Cyber Security Test Report

EN 18031-1:2024

Test Report produced for

Westermo Ireland

covering the testing of

Merlin Series Router

Report Number TRA-067527-41-01A

10th December 2025

General Details

Report Number	TRA-067527-41-01A
Date of Issue	10th December 2025
Total Number of Pages	168 (including appendices) 6 (not including appendices)

Test Specification	EN 18031-1:2024
Test Procedure	CYB-PRO-002
Report Blank	CYB-REP-002-1

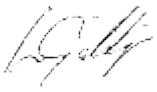
Device Under Test (DUT)	Merlin Series Router
DUT Description	Versatile Cat 4 LTE router for energy, industrial and trackside applications
Applicant	Westermo Ireland Unit A, Westland Park, Willow Rd, Fox-And-Geese, Dublin 12, D12 V598 IRELAND
Applicant Contact Information	Artur Wachowski Artur.Wachowski@westermo.com
Manufacturer	Westermo Ireland Unit A, Westland Park, Willow Rd, Fox-And-Geese, Dublin 12, D12 V598 IRELAND

Testing Laboratory	Element Materials Technology Warwick Limited
Testing Location	Unit E, South Orbital Trading Park Hedon Road, Hull HU9 1NJ United Kingdom
Date(s) of Testing	27th June 2025 – 21st November 2025

Reproduction Rights	This Test Report may only be reproduced in full, except with the explicit written permission from the Testing Laboratory.

Possible Test Case Verdicts	**PASS (Pass)**	The DUT meets the requirement of the test case
	FAIL (Fail)	The DUT fails to meet the requirement of the test case
	NC (Not Conclusive)	The DUT has only been partially assessed against the test case
	NA (Not Applicable)	The test case does not apply to the DUT
	NT (Not Tested)	The applicant has requested the test case is not to be assessed
	-	No testing necessary as per the standard
Possible Overall Verdicts	**PASS (Pass)**	The DUT meets all applicable requirements
	FAIL (Fail)	The DUT fails to meet all applicable requirements
	NC (Not Conclusive)	The DUT has not been fully assessed against all requirements
Overall Verdict	**PASS**	

Author	Gregory Parrott
Position	Protocol Test Engineer
Signature	Author signature 

Approver	Liam Giddings
Position	Department Manager – Smart Technology
Signature	Approver signature 

Test Case Verdict Summary

This section details the verdicts for each provision in the standard.

Provision ID	Provision Title	Conceptual Assessment	Completeness Assessment	Sufficiency Assessment	Overall Verdict
GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	PASS	PASS	PASS	PASS
GEC-2	Limit exposure of services via related network interfaces	PASS	PASS	-	PASS
GEC-3	Configuration of optional services and the related exposed network interfaces	PASS	PASS	PASS	PASS
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	PASS	PASS	-	PASS
GEC-5	No unnecessary external interfaces	PASS	PASS	-	PASS
GEC-6	Input validation	PASS	PASS	PASS	PASS
ACM-1	Applicability of access control mechanisms	PASS	PASS	PASS	PASS
ACM-2	Appropriate access control mechanisms	PASS	-	PASS	PASS
AUM-1-1	Applicability of authentication mechanisms (network interface)	NA	PASS	NA	PASS
AUM-1-2	Applicability of authentication mechanisms (user interface)	PASS	PASS	PASS	PASS
AUM-2	Appropriate authentication mechanisms	PASS	-	PASS	PASS
AUM-3	Authenticator validation	PASS	-	PASS	PASS
AUM-4	Changing authenticators	PASS	-	PASS	PASS
AUM-5-1	Password strength (factory default passwords)	PASS	-	PASS	PASS
AUM-5-2	Password strength (non-factory default passwords)	NA	-	NA	NA
AUM-6	Brute force protection	PASS	-	PASS	PASS
SUM-1	Applicability of update mechanisms	PASS	-	PASS	PASS
SUM-2	Secure updates	PASS	-	PASS	PASS
SUM-3	Automated updates	PASS	-	NA	PASS
SSM-1	Applicability of secure storage mechanisms	NA	PASS	NA	PASS
SSM-2	Appropriate integrity protection for secure storage mechanisms	NA	-	NA	NA
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	NA	PASS	NA	PASS
SCM-1	Applicability of secure communication mechanisms	PASS	PASS	PASS	PASS
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	PASS	-	PASS	PASS
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	PASS	-	PASS	PASS
SCM-4	Appropriate replay protection for secure communication mechanisms	PASS	-	PASS	PASS
RLM-1	Applicability and appropriateness of resilience mechanisms	PASS	PASS	PASS	PASS
NMM-1	Applicability and appropriateness of network monitoring mechanisms	PASS	-	PASS	PASS

Provision ID	Provision Title	Conceptual Assessment	Completeness Assessment	Sufficiency Assessment	Overall Verdict
TCM-1	Applicability and appropriateness of traffic control mechanisms	PASS	-	PASS	PASS
CCK-1	Confidential cryptographic keys	PASS	PASS	PASS	PASS
CCK-2	CCK generation mechanisms	PASS	PASS	-	PASS
CCK-3	Preventing static default values for preinstalled CCKs	NA	PASS	NA	PASS
CRY-1	Best practice cryptography	PASS	PASS	PASS	PASS
EN 18031-1	**Overall Verdict**				**PASS**

Equipment Under Test

The equipment under test is as described below.

ID	Description	Make (Model)	Serial
TRA-067527-S1	Merlin Router	Merlin-4609-F2G-T4-S2-DI6-DO2-LV-QFZ	00E0C819AA24
TRA-067527-S7	Merlin Router	Merlin-4609-F2G-T4-S2-DI6-DO2-LV-QFZ	00E0C819AA0E
Notes			
No notes.			

Support Equipment

The following support equipment was provided by the client for use during the assessment.

ID	Description
TRA-067527-S2	Power supply
TRA-067527-S3	Kettle Lead
TRA-067527-S4	Antenna
TRA-067527-S5	Antenna
TRA-067527-S6	Ethernet Cable
TRA-067527-S13	SFP Connector
Notes	
No notes.	

Laboratory Equipment

The laboratory used the following equipment during the assessment.

ID	Description
SMRT-CYB-001	Test Laptop
SMRT-CYB-005	RF Chamber
SMRT-CYB-006	Test SIM Card
SMRT-CYB-015	RJ 45 to 8 pin adapter
SMRT-CYB-016	Serial to 9 pin adapter
SMRT-CYB-017	Serial to 9 pin adapter
Keysight	Fuzzing tools
Notes	
No notes.	

Record of Revision

The following revisions of this report have been created. Draft versions are not listed.

Revision	Details	Date
A	First issue.	10th December 2025

END of Test Report. The following pages contain appendices only.

Appendix A – Test Case Remarks

This appendix details the Testing Laboratory's remarks against each provision of the standard. This appendix need not be included in any reproduction of this report.

Provision ID	**Provision Title**	**Verdict**
GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	**PASS**
Conceptual Assessment See Appendix B, GEC-1 for Decision Trees		PASS
Functional Completeness Assessment There were no unreported vulnerabilities found		PASS
Functional Sufficiency Assessment All vulnerabilities found have been fixed in the version of the OpenSSL (1.1.1m) used in the DUT or not applicable to the device		PASS
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
GEC-2	Limit exposure of services via related network interfaces	**PASS**
Conceptual Assessment See Appendix B, GEC-2 for Decision Trees		PASS
Functional Completeness Assessment		PASS
Cellular	Cellular interface is available in the default state and is necessary for the basic functionality of the DUT	
Ethernet	Ethernet functionality is available in the default state and is necessary for the basic functionality of the DUT	
Web UI	Web UI is available in the default state and is necessary for the basic functionality of the DUT	
CLI (SSH)	CLI (SSH) is available in the default state and is necessary for the basic functionality of the DUT	
VPN	VPN is encouraged to be used and therefore should be available in the default state	
SFP	SFP functionality is available in the default state and is necessary for the basic functionality of the DUT	
There is no evidence of any undocumented network interfaces or exposed services		
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
GEC-3	Configuration of optional services and the related exposed network interfaces	**PASS**
Conceptual Assessment See Appendix B, GEC-3 for Decision Trees		PASS
Functional Completeness Assessment All optional services are described and listed in: https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv And attached documents . There is no evidence of any undocumented optional services		PASS
Functional Sufficiency Assessment All optional interfaces were confirmed to be configurable via the Web UI or CLI (SSH)		PASS
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	**PASS**
Conceptual Assessment See Appendix B, GEC-4 for Decision Trees		PASS
Functional Completeness Assessment		PASS
Cellular	Cellular interface is available in the default state and is necessary for the basic functionality of the DUT	
Ethernet	Ethernet functionality is available in the default state and is necessary for the basic functionality of the DUT	
Web UI	Web UI is available in the default state and is necessary for the basic functionality of the DUT	
CLI (SSH)	CLI (SSH) is available in the default state and is necessary for the basic functionality of the DUT	
VPN	VPN is encouraged to be used and therefore should be available in the default state	
SFP	SFP functionality is available in the default state and is necessary for the basic functionality of the DUT	
All interfaces listed in: https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv		
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
GEC-5	No unnecessary external interfaces	**PASS**
Conceptual Assessment See Appendix B, GEC-5 for Decision Trees		PASS
Functional Completeness Assessment The DUT had the following external interfaces: Serial, USB-C, Ethernet, GPIO and SFP All interfaces are documented in the technical notes found at https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv There are no external interfaces on the device which are not listed.		PASS
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
GEC-6	Input validation	**PASS**
Conceptual Assessment See Appendix B, GEC-6 for Decision Trees		PASS
Functional Completeness Assessment The following interfaces were declared to be able to receive input: Serial, USB-C, Ethernet, Cellular, SFP, GPIO, Web UI, CLI (SSH) There was no evidence of any input mechanism not documented		PASS
Functional Sufficiency Assessment		PASS
Serial	Serial AT Command service set up – malformed / bad commands were rejected and had no impact on the device functionality	
USB-C	Incorrect commands sent via Docklight confirmed to be rejected by the DUT	
Ethernet	Keysight fuzzing equipment confirmed input validation over Ethernet	
Cellular	Confirmed by using the Firewall to do IP filtering to validate the input over the cellular interface. The Security Hardening document provided to all clients shows how to set up firewall and recommends best practices to secure the device over the Cellular network	
SFP	Keysight fuzzing equipment confirmed input validation over SFP	
GPIO	Has no affect on network / security assets – used for sensing capabilities	
Web UI	Incorrect / invalid commands are rejected by the DUT - e.g pop up saying invalid entry	
CLI (SSH)	Incorrect commands are rejected by the DUT	
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
ACM-1	Applicability of access control mechanisms	**PASS**
Conceptual Assessment See Appendix B, ACM-1 for Decision Trees		PASS
Functional Completeness Assessment The following were declared to be all network and security assets accessible by entities: Passwords, Certificates, TPM content, Configuration Data, Ethernet (x4), Cellular, SFP(2x), Web Interface, CLI (SSH) There was no evidence of any network and security assets accessible by entities that were not documented		PASS
Functional Sufficiency Assessment The Ethernet and SFP (2x) are protected by the target operational environment and all other network or security were confirmed to be protected by username/password access control in addition to the inherent increased security from the target operational environment		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
ACM-2	Appropriate access control mechanisms	**PASS**
Conceptual Assessment The following were declared as the access control mechanisms used by the device: Authentication via WebUI, Authentication via SSH		PASS
Functional Sufficiency Assessment Both authentication mechanisms were found to be implemented on the device		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
AUM-1-1	Applicability of authentication mechanisms (network interface)	**PASS**
Conceptual Assessment See Appendix B, AUM-1-1 for Decision Trees		NA
Functional Completeness Assessment There is no evidence of any access control mechanism required by ACM-1 not documented		PASS
Functional Sufficiency Assessment No remarks.		NA
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
AUM-1-2	Applicability of authentication mechanisms (user interface)	**PASS**
Conceptual Assessment See Appendix B, AUM-1-2 for Decision Trees		PASS
Functional Completeness Assessment The following were the User interfaces declared: WebUI, CLI (SSH) There was no evidence of any user interface not documented		PASS
Functional Sufficiency Assessment Both the WebUI and CLI (SSH) user interfaces were confirmed to be implemented as documented		PASS
Other Remarks No remarks.		

Provision ID AUM-2	**Provision Title** Appropriate authentication mechanisms	**Verdict PASS**
Conceptual Assessment See Appendix B, AUM-2 for Decision Trees		PASS
Functional Sufficiency Assessment Both the WebUI and CLI (SSH) user interfaces were confirmed to be implementing 1-factor authentication as documented		PASS
Other Remarks No remarks.		

Provision ID AUM-3	**Provision Title** Authenticator validation	**Verdict PASS**
Conceptual Assessment See Appendix B, AUM-3 for Decision Trees		PASS
Functional Sufficiency Assessment Both the WebUI and CLI (SSH) user interfaces were confirmed to reject incorrect passwords, passwords of different authenticators as well as parts of the correct password		PASS
Other Remarks No remarks.		

Provision ID AUM-4	**Provision Title** Changing authenticators	**Verdict PASS**
Conceptual Assessment See Appendix B, AUM-4 for Decision Trees		PASS
Functional Sufficiency Assessment A change of authenticator as was confirmed to be possible via the WebUI and CLI (SSH)		PASS
Other Remarks No remarks.		

Provision ID AUM-5-1	**Provision Title** Password strength (factory default passwords)	**Verdict PASS**
Conceptual Assessment See Appendix B, AUM-5-1 for Decision Trees		PASS
Functional Sufficiency Assessment The forced change of password on first login was confirmed on both the WebUI and CLI (SSH)		PASS
Other Remarks No remarks.		

Provision ID AUM-5-2	**Provision Title** Password strength (non-factory default passwords)	**Verdict NA**
Conceptual Assessment See Appendix B, AUM-5-2 for Decision Trees		NA
Functional Sufficiency Assessment No remarks.		NA
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
AUM-6	Brute force protection	**PASS**
Conceptual Assessment See Appendix B, AUM-6 for Decision Trees		PASS
Functional Sufficiency Assessment Firewall was confirmed to be configurable for Time Delay/IP Restrictions/number of allowed attempts, these are documented in their security hardening document for recommended configuration. Each method was validated and confirmed to provide brute force protection		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
SUM-1	Applicability of update mechanisms	**PASS**
Conceptual Assessment See Appendix B, SUM-1 for Decision Trees		PASS
Functional Sufficiency Assessment The following software/firmware were confirmed to be updateable via the described mechanisms: Main Image, Cellular FW, Secondary Bootloader Note the secondary bootloader would require the device to be sent back to the factory to update		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
SUM-2	Secure updates	**PASS**
Conceptual Assessment See Appendix B, SUM-2 for Decision Trees		PASS
Functional Sufficiency Assessment All update mechanisms were confirmed to reject bad/malformed images		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
SUM-3	Automated updates	**PASS**
Conceptual Assessment See Appendix B, SUM-3 for Decision Trees		PASS
Functional Sufficiency Assessment No remarks.		NA
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
SSM-1	Applicability of secure storage mechanisms	**PASS**
Conceptual Assessment See Appendix B, SSM-1 for Decision Trees		NA
Functional Completeness Assessment There is no evidence of any persistently stored network / security assets which are not listed or documented		PASS
Functional Sufficiency Assessment No remarks.		NA
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
SSM-2	Appropriate integrity protection for secure storage mechanisms	**NA**
Conceptual Assessment See Appendix B, SSM-2 for Decision Trees		NA
Functional Sufficiency Assessment No remarks.		NA
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	**PASS**
Conceptual Assessment See Appendix B, SSM-3 for Decision Trees		NA
Functional Completeness Assessment A review of the software block diagram and additional documentation showed no evidence that there are any persistently stored security parameters or network function configurations that are not documented		PASS
Functional Sufficiency Assessment No remarks.		NA
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
SCM-1	Applicability of secure communication mechanisms	**PASS**
Conceptual Assessment See Appendix B, SCM-1 for Decision Trees		PASS
Functional Completeness Assessment There is no evidence of any security or network assets communicated over any interface that is not documented		PASS
Functional Sufficiency Assessment		PASS
Cellular Ethernet SFP CLI (SSH) WebUI	IPSec controlled through the UI and is confirmed enabled through this Confirmed to be using TLSv1.3 using Wireshark IPSec controlled through the UI and is confirmed enabled through this Confirmed to be using SSHv2 using Wireshark Confirmed to be using TLS1.3	
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	**PASS**
Conceptual Assessment See Appendix B, SCM-2 for Decision Trees		PASS
Functional Sufficiency Assessment		PASS
VPN (IPSEC) Cellular	A correctly configured IPsec (ESP) tunnel using IKEv2 and modern cryptography, as per the security hardening document provided fully satisfies SCM-2 for integrity and authenticity protection	
VPN (IPSEC) Ethernet	IPsec - IKEv2 was used and data fuzzing was completed using Keysight Fuzzing equipment ensuring incorrect commands/packets were rejected by the DUT	
VPN (IPSEC) SFP	IPsec - IKEv2 was used and data fuzzing was completed using Keysight Fuzzing equipment ensuring incorrect commands/packets were rejected by the DUT	
SSH CLI (SSH)	SSHv2 is used by the device and incorrect commands confirmed to be rejected by the DUT	
TLS WebUI	TLS 1.3 with AES-GCM was used during testing with incorrect commands confirmed to be rejected by the DUT	
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	**PASS**
Conceptual Assessment See Appendix B, SCM-3 for Decision Trees		PASS
Functional Sufficiency Assessment		PASS
VPN (IPSec)	IPsec ESP encryption with modern ciphers as per the security hardening document provided satisfies SCM-3 for confidentiality protection	
SSH	All SSH sessions negotiate symmetric encryption, with modern ciphers as per the security hardening document provided satisfies SCM-3	
TLS	TLS 1.2 (with AEAD ciphers) and TLS 1.3 provide encryption of all application data after handshake with modern ciphers (tested with AES-GCM) as per the security hardening document provided satisfies SCM-3	
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
SCM-4	Appropriate replay protection for secure communication mechanisms	**PASS**
Conceptual Assessment See Appendix B, SCM-4 for Decision Trees		PASS
Functional Sufficiency Assessment		PASS
VPN (IPSEC) Cellular	IPSec with VPN inherently has replay protection and is shown to be enabled	
VPN (IPSEC) Ethernet	IPSec with VPN inherently has replay protection and is shown to be enabled	
VPN (IPSEC) SFP	IPSec with VPN inherently has replay protection and is shown to be enabled	
SSH CLI (SSH)	Inherent Replay protection as per the guidance for this provision 6.5.4.3	
TLS WebUI	Inherent Replay protection as per the guidance for this provision 6.5.4.3	
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
RLM-1	Applicability and appropriateness of resilience mechanisms	**PASS**
Conceptual Assessment See Appendix B, RLM-1 for Decision Trees		PASS
Functional Completeness Assessment There is no evidence of any resilience mechanism present that has not been documented		PASS
Functional Sufficiency Assessment The DUT firewall was confirmed to be present on the device and confirmed to be configurable as per the security hardening documentation		PASS
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
NMM-1	Applicability and appropriateness of network monitoring mechanisms	**PASS**
Conceptual Assessment See Appendix B, NMM-1 for Decision Trees		PASS
Functional Sufficiency Assessment The applicant demonstrated the network monitoring mechanism present on the device and it was as described		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
TCM-1	Applicability and appropriateness of traffic control mechanisms	**PASS**
Conceptual Assessment See Appendix B, TCM-4 for Decision Trees		PASS
Functional Sufficiency Assessment The firewall was observed to be monitoring traffic and dropping packets that do not meet requirements		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
CCK-1	Confidential cryptographic keys	**PASS**
Conceptual Assessment See Appendix B, CCK -1 for Decision Trees		PASS
Functional Completeness Assessment It was declared that the DUT has the following CCKs: TLS/IPSec/SSH session keys There was no evidence of any CCKs present on the device that was not documented		PASS
Functional Sufficiency Assessment The DUT was confirmed to use Diffie-Hellman Key exchange with minimum key length as described		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
CCK-2	CCK generation mechanisms	**PASS**
Conceptual Assessment See Appendix B, CCK -2 for Decision Trees		PASS
Conceptual Completeness Assessment It was declared that the DUT had the following key generation mechanisms TLS/IPsec/SSH Key generation mechanisms There is no evidence of any key generation mechanisms that are not listed		PASS
Other Remarks No remarks.		

Provision ID	Provision Title	Verdict
CCK-3	Preventing static default values for preinstalled CCKs	**PASS**
Conceptual Assessment See Appendix B, CCK -3 for Decision Trees		NA
Functional Completeness Assessment No evidence of any undocumented Preinstalled CCKs		PASS
Functional Sufficiency Assessment No remarks.		NA
Other Remarks No remarks.		

Provision ID	**Provision Title**	**Verdict**
CRY-1	Best practice cryptography	**PASS**
Conceptual Assessment See Appendix B, CRY -1 for Decision Trees		PASS
Functional Completeness Assessment The DUT is designed to use a wide range of cryptographies, too many to list, as such it was agreed for the applicant to list only the most popular as a representation of the DUT's capabilities		PASS
Functional Sufficiency Assessment The was confirmed to use/have the capability to use the following cryptographic algorithms: AES_CBC[aes] 256bit, 3DES_CBC[des] 156bit, TLS, SSH - aes256-ctr, SSH - aes128-ctr, SHA-2, SHA-3, as well as sha256,rsa2048 to sign OTA upgrade images		PASS
Other Remarks No remarks.		

Appendix B – Decision Tree Paths, Justifications, and Remarks

This appendix includes a replication of the assessments against each decision tree in each provision of the standard. This appendix need not be included in any reproduction of this report.

GEC-1 Up-to-date software and hardware with no publicly known exploitable vulnerabilities

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2016-1245		Vulnerability affect BGPD, used for very specific scenarios.		
Does the vulnerability affect security assets or network assets?	NO	Vulnerability does not directly affect security or network asset. Security nor network assets are not transported or accessed via BGPD. Vulnerbility is not listed as exploitable, EPS 1.19 % https://euvd.enisa.europa.eu/vulnerability/CVE-2016-1245	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2024-27913		Vulnerability affect FRR, used for very specific scenarios.		
Does the vulnerability affect security assets or network assets?	NO	Vulnerability does not directly affect security or network asset. Security nor network assets are not transported or accessed via FRR. Vulnerbility is not listed as exploitable, EPS 0.08 % https://euvd.enisa.europa.eu/vulnerability/CVE-2024-27913	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2022-1292		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 67.68 % https://euvd.enisa.europa.eu/vulnerability/CVE-2022-1292	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2022-2097		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 0.75 % https://euvd.enisa.europa.eu/vulnerability/CVE-2022-2097	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2022-4304		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 0.23 % https://euvd.enisa.europa.eu/vulnerability/CVE-2022-4304	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2022-4450		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 0.13 % https://euvd.enisa.europa.eu/vulnerability/CVE-2022-4450	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2023-0215		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 0.35 % https://euvd.enisa.europa.eu/vulnerability/CVE-2023-0215	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2023-0286		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 0.23 % https://euvd.enisa.europa.eu/vulnerability/CVE-2023-0286	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2023-0464		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 90.14% https://euvd.enisa.europa.eu/vulnerability/CVE-2023-0464	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2023-0465		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 0.42% https://euvd.enisa.europa.eu/vulnerability/CVE-2023-0465	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2023-0466		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 0.67% https://euvd.enisa.europa.eu/vulnerability/CVE-2023-0466	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2023-2650		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	openssl vulnerabilities are affecting current version of openssl, do not directly affect security or network asset. Vulnerbility is not listed as exploitable, EPS 91.97% https://euvd.enisa.europa.eu/vulnerability/CVE-2023-2650	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2023-3817		Vulnerability affects current version of openssl		
Does the vulnerability affect security assets or network assets?	NO	OpenSSL vulnerabilities are affecting current version of OpenSSL, do not directly affect security or network asset. Vulnerability is not listed as exploitable, EPS 0.27% https://euvd.enisa.europa.eu/vulnerability/CVE-2023-3817	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> CPU		Sierra Wireless - WP7607G Cat4 module https://www.tme.eu/Document/a35cc5e6bd3082e5324b80717b67cb50/SierraWireless_AirPrime.pdf		
Does the software and/or hardware contain publicly known vulnerabilities?	NO	https://euvd.enisa.europa.eu/search	Accept	
PASS			Accept	

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Trusted Platform Module		Infineon - TPM 2.0 SLB-9670 https://www.infineon.com/cms/en/product/security-smart-card-solutions/optiga-embedded-security-solutions/optiga-tpm/slb-9670vq2.0/		
Does the software and/or hardware contain publicly known vulnerabilities?	NO	https://euvd.enisa.europa.eu/search	Accept	
PASS			Accept	

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> RF		Sierra Wireless - WP7607G Cat4 module (RF is combined with CPU) https://www.tme.eu/Document/a35cc5e6bd3082e5324b80717b67cb50/SierraWireless_AirPrime.pdf		
Does the software and/or hardware contain publicly known vulnerabilities?	NO	https://euvd.enisa.europa.eu/search	Accept	
PASS			Accept	

Detail	Answer	Justification / Comment	Decision	Feedback

For each software and hardware:				
> Main Image				
Does the software and/or hardware contain publicly known vulnerabilities?	YES	-	Accept	
For each hardware's and/or software's publicly known exploitable vulnerability:				
> CVE-2022-0788		Vulnerability affects current version of OpenSSL		
Does the vulnerability affect security assets or network assets?	NO	OpenSSL vulnerabilities are affecting current version of OpenSSL, do not directly affect security or network asset. Vulnerability is not listed as exploitable, EPS 7.07% https://euvd.enisa.europa.eu/vulnerability/CVE-2022-0778	Accept	
NA				

GEC-2 Limit exposure of services via related network interfaces

Detail	Answer	Justification / Comment	Decision	Feedback
For each network interface and exposed service (via network interfaces):				
> Cellular				
Is the network interface or service available in the factory default state?	YES	Enabled for intended use	Accept	
Does the network interface or service affect security assets or network assets?	YES	Affects multiple assets	Accept	
Is the network interface or service necessary for equipment setup or for the basic operation?	YES	Part of intended use - needs to be enabled and communicate assets by design	Accept	Intended Functionality
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> Ethernet (x4)				
Is the network interface or service available in the factory default state?	YES	Enabled for intended use	Accept	
Does the network interface or service affect security assets or network assets?	YES	Affects multiple assets	Accept	
Is the network interface or service necessary for equipment setup or for the basic operation?	YES	Part of intended use - needs to be enabled and communicate assets by design	Accept	Intended Functionality
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> Web interface				
Is the network interface or service available in the factory default state?	YES	Enabled for intended use	Accept	
Does the network interface or service affect security assets or network assets?	YES	Affects multiple assets	Accept	
Is the network interface or service necessary for equipment setup or for the basic operation?	YES	Part of intended use - needs to be enabled and communicate assets by design	Accept	Intended Functionality
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> CLI (SSH)				
Is the network interface or service available in the factory default state?	YES	Enabled for intended use - Device Configuration	Accept	
Does the network interface or service affect security assets or network assets?	YES	Affects multiple assets	Accept	
Is the network interface or service necessary for equipment setup or for the basic operation?	YES	Part of intended use - needs to be enabled and communicate assets by design	Accept	Intended Functionality
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> VPN		VPN typically is not exposed, it works in client mode.		
Is the network interface or service available in the factory default state?	YES	Available in most configurations of the device	Accept	
Does the network interface or service affect security assets or network assets?	YES	Affects multiple assets	Accept	
Is the network interface or service necessary for equipment setup or for the basic operation?	YES	Part of intended use - needs to be enabled and communicate assets by design	Accept	Intended Functionality
PASS			Accept	

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> SFP(2x)				
Is the network interface or service available in the factory default state?	YES	Enabled for intended use - Device Configuration	Accept	
Does the network interface or service affect security assets or network assets?	YES	Affects multiple assets	Accept	
Is the network interface or service necessary for equipment setup or for the basic operation?	YES	Part of intended use - needs to be enabled and communicate assets by design	Accept	Intended Functionality
PASS				

GEC-3 Configuration of optional services and the related exposed network interfaces

Detail	Answer	Justification / Comment	Decision	Feedback

For each optional network interface and exposed optional service (via network interfaces) that is part of the factory default state:				
> Cellular				
Are security assets or network assets affected by the network interface or service?	YES	Affects multiple assets	Accept	
Is an option provided for an authorized user to enable and disable the network interface or service?	YES	Can be disabled by user configuration	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each optional network interface and exposed optional service (via network interfaces) that is part of the factory default state:				
> Ethernet (x4)				
Are security assets or network assets affected by the network interface or service?	YES	Affects multiple assets	Accept	
Is an option provided for an authorized user to enable and disable the network interface or service?	YES	Can be disabled by user configuration	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each optional network interface and exposed optional service (via network interfaces) that is part of the factory default state:				
> Web interface				
Are security assets or network assets affected by the network interface or service?	YES	Affects multiple assets	Accept	
Is an option provided for an authorized user to enable and disable the network interface or service?	YES	Can be disabled by user configuration	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each optional network interface and exposed optional service (via network interfaces) that is part of the factory default state:				
> VPN				
Are security assets or network assets affected by the network interface or service?	YES	Affects multiple assets	Accept	
Is an option provided for an authorized user to enable and disable the network interface or service?	YES	Can be disabled by user configuration	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each optional network interface and exposed optional service (via network interfaces) that is part of the factory default state:				
> Serial(2x)				
Are security assets or network assets affected by the network interface or service?	YES	Affects multiple assets	Accept	
Is an option provided for an authorized user to enable and disable the network interface or service?	YES	Can be disabled by user configuration	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each optional network interface and exposed optional service (via network interfaces) that is part of the factory default state:				
> SFP(2x)				
Are security assets or network assets affected by the network interface or service?	YES	Affects multiple assets	Accept	
Is an option provided for an authorized user to enable and disable the network interface or service?	YES	Can be disabled by user configuration	Accept	
PASS				

GEC-4 Documentation of exposed network interfaces and exposed services via network interfaces

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> Cellular				
Is the network interface or service delivered as part of the factory default state?	YES	Necessary for intended use	Accept	
Is the exposed network interface or exposed service described in the user documentation?	YES	Documented https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv	Accept	Documented as such
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> Ethernet (x4)				
Is the network interface or service delivered as part of the factory default state?	YES	Necessary for intended use	Accept	
Is the exposed network interface or exposed service described in the user documentation?	YES	Documented https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv	Accept	Documented as such
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> Web interface				
Is the network interface or service delivered as part of the factory default state?	YES	Necessary for intended use	Accept	
Is the exposed network interface or exposed service described in the user documentation?	YES	Documented https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv	Accept	westermo_ds_merlin-4600_0307_en_revg.pdf
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> CLI (SSH)				
Is the network interface or service delivered as part of the factory default state?	YES	Necessary for intended use	Accept	
Is the exposed network interface or exposed service described in the user documentation?	YES	Documented https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv	Accept	westermo_ds_merlin-4600_0307_en_revg.pdf
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> VPN				
Is the network interface or service delivered as part of the factory default state?	YES	Necessary for intended use	Accept	
Is the exposed network interface or exposed service described in the user documentation?	YES	Documented https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv	Accept	westermo_ds_merlin-4600_0307_en_revg.pdf
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface and exposed service (via network interfaces):				
> SFP(2x)				
Is the network interface or service delivered as part of the factory default state?	YES	Necessary for intended use	Accept	
Is the exposed network interface or exposed service described in the user documentation?	YES	Documented https://www.westermo.com/support/product-support/merlin-4609-f2g-t4-s2-di6-do2-lv	Accept	Documented as such
PASS				

GEC-5 No unnecessary external interfaces

Detail	Answer	Justification / Comment	Decision	Feedback

For each physical external interface:				
> Serial (x2)				
Is the physical external interface necessary for the intended functionality?	YES	Primary Functionality	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback
For each physical external interface:				
> USB-C (RS232)				
Is the physical external interface necessary for the intended functionality?	YES	Primary Functionality	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each physical external interface:				
> Ethernet (x4)				
Is the physical external interface necessary for the intended functionality?	YES	Primary Functionality	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback
For each physical external interface:				
> GPIO				
Is the physical external interface necessary for the intended functionality?	YES	Primary Functionality	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each physical external interface:				
> SFP(2x)				
Is the physical external interface necessary for the intended functionality?	YES	Primary Functionality	Accept	
PASS				

GEC-6 Input validation

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> Serial (x2)				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Data				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	Checksum validation	Accept	Appropriate Validation
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> USB-C (RS232)				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Data				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	RS232 Serial communication - Checksum Validation	Accept	Appropriate Validation
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> Ethernet (x4)				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Data				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	Checksum Validation	Accept	Appropriate Validation
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> Cellular				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Data				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	Checksum Validation	Accept	Appropriate Validation
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> SFP(2x)				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Data				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	Checksum Validation	Accept	Appropriate Validation
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> GPIO (6xIN + 2xOUT)				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Signal				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	No input that affects any assets	Accept	Accepted
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> Web Interface				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Data				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	Protected via HTTPs (TLS)	Accept	The justification is not correct but accepted as semantic input only allows a predefined list of values to be entered into the configuration inputs
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each external interface:				
> CLI (SSH)				
Is the interface capable of receiving input?	YES	-	Accept	
For each means of receiving input:				
> Data				
Is input validation functionality used for input that has potential impact on security assets and/or network assets?	YES	Protecrted via SSH.	Accept	The justification is not correct but accepted as semantic input only allows a predefined list of values to be entered into each menu
PASS				

ACM-1 Applicability of access control mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> Passwords				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	NO	-	Accept	
Do legal implications not allow access control mechanisms?	NO	No Legal Implecations	Accept	
Are there access control mechanisms that manage entities' access to the security assets and network assets?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operating environment will inherently increase device security.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> Certificates				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	NO	-	Accept	
Do legal implications not allow access control mechanisms?	NO	No Legal Implecations	Accept	
Are there access control mechanisms that manage entities' access to the security assets and network assets?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operating environment will inherently increase device security.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> TPM content				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	NO	-	Accept	
Do legal implications not allow access control mechanisms?	NO	No Legal Implecations	Accept	
Are there access control mechanisms that manage entities' access to the security assets and network assets?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operating environment will inherently increase device security.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> Configuration Data				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	NO	-	Accept	
Do legal implications not allow access control mechanisms?	NO	No Legal Implecations	Accept	
Are there access control mechanisms that manage entities' access to the security assets and network assets?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operating environment will inherently increase device security.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> Ethernet (x4)				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operational environment will inherently increase device security.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> Cellular				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	NO	-	Accept	
Do legal implications not allow access control mechanisms?	NO	No Legal Implecations	Accept	
Are there access control mechanisms that manage entities' access to the security assets and network assets?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operating environment will inherently increase device security.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> SFP(2x)				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operational environment will inherently increase device security.	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> Web Interface				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	NO	-	Accept	
Do legal implications not allow access control mechanisms?	NO	No Legal Implecations	Accept	
Are there access control mechanisms that manage entities' access to the security assets and network assets?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operating environment will inherently increase device security.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each security asset and network asset that is accessible by entities:				
> CLI (SSH)				
Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Not intended functionality	Accept	
Do the physical or logical measures in the targeted operational environment limit the accessibility to authorized entities?	NO	-	Accept	
Do legal implications not allow access control mechanisms?	NO	No Legal Implecations	Accept	
Are there access control mechanisms that manage entities' access to the security assets and network assets?	YES	Each interface that provides access to the device requires authorization via embeded access control. A targeted operating environment will inherently increase device security.	Accept	
PASS				

ACM-2 Appropriate access control mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism that is required per ACM-1:				
> Authentication (WebUI)				
Do the access control mechanisms ensure that only authorized entities have access to the protected security asset or network asset?	YES	Yes, requires Username/Password	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism that is required per ACM-1:				
> Authentication (SSH)				
Do the access control mechanisms ensure that only authorized entities have access to the protected security asset or network asset?	YES	Yes, requires Username/Password	Accept	
PASS				

AUM-1-1 Applicability of authentication mechanisms (network interface)

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication				
For each network interface the access control mechanism manages access over:				
> USB-C (RS232)				
For each managed access to network asset or security asset via the network interface:				
> Passwords				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication(+SSH)				
For each network interface the access control mechanism manages access over:				
> Ethernet (x4)				
For each managed access to network asset or security asset via the network interface:				
> Passwords				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> SFP(2x)				
For each managed access to network asset or security asset via the network interface:				
> Passwords				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> Cellular				
For each managed access to network asset or security asset via the network interface:				
> Passwords				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication				
For each network interface the access control mechanism manages access over:				
> USB-C (RS232)				
For each managed access to network asset or security asset via the network interface:				
> Certificates				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> Ethernet (x4)				
For each managed access to network asset or security asset via the network interface:				
> Certificates				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> SFP(2x)				
For each managed access to network asset or security asset via the network interface:				
> Certificates				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> Cellular				
For each managed access to network asset or security asset via the network interface:				
> Certificates				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication				
For each network interface the access control mechanism manages access over:				
> USB-C (RS232)				
For each managed access to network asset or security asset via the network interface:				
> TPM content				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> Ethernet (x4)				
For each managed access to network asset or security asset via the network interface:				
> TPM content				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> SFP(2x)				
For each managed access to network asset or security asset via the network interface:				
> TPM content				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a network interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each network interface the access control mechanism manages access over:				
> Cellular				
For each managed access to network asset or security asset via the network interface:				
> TPM content				
Is the managed access for network functions or network functions configuration and is the absence of authentication required for the equipment's functionality?	NO	Not intended Functionality	Accept	
Is the managed access performed over networks where access is limited to authorized entities?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

AUM-1-2 Applicability of authentication mechanisms (user interface)

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a user interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+TLS)				
For each user interface the access control mechanism manages access over:				
> Web interface				
For each managed access to network asset or security asset via the user interface:				
> Passwords				
Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entities claim?	NO	Isolated and secured networks are the intended operational environment.	Accept	

Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed to enable the equipment's intended equipment functionality?	NO	Not inteded functionality	Accept	
Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed because legal implications do not allow for authentication mechanisms?	NO	No Legal Implecations	Accept	
Does the managed access use authentication mechanisms?	YES	Web UI Username and Password	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a user interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+TLS)				
For each user interface the access control mechanism manages access over:				
> Web interface				
For each managed access to network asset or security asset via the user interface:				
> Certificates				
Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entities claim?	NO	Isolated and secured networks are the intended operational environment.	Accept	

Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed to enable the equipment's intended equipment functionality?	NO	Not inteded functionality	Accept	
Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed because legal implications do not allow for authentication mechanisms?	NO	No Legal Implecations	Accept	
Does the managed access use authentication mechanisms?	YES	Web UI Username and Password	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a user interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+TLS)				
For each user interface the access control mechanism manages access over:				
> Web interface				
For each managed access to network asset or security asset via the user interface:				
> TPM content				
Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entities claim?	NO	Isolated and secured networks are the intended operational environment.	Accept	

Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed to enable the equipment's intended equipment functionality?	NO	Not inteded functionality	Accept	
Is the managed access only for reading of network functions or network functions configuration where access without authentication is needed because legal implications do not allow for authentication mechanisms?	NO	No Legal Implecations	Accept	
Does the managed access use authentication mechanisms?	YES	Web UI Username and Password	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a user interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each user interface the access control mechanism manages access over:				
> CLI				
For each managed access to network asset or security asset via the user interface:				
> Passwords				
Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entities claim?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a user interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each user interface the access control mechanism manages access over:				
> CLI				
For each managed access to network asset or security asset via the user interface:				
> Certificates				
Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entities claim?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each access control mechanism required per ACM-1 that manages entities' access via a user interface and allows to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions:				
> Authentication (+SSH)				
For each user interface the access control mechanism manages access over:				
> CLI				
For each managed access to network asset or security asset via the user interface:				
> TPM content				
Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entities claim?	YES	Isolated and secured networks are the intended operational environment.	Accept	

NA

AUM-2 Appropriate authentication mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback
For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (WebUI)				
Does the authentication mechanism examine evidence from at least one element of the categories knowledge, possession, and inherence (one factor authentication)?	YES	via local password	Accept	

PASS

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (SSH)				
Does the authentication mechanism examine evidence from at least one element of the categories knowledge, possession, and inherence (one factor authentication)?	YES	via local password	Accept	
PASS				

AUM-3 Authenticator validation

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (WebUI)		3.4 authenticator something known or possessed, and controlled by an entity that is used for authentication		
Does the authentication mechanism validate all relevant properties considering the available information about the authenticator in the operational environments of use?	YES	authenticator	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (SSH)		3.4 authenticator something known or possessed, and controlled by an entity that is used for authentication		
Does the authentication mechanism validate all relevant properties considering the available information about the authenticator in the operational environments of use?	YES	authenticator	Accept	
PASS				

AUM-4 Changing authenticators

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (WebUI)		3.4 authenticator something known or possessed, and controlled by an entity that is used for authentication		
Does the change of the authenticator conflict security goals?	NO	-	Accept	
Does the authentication mechanism allow the change of the authenticator?	YES	Password change is allowed.	Accept	
PASS			Accept	

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (SSH)		3.4 authenticator something known or possessed, and controlled by an entity that is used for authentication		
Does the change of the authenticator conflict security goals?	NO	-	Accept	
Does the authentication mechanism allow the change of the authenticator?	YES	Password change is allowed.	Accept	
PASS			Accept	

AUM-5-1 Password strength (factory default passwords)

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2 that uses factory default passwords:				
> Authentication (WebUI)				
Is the password enforced to be changed by the user before or on first use?	YES	Enforced on first login	Accept	
Is the user allowed not to set and use any password?	NO	Minimum character length enforced	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2 that uses factory default passwords:				
> Authentication (SSH)				
Is the password enforced to be changed by the user before or on first use?	YES	Not Enforced	Accept	
Is the user allowed not to set and use any password?	NO	Minimum character length enforced	Accept	
PASS				

AUM-5-2 Password strength (non-factory default passwords)

AUM-6 Brute force protection

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (WebUI)				
Has the authentication mechanism the capability to be resilient against brute force attacks?	YES	Via build in mechnisms and external configurations such as firewall.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each authentication mechanism required per AUM-1-1 or AUM-1-2:				
> Authentication (SSH)				
Has the authentication mechanism the capability to be resilient against brute force attacks?	YES	Via build in mechnisms and external configurations such as firewall.	Accept	
PASS				

SUM-1 Applicability of update mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each part of the software, including firmware:				
> Main Image				
Does the part of the software affect security assets or network assets?	YES	Affects multiple assets	Accept	
Do functional safety implications prohibit updatability?	NO	-	Accept	
Is the software or firmware immutable?	NO	Not Immutable	Accept	
Do alternative measures exist that protect security assets and/or network assets during the entire lifecycle?	NO	Supplementary measures and services exist.	Accept	
Does the equipment provide at least one update mechanism for updating the part of the software?	YES	Via WebUI.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each part of the software, including firmware:				
> Primary Bootloader				
Does the part of the software affect security assets or network assets?	YES	Affects multiple assets	Accept	
Do functional safety implications prohibit updatability?	NO	-	Accept	
Is the software or firmware immutable?	YES	Immutable	Accept	

NA

Detail	Answer	Justification / Comment	Decision	Feedback

For each part of the software, including firmware:				
> Cellular FW				
Does the part of the software affect security assets or network assets?	YES	Affects multiple asssets	Accept	
Do functional safety implications prohibit updatability?	NO	-	Accept	
Is the software or firmware immutable?	NO	Not Immutable	Accept	
Do alternative measures exist that protect security assets and/or network assets during the entire lifecycle?	NO	-	Accept	
Does the equipment provide at least one update mechanism for updating the part of the software?	YES	FOTA.	Accept	Over the air updates
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each part of the software, including firmware:				
> Secondary Bootloader				
Does the part of the software affect security assets or network assets?	YES	Affects multiple assets	Accept	
Do functional safety implications prohibit updatability?	NO	-	Accept	
Is the software or firmware immutable?	NO	Not Immutable	Accept	
Do alternative measures exist that protect security assets and/or network assets during the entire lifecycle?	NO	-	Accept	
Does the equipment provide at least one update mechanism for updating the part of the software?	YES	Updates are available via Vendors Support Service.	Accept	
PASS				

SUM-2 Secure updates

Detail	Answer	Justification / Comment	Decision	Feedback

For each update mechanism for updating software that affects security or network assets (including firmware):				
> Main Image update mechanism				
Does the update mechanism ensure to only install software whose integrity and authenticity are valid at the time of installation?	YES	With an aid of digital signatures.	Accept	Appropriate Mechanism
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each update mechanism for updating software that affects security or network assets (including firmware):				
> Bootloader update mechanism				
Does the update mechanism ensure to only install software whose integrity and authenticity are valid at the time of installation?	YES	With an aid of OTP digital signatures.	Accept	Appropriate Mechanism
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each update mechanism for updating software that affects security or network assets (including firmware):				
> Cellular FW update				
Does the update mechanism ensure to only install software whose integrity and authenticity are valid at the time of installation?	YES	With an aid of digital signatures via FOTA.	Accept	Appropriate Mechanism
PASS				

SUM-3 Automated updates

Detail	Answer	Justification / Comment	Decision	Feedback

For each update mechanism required per SUM-1:				
> Main Image update mechanism				
Is the update mechanism capable of updating the software without human intervention at the equipment?	NO	Requires Human Intervention	Accept	
Is the update mechanism capable of updating the software via scheduling the installation of an update under human approval?	YES	Needs human interaction to schedule updates – Cannot be automated	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each update mechanism required per SUM-1:				
> Bootloader update mechanism				
Is the update mechanism capable of updating the software without human intervention at the equipment?	NO	Requires Human Intervention	Accept	
Is the update mechanism capable of updating the software via scheduling the installation of an update under human approval?	YES	Needs human interaction to schedule updates – Cannot be automated	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each update mechanism required per SUM-1:				
> Cellular FW update				
Is the update mechanism capable of updating the software without human intervention at the equipment?	NO	Requires Human Intervention	Accept	
Is the update mechanism capable of updating the software via scheduling the installation of an update under human approval?	YES	Needs human interaction to schedule updates – Cannot be automated	Accept	
PASS				

SSM-1 Applicability of secure storage mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each network asset and security asset persistently stored on the equipment:				
> Passwords				
For each persistent storage of the network asset or security asset on the equipment:				
> Flash				
Is the storage of the network asset or security asset protected by physical or logical measures in the equipment's target operational environment?	YES	Physical measures: The intended operational environment includes secure physical cabinet or enclosure. Logical measure: Access to device requires Authentication by Username/Password authentication.	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network asset and security asset persistently stored on the equipment:				
> Certificates				
For each persistent storage of the network asset or security asset on the equipment:				
> Flash				
Is the storage of the network asset or security asset protected by physical or logical measures in the equipment's target operational environment?	YES	Physical measures: The intended operational environment includes secure physical cabinet or enclosure. Logical measure: Access to device requires Authentication by Username/Password authentication.	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network asset and security asset persistently stored on the equipment:				
> TPM content				
For each persistent storage of the network asset or security asset on the equipment:				
> Flash				
Is the storage of the network asset or security asset protected by physical or logical measures in the equipment's target operational environment?	YES	Physical measures: The intended operational environment includes secure physical cabinet or enclosure. Logical measure: Access to device requires Authentication by Username/Password authentication.	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network asset and security asset persistently stored on the equipment:				
> Configuration Data				
For each persistent storage of the network asset or security asset on the equipment:				
> Flash				
Is the storage of the network asset or security asset protected by physical or logical measures in the equipment's target operational environment?	YES	Physical measures: The intended operational environment includes secure physical cabinet or enclosure. Logical measure: Access to device requires Authentication by Username/Password authentication.	Accept	
NA				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network asset and security asset persistently stored on the equipment:				
> Certificates				
For each persistent storage of the network asset or security asset on the equipment:				
> TPM content				
Is the storage of the network asset or security asset protected by physical or logical measures in the equipment's target operational environment?	YES	Physical measures: The intended operational environment includes secure physical cabinet or enclosure. Logical measure: Access to device requires Authentication by Username/Password authentication.	Accept	
NA				

SSM-2 Appropriate integrity protection for secure storage mechanisms

SSM-3 Appropriate confidentiality protection for secure storage mechanisms

SCM-1 Applicability of secure communication mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback
For each communication of network assets or security assets via network interface:				
> Cellular				
Is the secure communication of network assets or security assets ensured by a secure communication mechanism?	YES	Secure communication mechanism used: VPN (e.g. Ipsec) is an industry standard and recommended practice.	Accept	Appropriate SCM
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each communication of network assets or security assets via network interface:				
> Ethernet (x4)				
Is the secure communication of network assets or security assets ensured by a secure communication mechanism?	YES	Secure communication mechanism used: VPN (e.g. Ipsec) is an industry standard and recommended practice.	Accept	Appropriate SCM
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each communication of network assets or security assets via network interface:				
> SFP(2x)				
Is the secure communication of network assets or security assets ensured by a secure communication mechanism?	YES	Secure communication mechanism used: VPN (e.g. Ipsec) is an industry standard and recommended practice.	Accept	Appropriate SCM
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each communication of network assets or security assets via network interface:				
> CLI (SSH)				
Is the secure communication of network assets or security assets ensured by a secure communication mechanism?	YES	Secure communication mechanism used: SSH Protocol	Accept	Appropriate SCM
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each communication of network assets or security assets via network interface:				
> Web Interface				
Is the secure communication of network assets or security assets ensured by a secure communication mechanism?	YES	Secure communication mechanism used: HTTPs (TLS)	Accept	Appropriate SCM
PASS				

SCM-2 Appropriate integrity and authenticity protection for secure communication mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets:				
> Cellular				
Are best practices applied to protect the integrity and authenticity of the communicated asset?	YES	Integrity and authenticity of passwords is protected via VPN (Ipsec via IKEv2) protocol authentication mechanism.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets:				
> Ethernet (x4)				
Are best practices applied to protect the integrity and authenticity of the communicated asset?	YES	Integrity and authenticity of passwords is protected via VPN (Ipsec via IKEv2) protocol authentication mechanism.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets:				
> SFP(2x)				
Are best practices applied to protect the integrity and authenticity of the communicated asset?	YES	Integrity and authenticity of passwords is protected via VPN (Ipsec via IKEv2) protocol authentication mechanism.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> SSH				
For each communication of security assets or network assets:				
> CLI (SSH)				
Are best practices applied to protect the integrity and authenticity of the communicated asset?	YES	Integrity and authenticity of passwords is protected via SSH (SSH-2) protocol authentication mechanism.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> TLS				
For each communication of security assets or network assets:				
> Web Interface				
Are best practices applied to protect the integrity and authenticity of the communicated asset?	YES	Integrity and authenticity of passwords is protected via TLS (TLS 1.3) protocol authentication mechanism.	Accept	
PASS				

SCM-3 Appropriate confidentiality protection for secure communication mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets where confidentiality protection is needed:				
> VPN (Ipsec)				
Are best practices applied to protect the confidentiality of the communicated asset?	YES	VPN (Ipsec - IKEv2) follows best practices.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets where confidentiality protection is needed:				
> SSH				
Are best practices applied to protect the confidentiality of the communicated asset?	YES	SSH (SSH-2) follows best practices.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets where confidentiality protection is needed:				
> TLS				
Are best practices applied to protect the confidentiality of the communicated asset?	YES	TLS (TLS 1.3) follows best practices.	Accept	
PASS				

SCM-4 Appropriate replay protection for secure communication mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets:				
> Cellular				
Are best practices applied to protect the communicated asset against replay attacks?	YES	VPN (e.g. Ipsec) has a built-in replay protection.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets:				
> Ethernet (x4)				
Are best practices applied to protect the communicated asset against replay attacks?	YES	VPN (e.g. Ipsec) has a built-in replay protection.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> VPN (Ipsec)				
For each communication of security assets or network assets:				
> SFP(2x)				
Are best practices applied to protect the communicated asset against replay attacks?	YES	VPN (e.g. Ipsec) has a built-in replay protection.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> SSH				
For each communication of security assets or network assets:				
> CLI (SSH)				
Are best practices applied to protect the communicated asset against replay attacks?	YES	SSH has a built-in replay protection.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each secure communication mechanism that is required per SCM-1:				
> TLS				
For each communication of security assets or network assets:				
> Web Interface				
Are best practices applied to protect the communicated asset against replay attacks?	YES	TLS has a built-in replay protection.	Accept	
PASS				

RLM-1 Applicability and appropriateness of resilience mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface:				
> Cellular				
Does the equipment use resilience mechanisms to mitigate the effects of DoS attacks on the network interfaces and return to a defined state after the attack?	YES	Firewall - Rate Limiting filtering of devices Linux Kernal has built in mechanisms	Accept	Appropriate Resiliance Mechanism
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface:				
> Ethernet (x4)				
Does the equipment use resilience mechanisms to mitigate the effects of DoS attacks on the network interfaces and return to a defined state after the attack?	YES	Firewall - Rate Limiting filtering of devices Linux Kernal has built in mechanisms	Accept	Appropriate Resiliance Mechanism
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each network interface:				
> SFP(2x)				
Does the equipment use resilience mechanisms to mitigate the effects of DoS attacks on the network interfaces and return to a defined state after the attack?	NO	-	Accept	
Is the network interface intended to be used to communicate with other equipment in a local network only?	YES	Requires Physical access to the device	Accept	By its nature is only local
NA				

NMM-1 Applicability and appropriateness of network monitoring mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

> For the equipment:				
Is the equipment a network equipment?	YES	Network Equipment by design	Accept	
Does the network equipment provide a network monitoring mechanism to detect indicators of DoS attacks?	YES	Rate Limiting monitoring through the firewall system logging feature	Accept	Appropriate NMM
PASS				

TCM-1 Applicability and appropriateness of traffic control mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

> For the equipment:				
Is the equipment a network equipment?	YES	Network Equipment by design	Accept	
Does the network equipment provide a traffic control mechanism?	YES	Firewall provide capability to filter, control and monitor of all traffic.	Accept	Appropriate TCM
PASS				

CCK-1 Confidential cryptographic keys

Detail	Answer	Justification / Comment	Decision	Feedback

For each confidential cryptographic key (preinstalled or generated during usage):				
> Session keys		(All auto generated key, device has no preinstalled keys)		
Is the CCK solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Does the CCK support a minimumsecurity strength of 112 bits?	YES	CCK are autogenerated, based on user selected ciphers, recommendation is to use 256bit lengths + (To collect evidences for this requirement, the traces shall be coolected .e.g. tcpdump. The selected algorithms will be listed in msg exchanges)	Accept	
PASS			Accept	

CCK-2 CCK generation mechanisms

Detail	Answer	Justification / Comment	Decision	Feedback

For each CCK generation mechanism:				
> TLS key generation mechanism				
For each generated CCK:				
> Session keys				
Is the CCK solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Does the generation mechanism for the CCK adhere to best practice cryptography?	YES	Generation mechanism is based on the industry standard TLS library.	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each CCK generation mechanism:				
> IPSEC key generation mechanism				
For each generated CCK:				
> Session keys				
Is the CCK solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Does the generation mechanism for the CCK adhere to best practice cryptography?	YES	Generation mechanism is based on the industry standard Ipsec (IKEv2)	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each CCK generation mechanism:				
> SSH key generation mechanism				
For each generated CCK:				
> Session keys				
Is the CCK solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Does the generation mechanism for the CCK adhere to best practice cryptography?	YES	Generation mechanism is based on the industry standard SSH (SSH2)	Accept	
PASS				

CCK-3 Preventing static default values for preinstalled CCKs

CRY-1 Best practice cryptography

Detail	Answer	Justification / Comment	Decision	Feedback
For each cryptography used to protect security assets or network assets:				
> AES_CBC[aes] 128bit				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each cryptography used to protect security assets or network assets:				
> AES_CBC[aes] 256bit				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each cryptography used to protect security assets or network assets:				
> 3DES_CBC[des] 156bit				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each cryptography used to protect security assets or network assets:				
> TLS				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each cryptography used to protect security assets or network assets:				
> SSH - aes256-ctr				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each cryptography used to protect security assets or network assets:				
> SSH - aes128-ctr				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each cryptography used to protect security assets or network assets:				
> SHA-2				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				

Detail	Answer	Justification / Comment	Decision	Feedback

For each cryptography used to protect security assets or network assets:				
> SHA-3				
Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM?	NO	No Deviation	Accept	
Is the cryptography best practice concerning the protection of the security assets or network assets?	YES	OpenSSL is an industry standard, contains suite of ciphers and algorithms used for secure communications and CCK generation. As per https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf	Accept	
PASS				