# GE VERNOVA

H49-2.1.0 product

Self-assessment according to IEC62443-4-2 Standard

Goal of this doccument

This document describes the conformance of the product with the security requirements of IEC62443-4-2 standard.

Legend:

-	Not Applicable
✓	Comply
▲	Partially comply
◆	Exception

Glossary

CR	**C**omponent **R**equirement
EDR	**E**mbedded **D**evice **R**equirement
EST	**E**nrollment over **S**ecure **T**ransport
FR	**F**oundational **R**equirement
HDR	**H**ost **D**evice **R**equirement
IEC	**I**nternational **E**lectrotechnical **C**ommission, standards organization; communication standard for substations and protection equipment
NDR	**N**etwork **D**evice **R**equirement
RE	**R**equirement **E**nhancement

SLC vector

Product family:	Network Switch
Product name:	H49-2.1.0
SLC=	{ 2 2 2 2 2 2 2 }

FR	Vector	Comments & Missing features for current SL
FR1	2	Except: - CR-1.9 c): check of certificate revocation status not supported - CR-1.12: system notification displayed after user authentication
FR2	2	Except: - CR-2.1 RE(2): configuration of the permissions of the roles not supported - CR-2.8: some categories not supported
FR3	2	Except: - CR-3.3: No testbook provided - CR-3.8: Session integrity partially supported
FR4	2	-
FR5	2	-
FR6	2	Except: - CR-6.2: Not tested
FR7	2	Except: - CR-7.1: Not tested - CR-7.1 RE(1): Not tested - CR-7.2: Not tested

FR 1 – Identification and authentication control (IAC)

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 1.1	Human user identification and authentication	✓	✓	✓	✓	
CR 1.1 RE (1)	Unique identification and authentication		✓	✓	✓	
CR 1.1 RE (2)	Multifactor authentication for all interfaces			⚠	⚠	May be achieved through a third party LDAP server proxy supporting
CR 1.2	Software process and device identification and authentication		✓	✓	✓	
CR 1.2 RE (1)	Unique identification and authentication			-	-	
CR 1.3	Account management	✓	✓	✓	✓	
CR 1.4	Identifier management	✓	✓	✓	✓	
CR 1.5	Authenticator management	✓	✓	✓	✓	
CR 1.5 RE (1)	Hardware security for authenticators			-	-	
CR 1.6	Wireless access management	-	-	-	-	Not applicable for embedded devices
CR 1.7	Strength of password-based authentication	✓	✓	✓	✓	
CR 1.7 RE (1)	Password generation and lifetime restrictions for human users			-	-	
CR 1.7 RE (2)	Password lifetime restrictions for all users (human, software process, or device)				⚠	
CR 1.8	Public key infrastructure certificates		✓	✓	✓	
CR 1.9	Strength of public key-based authentication		⚠	⚠	⚠	Revocation status check not implemented.
CR 1.9 RE (1)	Hardware security for public key-based authentication			-	-	
CR 1.10	Authenticator feedback	✓	✓	✓	✓	
CR 1.11	Unsuccessful login attempts	✓	✓	✓	✓	
CR 1.12	System use notification	⚠	⚠	⚠	⚠	Notification displayed after
CR 1.13	Access via untrusted networks	-	-	-	-	Not applicable for embedded devices
CR 1.14	Strength of symmetric key based authentication		✓	✓	✓	

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 1.14 RE (1)	Hardware security for symmetric key-based authentication			-	-	

FR 2 – Use control (UC)

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 2.1	Authorization enforcement	✓	✓	✓	✓	
CR 2.1 RE (1)	Authorization enforcement for all users (humans, software processes and devices)		✓	✓	✓	
CR 2.1 RE (2)	Permission mapping to roles		⚠	⚠	⚠	Applicable roles are configurable for each user
CR 2.1 RE (3)	Supervisor override			-	-	
CR 2.1 RE (4)	Dual approval				-	
CR 2.2	Wireless use control	-	-	-	-	
CR 2.3	Use control for portable and mobile devices	-	-	-	-	Not applicable
CR 2.4	Mobile code	-	-	-	-	Refer to SAR/EDR/HDR/NDR chapter
CR 2.5	Session lock	✓	✓	✓	✓	
CR 2.6	Remote session termination		✓	✓	✓	
CR 2.7	Concurent session control			-	-	
CR 2.8	Auditable events	⚠	⚠	⚠	⚠	Some events missing
CR 2.9	Audit storage capacity	✓	✓	✓	✓	
CR 2.9 RE (1)	Warn when audit record storage capacity threshold reached			-	-	
CR 2.10	Response to audit processing failure	✓	✓	✓	✓	
CR 2.11	Timestamps	✓	✓	✓	✓	
CR 2.11 RE (1)	Time synchronization		✓	✓	✓	
CR 2.11 RE (2)	Protection of time source integrity				-	
CR 2.12	Non-repudiation	✓	✓	✓	✓	
CR 2.12 RE (1)	Non-repudiation for all users				⚠	
CR 2.13	Use of physical diagnostic and test interfaces	-	-	-	-	Refer to SAR/EDR/HDR/NDR chapter

FR 3 – System integrity (SI)

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 3.1	Communication integrity	✓	✓	✓	✓	
CR 3.1 RE (1)	Communication authentication		✓	✓	✓	
CR 3.3	Security functionality verification	◆	◆	◆	◆	Security testbook missing
CR 3.3 RE (1)	Security functionality verification during normal operation				-	
CR 3.4	Software and information integrity	✓	✓	✓	✓	
CR 3.4 RE (1)	Authenticity of software and information		✓	✓	✓	
CR 3.4 RE (2)	Automated notification of integrity violations			-	-	
CR 3.5	Input validation	✓	✓	✓	✓	
CR 3.6	Deterministic output	✓	✓	✓	✓	
CR 3.7	Error handling	✓	✓	✓	✓	
CR 3.8	Session integrity	△	△	△	△	
CR 3.9	Protection of audit information		✓	✓	✓	
CR 3.9 RE (1)	Audit records on write-once media				-	
CR 3.10	Support for updates	-	-	-	-	Refer to SAR/EDR/HDR/NDR chapter
CR 3.11	Physical tamper resistance and detection	-	-	-	-	Refer to SAR/EDR/HDR/NDR chapter
CR 3.12	Provisioning product supplier roots of trust	-	-	-	-	Refer to SAR/EDR/HDR/NDR chapter
CR 3.13	Provisioning asset owner roots of trust	-	-	-	-	Refer to SAR/EDR/HDR/NDR chapter
CR 3.14	Integrity of the boot process	-	-	-	-	Refer to SAR/EDR/HDR/NDR chapter

FR 4 – Data confidentiality (DC)

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 4.1	Information confidentiality	✓	✓	✓	✓	
CR 4.2	Information persistence		✓	✓	✓	
CR 4.2 RE (1)	Erase of shared memory resources			-	-	
CR 4.2 RE (2)	Erase verification			-	-	
CR 4.3	Use of cryptography		✓	✓	✓	

FR 5 – Restricted data flow

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 5.1	Network segmentation	✓	✓	✓	✓	
CR 5.2	Zone boundary protection	-	-	-	-	Not applicable for embedded devices Refer to NDR chapter
CR 5.3	General, person-to-person communication restrictions	-	-	-	-	Not applicable for embedded devices Refer to NDR chapter
CR 5.4	Application partitioning	-	-	-	-	Not required by the standard

FR 6 – Timely response to events

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 6.1	Audit log accessibility	✓	✓	✓	✓	
CR 6.1 RE (1)	Programmatic access to audit logs			✓	✓	
CR 6.2	Continuous monitoring		◆	◆	◆	Not tested on this release

FR 7 – Resource availability

SRs and REs		SL1	SL2	SL3	SL4	Comments
CR 7.1	Denial of service protection	◆	◆	◆	◆	Not tested on this release
CR 7.1 RE (1)	Manage communication load from component		◆	◆	◆	Not tested on this release
CR 7.2	Resource management	◆	◆	◆	◆	Not tested on this release
CR 7.3	Control system backup	✓	✓	✓	✓	
CR 7.3 RE (1)	Backup integrity verification		✓	✓	✓	
CR 7.4	Control system recovery and reconstitution	✓	✓	✓	✓	
CR 7.6	Network and security configuration settings	✓	✓	✓	✓	
CR 7.6 RE (1)	Machine-readable reporting of current security settings			-	-	
CR 7.7	Least functionality	✓	✓	✓	✓	
CR 7.8	Control system component inventory		✓	✓	✓	

NDR

NDR		SL1	SL2	SL3	SL4	Comments
NDR 1.6	Wireless access management	-	-	-	-	
NDR 1.6 RE (1)	Unique identification and authentication		-	-	-	
NDR 1.13	Access via untrusted networks	⚠	⚠	⚠	⚠	Unused network ports and protocls can be disable
NDR 1.13 RE (1)	Explicit access request approval		◆	◆	◆	Not implemented
NDR 2.4	Mobile code	-	-	-	-	
NDR 2.4 RE (1)	Mobile code authenticity check		-	-	-	
NDR 2.13	Use of physical diagnostic and test interfaces		⚠	⚠	⚠	Protected by physical design
NDR 2.13 RE (1)	Active monitoring			-	-	
NDR 3.2	Protection from malicious code	✓	✓	✓	✓	
NDR 3.10	Support for updates	✓	✓	✓	✓	
NDR 3.10 RE (1)	Update authenticity and integrity		✓	✓	✓	
NDR 3.11	Physical tamper resistance and detection		✓	✓	✓	
NDR 3.11 RE (1)	Notification of a tampering attempt			-	-	
NDR 3.12	Provisioning product supplier roots of trust		◆	◆	◆	Not implemented
NDR 3.13	Provisioning asset owner roots of trust		◆	◆	◆	Not implemented
NDR 3.14	Integrity of the boot process	◆	◆	◆	◆	Not implemented
NDR 3.14 RE (1)	Authenticity of the boot process		◆	◆	◆	Not implemented
NDR 5.2	Zone boundary protection	✓	✓	✓	✓	
NDR 5.2 RE (1)	Deny all, permit by exception		✓	✓	✓	
NDR 5.2 RE (2)	Island mode			-	-	
NDR 5.2 RE (3)	Fail close			-	-	
NDR 5.3	General purpose, person to person communication restrictions	-	-	-	-	