

**Cyber Security Requirements**

1.IED Cyber Security capability compliance in the IEDs: following requirements shall be met by IED as per IEEE 1686:2013 clause 5.

Clause Number	Sub Category	Checklist
<b>5 IED Cybersecurity features</b>		
5.1	Electronic access control	Check the IED is protected by unique ID and Password Combination. Check it shall not be possible to gain access to the device without a proper ID/password combination that user has generated.
5.1.2	Password defeat mechanism	Check IED does not have undisclosed means whereby user-created ID/password can be defeated. Check Embedded master password technique is implemented? Check whether chip-embedded routines that automatically run in the event of hardware or software failure? Check Hardware bypass of passwords, such as jumpers and switch settings is implemented?
5.1.3	Number of Individual users	Minimum 04 users shall be supported by IED
5.1.4	Password Construction	Check password supported is At least 8 characters and is case-sensitive. When encoding is in plain text, it shall contain: -At least one uppercase and one lowercase - At least one number - One non-alpha numeric character (@,%,&,* ) Check the user is notified and prompted to choose another password that conforms if it violates.
<b>5.1.6 IED main security functions</b>		
5.1.6 b)	View configuration settings	Check IED's ability to view configuration settings such as scaling, communication addressing, programmable logic routines(through configuration software), and firmware version
5.1.6 d)	Configuration change	Check IED's ability to <b>extract &amp; upload configuration files from/to IED</b> to the unit and /or effect changes to the existing configuration
5.1.6 e)	Firmware change	Firmware change refers to the ability to load new firmware that does not require hardware change.
5.1.6 f)	ID/Password or RBAC management	ID/Password or RBAC management refers to the ability to load new id that does not require hardware management.
5.1.6 g)	Audit trail	Audit trail refers to the ability to view and download the audit trail.
5.1.7	Password Display	Check the vulnerability of password disclosure in local display panel, configuration software (local or remote; offline or online), web browser and terminal access
<b>5.2 Audit trail</b>		
<b>5.2.4 Audit trail event types</b>		
5.2.4 a)	Log In	Log In (locally or remotely) as a user to the device and check the event is created in audit log.
5.2.4 f)	Configuration change	Check new configuration file to the IED or new configuration parameters that causes a change in IED configuration is logged in Audit trail
5.2.4 h)	ID/password creation or modification	Check new ID/password creation/modification is logged in audit log
5.2.4 i)	ID/Password deletion	Check new ID/password deletion is logged in audit log
<b>5.3 Supervisory monitoring and control</b>		

5.3.1	Overview of supervisory monitoring and control	IED shall monitor security related activity and shall make the information available through a real time communication protocol for transmission to the supervisory system.
5.3.3 Alarms: Following shall cause unique alarm occurrence		
5.3.3 b)	Reboot	Rebooting or restarting of IED by means of removing power or through the use of a device resident rebooting mechanism such as reset button, power-up sequence, or access software failure.
5.3.4	Alarm point change detect	Check the momentary change of events and Alarms is detected as individual alarm and event.
5.4 IED Cyber Security features		
5.4.2 Specific Cryptographic features		
5.4.2 e)	Network time synchronization	NTP shall be NTP v3/4 or SNTP 3/4
5.5 IED configuration software		
5.5.4.2 change configuration data		
5.5.4.2. a)	Full access	In full access mode, all functions, including ID/password changes and user assignment can be made.
5.6	Communications port access	Check the communication is not possible in disabled communication port and all the unused UDP/TCP ports are disabled

2. Following Security features shall be available in each IED including PMU:

- DOS protection
- NTP/PTP synchronization
- Role Based Access Control compliance as per IEC 62351-8 as per the OEM compliance chart
- Emergency access to device if connection to RBAC Server is lost
- LDAP/AD/Radius support for Authentication and account management

3. Following Security features shall be available in Computers/ workstations/ servers/software for Substation Automation System:

- All applications(software)/ OS supplied shall be licensed to POWERGRID (if applicable) and any updates shall be supplied during the Warranty period.
- Computer names shall be as per the standard naming convention of POWERGRID.
- BIOS Password shall be set/enabled at system boot. Disk encryption policy shall be enabled on mobile devices(laptop/External HDD), if possible.
- Bluetooth and Wi-Fi driver shall be uninstalled. Corresponding hardware shall be disabled from OS or BIOS, if possible.
- Wake on LAN feature shall be disabled.
- System boot from USB or other means shall be disabled.
- Virtualization feature in CPU shall be disabled, wherever applicable.
- Standard user (non-administrator) accounts shall be enabled for regular work. Privileges and use of admin privilege shall only be required for specific tasks wherever applicable.
- Roles such as user, administrator, auditor shall be configured in IEDs and Associated applications.
- Only whitelisted software shall be installed on systems.
- Security features such as RBAC, password complexity, syslog, Radius/ AD authentication, enabling of certificates shall be ensured in all installed applications, wherever applicable.
- Only whitelisted services shall be running on systems.

## Annexure-S12 (Annexure-II-CyberSecurity\_Requirements\_R0)

- External USB storage devices (i.e., pen drive, memory cards, hard disk, mobile phone storage etc.) shall NOT be allowed, only authorized USB storage devices (approved by POWERGRID) shall be allowed on systems based on the roles & requirements of the user.
  - Endpoint protection (Antivirus, Anti Malware protection) shall be loaded.
  - Host based firewall shall be enabled and only required ports for SAS should be opened in the host-based firewall.
  - System level user password policy (password complexity & password expiry) shall also be enabled.
  - IP address series will be as allocated by POWERGRID.
  - All required services such as Remote Desktop (RDP), SMB, PowerShell, if required for normal operation shall be listed. Any other specific service requirement of POWERGRID will be communicated at the time of execution for listing.
  - Offline backups for all systems with encryption/checksum shall be provided at the time of SAT.
  - Inventory of all assets shall be carried out as per format laid down in FAT.
  - Specific applications (software) used shall be as per Software Development Life Cycle/best practices. ( Such as ISO/IEC 42010:2011/IEC 62443-4-1)
  - Sensitive database information shall be encrypted.
  - All systems shall be enabled for security logs (for OS, Application security logs and shall have the facility to be routed to a standard syslog server in compatible log formats whose IP address will be shared by POWERGRID).
  - POWERGRID reserves the right to carry out VA at any point of time and vendor shall support for mitigation during warranty period as per CEA guidelines.
4. Following Security features shall be available in Network switches:
- Discovery protocol, Web view, Telnet, TFTP shall be disabled,
  - TLSv1.2 or higher access shall be enabled.
  - User Session timeout shall be enabled. Time of logout due to user inactivity shall be configured.
  - ACL on management interfaces shall be enabled to restrict access.
  - Unused ports, proxy ARP, unused protocols shall be disabled.
  - Broadcast suppression, loop protection shall be enabled.
  - Configurable port rate limiting provision shall be provided.
  - Password complexity shall be enabled.
  - SNMPv3 or higher shall be supported.
  - MAC address-based whitelisting shall be available.
  - Availability of IEEE 802.1x based authentication
5. Following Security features shall be available in Network switches, Firewalls and Networking devices:
- At least two roles should be configured for Network switches as per OEM role recommendation.
  - Default credentials shall be changed/ disabled.
  - Default services (i.e. FTP, HTTP, SMB, Telnet etc.) shall be disabled, if not in use. List of required services shall be verified at the time of FAT.
  - All devices shall be enabled for security logs and shall have the facility to be routed to a standard syslog server in compatible log formats whose IP address will be shared by POWERGRID.
  - Remote administration, if enabled shall be ensured with secure connection (HTTPS/ SSH) only with strong admin credentials.
  - Firmware version along with checksum, product number shall be provided.
  - Time synchronization shall be ensured.
6. Following Security features shall be available in GPS, Fault locators and other network elements:

## Annexure-S12 (Annexure-II-CyberSecurity\_Requirements\_R0)

- Roles should be configured for GPS, Fault locators and other devices .
  - Default credentials shall be changed/ disabled.
  - Default services (i.e. FTP, HTTP, SMB, Telnet etc.) shall be disabled, if not in use. List of required services shall be verified at the time of FAT.
  - All devices shall be enabled for security logs and shall have the facility to be routed to a standard syslog server in compatible log formats whose IP address will be shared by POWERGRID.
  - Remote administration, if enabled shall be ensured with secure connection (HTTPS/ SSH) only with strong admin credentials.
  - Firmware version along with checksum, product number shall be provided.
  - Time synchronization shall be ensured.
7. Training on cyber security should be provided by vendor including following topics but not limited to:
- Patch management
  - Firmware update procedure
  - Perimeter threat protection
  - Configuration of endpoints
  - Security configuration of supplied devices
  - Device hardening

**FAT checklist:**

1.IED Cyber Security capability compliance in the IEDs: following requirements shall be met by IED as per IEEE 1686:2013 clause 5.

Clause Number	Sub-Category	Checklist	Comply/ Exception/ Exceed	Remarks
5 IED Cybersecurity features				
5.1	Electronic access control	Check the IED is protected by unique ID and Password Combination. Check it shall not be possible to gain access to the device without a proper ID/password combination that user has generated.		
5.1.2	Password defeat mechanism	Check IED does not have undisclosed means whereby user-created ID/password can be defeated. Check Embedded master password technique is implemented? Check whether chip-embedded routines that automatically run in the event of hardware or software failure? Check Hardware bypass of passwords, such as jumpers and switch settings is implemented?		
5.1.3	Number of Individual users	Minimum 04 users shall be supported by IED		
5.1.4	Password Construction	Check password supported is At least 8 characters and is case-sensitive. When encoding is in plain text, it shall contain: -At least one uppercase and one lowercase - At least one number - One non-alpha numeric character (@,%,&,*)  Check the user is notified and prompted to choose another password that conforms if it violates.		
5.1.6 IED main security functions				
5.1.6 b)	View configuration settings	Check IED's ability to view configuration settings such as scaling, communication addressing, programmable logic routines(through configuration software), and firmware version		
5.1.6 d)	Configuration change	Check IED's ability to <b>extract &amp; upload configuration files from/to IED</b> to the unit and /or effect changes to the existing configuration		
5.1.6 e)	Firmware change	Firmware change refers to the ability to load new firmware that does not require hardware change.		

5.1.6 f)	ID/Password or RBAC management	ID/Password or RBAC management refers to the ability to load new id that does not require hardware management.	
5.1.6 g)	Audit trail	Audit trail refers to the ability to view and download the audit trail.	
5.1.7	Password Display	Check the vulnerability of password disclosure in local display panel, configuration software (local or remote; offline or online), web browser and terminal access	
5.2 Audit trail			
5.2.4 Audit trail event types			
5.2.4 a)	Log In	Log In (locally or remotely) as a user to the device and check the event is created in audit log.	
5.2.4 f)	Configuration change	Check new configuration file to the IED or new configuration parameters that causes a change in IED configuration is logged in Audit trail	
5.2.4 h)	ID/password creation or modification	Check new ID/password creation/modification is logged in audit log	
5.2.4 i)	ID/Password deletion	Check new ID/password deletion is logged in audit log	
5.3 Supervisory monitoring and control			
5.3.1	Overview of supervisory monitoring and control	IED shall monitor security related activity and shall make the information available through a real time communication protocol for transmission to the supervisory system.	
5.3.3 Alarms: Following shall cause unique alarm occurrence			
5.3.3 b)	Reboot	Rebooting or restarting of IED by means of removing power or through the use of a device resident rebooting mechanism such as reset button, power-up sequence, or access software failure.	
5.3.4	Alarm point change detect	Check the momentary change of events and Alarms is detected as individual alarm and event.	
5.4 IED cyber Security features			
5.4.2 Specific Cryptographic features			
5.4.2 e)	Network time synchronization	NTP shall be NTP v3/4 or SNTP 3/4	
5.5 IED configuration software			
5.5.4.2 change configuration data			
5.5.4.2. a)	Full access	In full access mode, all functions, including ID/password changes and user assignment can be made.	

5.6	Communications port access	Check the communication is not possible in disabled communication port and all the unused UDP/TCP ports are disabled		
-----	----------------------------	--	--	--

Verified by:	
POWERGRID Representative	Manufacturer Representative
Signature :	Signature :
Name :	Name :
Date :	Date :

**SAT checklist:**

1. Configured Security features in each IED including PMU:

Sl.No	IED model	Type of protection/function	Enabled (yes/no)	Remarks
1		DOS protection		
2		NTP/PTP synchronization		
3		Role Based Access Control compliance as per IEC 62351-8 as per the OEM compliance chart (as per table 1.1)		
4		Emergency access to device if connection to RBAC Server is lost		
5		LDAP/AD/Radius support for Authentication and account management		

1.1 RBAC roles as per IEC 62351-8:

Sl.No	IED Model	Type of Role	Created (yes/no)	Remarks
1		Viewer		
2		Operator		
3		Engineer		
4		Administrator		
5		Auditor		
6		RBAC Manager		
7		Super Admin		

2. Following features are to be checked and recorded in Computers/ workstations/ servers/software for Substation Automation System:

S.no	check	Server1	Server2	HMI1	HMI2	Gateway1	Gateway2	DR PC
1.	OS Version							
2.	OS licensed version is used (yes/ no)							
3.	Computer Name							
4.	Windows update date							

Annexure S-14 (Annexure-IV-SAT\_Checklist\_R0)

5.	BIOS Password enabled (yes/No)																			
6.	Check Bluetooth and Wi-Fi Driver are uninstalled.																			
7.	Corresponding hardware is disabled from OS or BIOS (yes/no), if possible.																			
8.	Wake on LAN feature is disabled (yes/no)																			
9.	Check System boot is disabled from USB or any other means (yes/no)																			
10.	Check virtualization feature in CPU is disable																			
11.	Non-administrator accounts enabled for regular work																			
12.	Check changes to setting like a) Boot Sequence b) Boot password c) Wake-on-Lan, d) System time etc. can be made by system admin only (yes/no)																			
13.	Roles such as user, administrator, auditor are configured in IEDs and Associated applications.																			
14.	Only whitelisted software are installed as per table 2.1																			
15.	Security feature enabled as per table 2.2																			
16.	Software license details as per table 2.3																			



30.	Facility provided to route logs to syslog server (yes/no)							
31.	Vulnerabilities mitigated as per assessment report (yes/no)							

2.1 List of software to be whitelisted

S.NO	IED/Machine	Name of White-listed software

2.2 Configured Security features in software application

Sl.No	Application	feature	Enabled or not
1		RBAC	
2		Password complexity	
3		Syslog	
4		Radius/AD Authentication	
5		Enabling of certificate	

2.3 List of software including the license to POWERGRID and validity of software

S. No.	Name of Third-Party Software	License details	Expiry date of License
1			

2.4 List of Services whitelisted:

S.NO	IED/Machine	Name of White-listed Services

**Annexure S-14 (Annexure-IV-SAT\_Checklist\_R0)**

2.5 List of services and TCP/UDP port required to be running in IED/ HMI/ Gateway/ Server/ Switch/ other computers

Computer Name	Name of Services	Status (Enabled/Disabled)	By Default, status	Port	Description

2.6 List of Required TCP/UDP Open Ports (for other devices)

IED/Machine	Service	Required TCP Port	Required UDP Port	IP Address

2.7 Inventory of Assets

Specify Name of PC, Name of software, Version, Application software, database, Open-source libraries used in the development of software.

S.No	Name of PC	Software Name	Version	Use of the software	Name of Open-source library used for the development of software	Name of 3 <sup>rd</sup> party library dll used for the development of software
1						

3. Check whether disk encryption policy is enabled on mobile devices (laptop/External HDD), if possible.
4. Network switches, Firewalls, and other networking devices:

	Firewall-1	Firewall-2	GPS	Fault locator 1..	Switch-1	Switch-2	...
Roles configured							
Default credentials changed/ deleted							
Default services (i.e. FTP, HTTP, SMB, Telnet etc.) disabled							
Security logging enabled							
Facility provided to route logs to syslog server (yes/no)							

Remote administration enabled (yes/no) If yes, secure connection (HTTPS/SSH) is ensured								
Firmware details are provided as per table 4.1								
Time synchronization done (yes/No)								

4.1 Specify Firmware version, Product No and Checksum of all Network switches, Firewalls, and other devices such as GPS, Fault locators, PMU including IEDs

S.No	Name of Device	Firmware Version	Product No	Checksum
1 (e.g.)	ABB (REL 670)	1.5.0.35	1.2.3.5	MD5/SHA/SHA256 of Firm Ware
2				

Note: In some cases, there are two firmware are present in the IED. For e.g. in Siemens IEDs there are two firmware. (EN 100 firmware and other Siprotech firmware).

5. Initialize and test following Cyber Security Logs in Switches

Sl.No	Log name	Availability of log (Yes/No)	Checked log generation OK/Not OK
1.	Login successful		
2.	Logout successful		
3.	Type of login (SSH/VPN/Telnet) successful		
4.	Configuration change successful		
5.	Configuration change failed		
6.	Switch port status changed (Up/Down/disabled/enabled)		
7.	Link status		

8.	Connections denied	
9.	Connections accepted	

6. Initialize and test following Cyber security logs in GPS unit, PMU, Cameras, Applications used for configuring IEDs, BCU, any other device/ application required to generate logs:

S.NO	Description	Checked	Remark
1	Check the Structure of Security Log Entry		Below fields need to be there in the log entry but not limited to this a) Severity b) Date and Time c) IP Address or Port d) Module name & Product Name e) Message
2	Check log is generated when user log in to the system		
3	Check log is generated when user logout from the system		
4	Check log when user enter wrong credentials consecutively three times		
5	Check Log is generated when time out occurs because of inactivity		
6	Check log is generated when a admin user create other user		
7	Check log is generated when user modify the password		
8	Check log is generated when a particular user is deleted from the system		
9	Check log is generated when a control action is performed by user		
10	Check log is generated when a configuration id downloaded		

11	Check log is generated when a configuration is changed		
12	Check log is generated when firmware was changed		
13	Check log is generated when firmware was uploaded		
14	Check log is generated when audit log is viewed/downloaded		
15	Check log is generated when user changed the date and time of a system		
16	Check log is generated when link status is changed on port		
17	Check log is generated when the system restarts automatically		Additional information what triggered the restart
18	Check log is generated when a user initiated the restart		
19	Check log storage capacity of every networking equipment.		

## 7. Check following features in Network Switches:

<b>Procedure</b>			
S.NO.	Description	Checked	Remark
1	Check whether Discovery Protocol is disabled or not		
2	Check whether Web View is disabled or not		
3	Check whether Telnet is disabled or not		
4	Check whether TLS1.2 or hi is enabled or not		
5	Check whether Session timeouts is enabled or not		
6	Check whether ACL on management interfaces to restrict access		
7	Check all unused ports are disabled or not		
8	Check proxy ARP is disable or not		
9	Check Port Configuration	Duplex/Auto/Full	Auto is preferred
10	Check broadcast suppression is enabled or not		
11	Check loop protection algorithm is enabled or not		
12	Check the version of SNMP.		SNMP v3 is recommended

Annexure S-14 (Annexure-IV-SAT\_Checklist\_R0)

13	Check whether all the Unused protocols are disabled or not		
14	Check for availability of IEEE 802.1x based authentication		

Verified by:	
POWERGRID Representative	Manufacturer Representative
Signature :	Signature :
Name :	Name :
Date :	Date :