

Systeme Electric Joint Stock Company

Russia, Moscow, st. Dvintsev, building 1 A

Date of issue	Date of expiration
15.04.2024	15.04.2026

Certified product

SystemeLogic X electronic control unit

Firmware version(s)

1.0.0

Security Maturity Target ID

2024-0002-SE-SL

Security Maturity Target and Assessment Report

https://kas.pr/9daz

Applicable models

SystemePact ACB 400-4000A air circuit breakers:
- SystemePact ACB1 frame size 400-1600A
- SystemePact ACB2 frame size 800-4000A

Vulnerability Research Report number

2024-0002-0003-VR

Terms and conditions of the certificate

1. This Certificate provides the following guarantees:
   a. that the current practices adopted to support product security are in line with the Security Maturity Target indicated on this Certificate.
   b. that the product vendor has implemented the infrastructure, organizational measures, processes, procedures, policies, tools and methods required to maintain the comprehensiveness level of all security practices defined in the Security Maturity Target and address the specific issues identified at the industry and system scope levels in the Security Maturity Target definition.
   This Certificate is issued based on the results of certification tests, including technical and vulnerability assessments.
2. All terms used in this Certificate should be construed to have meanings defined in the IIC Security Maturity Model (https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf).
3. This Certificate is valid until the Date of Expiration indicated on it, provided that the conditions of validity are not breached before that date.
4. Factors limiting the validity of this Certificate may include clear signs of failure to follow the security practices that were described as implemented when demonstrating conformance with the Security Maturity Target. Such signs may include:
   a. software vulnerabilities that were not properly addressed in accordance with the procedure and within the time frame meeting the requirements defined in the Security Maturity Target*;
   b. incidents that were not handled in accordance with the procedure and policies defined in the Security Maturity Target;
   c. demonstrated attitude towards cybersecurity risk that is significantly different from that specified in the Security Maturity Target;
   d. unavailability of important information, including information on practices implemented in accordance with the guidelines and recommendations contained in the Security Maturity Target, as well as information on the appropriate comprehensiveness level and target scope;
   e. other clear signs that the security practices described as implemented when demonstrating conformance with the Security Maturity Target were in fact not followed.
5. The Certificate can be revoked in the event of the existence of factors described in paragraph 4 above.

* Ithough the certification body has used its best effort and expertise to perform a comprehensive security analysis of the certified product, the certificate does not guarantee that all security vulnerabilities or weaknesses have been identified in the process of certification or that the product is not vulnerable or susceptible to exploitation and will not eventually be breached. This means that, if a new vulnerability is identified, the certificate will remain valid, provided that the vendor fully addresses the vulnerability in accordance with the procedure and within the time frame meeting the requirements defined in the Security Maturity Target.

Visit webpage to get full information