ICS Cybersecurity Compliance to IEC 62443

Fortinet Solution Mapping Quick Reference Guide

Asset owners and operators of industrial control systems (ICSs) recognize the need to both improve and effectively manage ICS cybersecurity. An abundance of security issues and vulnerabilities lurk within an ICS, mainly an effect of designing, deploying, and operating these systems on legacy technologies, methodologies, and ideologies. With guidance from IEC 62443 and implementation of the Fortinet OT Security Platform, one can approach the security of ICS strategically. Below see how the Fortinet solutions map to the IEC 62443 standard.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 1 – Identification and authentication control (IAC)					**FR 1 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManager**		
FR1 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration.
SR 1.1 RE 1 – Unique identification and authentication		✓	✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiPAM C: Product(s) integration.
SR 1.1 RE 2 – Multifactor authentication for untrusted networks			✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration.
SR 1.1 RE 3 – Multifactor authentication for all networks				✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration.
SR 1.2 – Software process and device identification and authentication		✓	✓	✓	Both	Full	P: FortiEDR, FortiClient, FortiGate C: Product(s) integration.
SR 1.2 RE 1 – Unique identification and authentication			✓	✓	Both	Full	P: FortiEDR, FortiClient, FortiGate C: Product(s) integration.
SR 1.3 – Account management	✓	✓	✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 1.3 RE 1 – Unified account management			✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 1.4 – Identifier management	✓	✓	✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 1.5 – Authenticator management	✓	✓	✓	✓	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 1.5 RE 1 – Hardware security for software process identity credentials			✓	✓	Both	Partial	N: Fortinet do not offer hardware security modules such as HSM or TPM for IACS however, Fortinet product(s) meet the requirement.
SR 1.6 – Wireless access management	✓	✓	✓	✓	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator C: Product(s) integration.
SR 1.6 RE 1 – Unique identification and authentication			✓	✓	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiToken C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 1 – Identification and authentication control (IAC)					**FR 1 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManager**		
FR1 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 1.7 – Strength of password-based authentication	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration.
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration.
SR 1.7 RE 2 – Password lifetime restrictions for all users				✔	Both	Full	P: FortiGate, FortiAuthenticator C: Product(s) integration.
SR 1.8 – Public key infrastructure certificates		✔	✔	✔	Both	Full	P: FortiGate C: PKI and digital certificate configuration within the product(s).
SR 1.9 – Strength of public key authentication		✔	✔	✔	Both	Full	P: FortiGate C: PKI and digital certificate configuration within the product(s).
SR 1.9 RE 1 – Hardware security for public key authentication			✔	✔	Both	Partial	N: Fortinet do not offer hardware security modules such as HSM or TPM for IACS however, Fortinet product(s) meet requirement.
SR 1.10 – Authenticator feedback	✔	✔	✔	✔	Both	Full	P: FortiGate C: Network traffic encryption if/where applicable.
SR 1.11 – Unsuccessful login attempts	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 1.12 – System use notification	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration.
SR 1.13 – Access via untrusted networks	✔	✔	✔	✔	Both	Full	P: FortiGate C: Security policies.
SR 1.13 RE 1 – Explicit access request approval		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiManager C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 2 – Use control (UC)					**FR 2 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiSOAR**		
FR 2 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 2.1 – Authorization enforcement	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.1 RE 1 – Authorization enforcement for all users		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiManager C: Product(s) integration.
SR 2.1 RE 2 – Permission mapping to roles		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiManager C: Product(s) integration.
SR 2.1 RE 3 – Supervisor override			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiManager C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 2 – Use control (UC)					**FR 2 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiSOAR**		
FR 2 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 2.1 RE 4 – Dual approval				✔	Both	Partial	N: IACS asset owner or manufacturer or integrator need to ensure such capability is available within the IACS. Fortinet product(s) can complement with additional features e.g. Multi-factor authentication to meet the requirement.
SR 2.2 – Wireless use control	✔	✔	✔	✔	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.2 RE 1 – Identify and report unauthorized wireless devices			✔	✔	Both	Full	P: FortiAP/FortiWiFi, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.3 – Use control for portable and mobile devices	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.4 – Mobile code	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration.
SR 2.4 RE 1 – Mobile code integrity check			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration.
SR 2.5 – Session lock	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.6 – Remote session termination		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.7 – Concurrent session control			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiManager C: Product(s) integration.
SR 2.8 – Auditable events	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 2.8 RE 1 – Centrally managed, system-wide audit trail			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiPAM, FortiAnalyzer, FortiManager, FortiSIEM, FortiSOAR C: Product(s) integration.
SR 2.9 – Audit storage capacity	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 2.10 – Response to audit processing failures	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 2.11 – Timestamps		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 2 – Use control (UC)					**FR 2 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiPAM, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiSOAR**		
FR 2 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	**SL2**	**SL3**	**SL4**	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 2.11 RE 1 – Internal time synchronization			✔	✔	Both	Full	P: FortiGate, FortiSwitch N: The product (s) can function as NTP server to provide time to the network connected assets. Precise time synchronization functionality over network e.g., IEEE 1588v2 PTP is available only in select product(s).
SR 2.11 RE 2 – Protection of time source integrity				✔	Both	Full	P: FortiGate N: Capability is limited to any network asset(s) connected to/via the product(s).
SR 2.12 – Non-repudiation			✔	✔	Both	Full	P: FortiGate N: Capability is limited to any network asset(s) connected to/via the product(s).
SR 2.12 RE 1 – Non-repudiation for all users				✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAuthenticator, FortiPAM, FortiAnalyzer, FortiManager C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 3 – System integrity (SI)					**FR 3 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiTester, FortiResponder**		
FR 3 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	**SL2**	**SL3**	**SL4**	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 3.1 – Communication integrity	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 3.1 RE 1 – Cryptographic integrity protection			✔	✔	Both	Full	P: FortiGate, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 3.2 – Malicious code protection	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration.
SR 3.2 RE 1 – Malicious code protection on entry and exit points		✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiSandbox C: Product(s) integration.
SR 3.2 RE 2 – Central management and reporting for malicious code protection			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiManager, FortiSandbox C: Product(s) integration.
SR 3.3 – Security functionality verification	✔	✔	✔	✔	Both	Full	P: FortiTester and FortiResponder N: The product can be offered as a service.
SR 3.3 RE 1 – Automated mechanisms for security functionality verification			✔	✔	Both	Full	P: FortiTester, FortiResponder N: The product can be offered as a service.
SR 3.3 RE 2 – Security functionality verification during normal operation				✔	Both	Full	P: FortiTester, FortiResponder N: The product can be offered as a service.
SR 3.4 – Software and information integrity	✔	✔	✔	✔	Both	Full	P: FortiTester, FortiResponder N: The product can be offered as a service.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 3 – System integrity (SI)					**FR 3 Product Mapping: FortiGate, FortiWiFi/FortiAP, FortiAuthenticator, FortiToken, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSandbox, FortiSIEM, FortiTester, FortiResponder**		
FR 3 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	**SL2**	**SL3**	**SL4**	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 3.4 RE 1 – Automated notification about integrity violations			✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration.
SR 3.5 – Input validation	✔	✔	✔	✔	Both	Partial	N: Fortinet product(s) are compliant with the requirement however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 3.6 – Deterministic output	✔	✔	✔	✔	Both	Partial	N: Fortinet product(s) are compliant with the requirement however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 3.7 – Error handling		✔	✔	✔	Both	Partial	N: Fortinet product(s) are compliant with the requirement however, IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 3.8 – Session integrity		✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 3.8 RE 1 – Invalidation of session IDs after session termination			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 3.8 RE 2 – Unique session ID generation			✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 3.8 RE 3 – Randomness of session IDs				✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiToken, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 3.9 – Protection of audit information		✔	✔	✔	Both	Full	C: Restrict access to the Fortinet product(s) that offer centralised logging and monitoring capability.
SR 3.9 RE 1 – Audit records on write-once media				✔	Both	Full	C: Restrict access to the Fortinet product(s) that offer centralised logging and monitoring capability.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 4 – Data confidentiality (DC)					**FR 4 Product Mapping: FortiGate**		
FR 4 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	**SL2**	**SL3**	**SL4**	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 4.1 – Information confidentiality	✔	✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement encryption of relevant information in transit.
SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks		✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement encryption of relevant information in transit for untrusted networks.
SR 4.1 RE 2 – Protection of confidentiality across zone boundaries				✔	Both	Full	P: FortiGate C: Using the product(s), implement protection/ encryption of relevant information in transit between the zones.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 4 – Data confidentiality (DC)					**FR 4 Product Mapping: FortiGate**		
FR 4 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 4.2 – Information persistence		✔	✔	✔	Both	Partial	N: IACS asset owner or manufacturer need to ensure such capability is available within the IACS. Fortinet product(s) have built-in capability to meet the requirement.
SR 4.2 RE 1 – Purging of shared memory resources			✔	✔	Both	Partial	N: IACS asset owner or manufacturer need to ensure such capability is available within the IACS. Fortinet product(s) have built-in capability to meet the requirement.
SR 4.3 – Use of cryptography	✔	✔	✔	✔	Both	Partial	N: IACS asset owner or manufacturer need to ensure such capability is available within the IACS. Fortinet product(s) have built-in capability to meet the requirement.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 5 – Restricted data flow (RDF)					**FR 5 Product Mapping: FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer**		
FR 5 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 5.1 – Network segmentation	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks.
SR 5.1 RE 1 – Physical network segmentation		✔	✔	✔	IACS	None	N: IACS asset owner or manufacturer or integrator need to ensure physical network segmentation for relevant IACS assets.
SR 5.1 RE 2 – Independence from non-control system networks			✔	✔	Both	Full	P: FortiGate, FortiNAC C: Products(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks.
SR 5.1 RE 3 – Logical and physical isolation of critical networks				✔	Both	Full	P: FortiGate, FortiNAC C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks. Applicable for logical segmentation.
SR 5.2 – Zone boundary protection	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiNAC, FortiAnalyzer C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks and centralised logging and monitoring.
SR 5.2 RE 1 – Deny by default, allow by exception		✔	✔	✔	Both	Full	P: FortiGate, FortiNAC, FortiAnalyzer C: Product(s) integration and implementation of security zones and conduits within Layer 3 and/or Layer 2 networks.
SR 5.2 RE 2 – Island mode			✔	✔	IACS	Partial	N: The requirement is applicable for IACS. Fortinet product(s) can offer such capability.
SR 5.2 RE 3 – Fail close			✔	✔	IACS	Partial	N: The requirement is applicable for IACS. Fortinet product(s) can offer such capability.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 5 – Restricted data flow (RDF)					**FR 5 Product Mapping: FortiGate, FortiSwitch, FortiNAC, FortiClient, FortiEDR, FortiAnalyzer**		
FR 5 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 5.3 – General purpose person-to-person communication restrictions	✔	✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement deny all network communication except allowed by the security policy.
SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications			✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement deny all network communication except allowed by the security policy.
SR 5.4 – Application partitioning	✔	✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 6 – Timely response to events (TRE)					**FR 6 Product Mapping: FortiGate, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSIEM**		
FR 6 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 6.1 – Audit log accessibility	✔	✔	✔	✔	Both	Full	P: FortiGate, FortiAuthenticator, FortiAnalyzer, FortiManager C: Product(s) integration.
SR 6.1 RE 1 – Programmatic access to audit logs			✔	✔	Both	Full	P: FortiAnalyzer C: Integration with IACS may be required for provisioning access to the logging and monitoring information available within Fortinet product(s) e.g. via syslog etc.
SR 6.2 – Continuous monitoring		✔	✔	✔	Both	Full	P: FortiEDR, FortiClient, FortiGate, FortiAnalyzer, FortiManager, FortiSIEM C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 7 – Resource availability (RA)					**FR 7 Product Mapping: FortiGate, FortiDDoS, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSOAR, Fabric-Ready Partner Solutions**		
FR 7 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	SL2	SL3	SL4	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 7.1 – Denial of service protection	✔	✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection policies.
SR 7.1 RE 1 – Manage communication loads		✔	✔	✔	Fortinet	Full	P: FortiGate C: Using the product(s), implement DoS protection, SYN flood protection, rate-limit, traffic shaping policies.
SR 7.1 RE 2 – Limit DoS effects to other systems or networks			✔	✔	Fortinet	Full	P: FortiGate, FortiDDoS C: Using the product(s), implement DoS protection, SYN flood protection, rate-limit policies.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 7 – Resource availability (RA)					**FR 7 Product Mapping: FortiGate, FortiDDoS, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSOAR, Fabric-Ready Partner Solutions**		
FR 7 – SRs & REs	**Security Levels**				Relevance	Compliance	Solution Description
	SL1	SL2	SL3	SL4	IACS/ Fortinet	Full/Partial/ None	(P: Product, C: Configuration, N: Note)
SR 7.2 – Resource management	✔	✔	✔	✔	Both	Full	P: FortiGate C: Using the product(s), implement, rate-limit and connection restriction policies.
SR 7.3 – Control system backup	✔	✔	✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 7.3 RE 1 – Backup verification		✔	✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 7.3 RE 2 – Backup automation			✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 7.4 – Control system recovery and reconstitution	✔	✔	✔	✔	Both	Partial	P: FortiEDR Manager, FortiAnalyzer, FortiManager, Fabric-Ready Partner Solutions C: The product(s) support configuration backup for Fortinet products and can be integrated with Fabric-Ready partner solutions that offer capability to meet the requirement. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 7.5 – Emergency power	✔	✔	✔	✔	Both	Partial	N: Fortinet product(s) are available with redundant power inputs/supplies and can be configured in high-availability and fault-tolerant configuration. IACS asset owner or manufacturer or integrator need to ensure the capability is also available within the IACS.
SR 7.6 – Network and security configuration settings	✔	✔	✔	✔	Both	Full	P: FortiGate N: Fortinet product(s) support baseline configuration and dedicated management interface for configuration and operations management.
SR 7.6 RE 1 – Machine-readable reporting of current security settings			✔	✔	Both	Full	P: FortiAnalyzer, FortiManager C: Product(s) integration.

IEC 62443-3-3 FRs, SRs and REs					Fortinet Solution Mapping and Compliance		
FR 7 – Resource availability (RA)					**FR 7 Product Mapping: FortiGate, FortiDDoS, FortiClient, FortiEDR, FortiAnalyzer, FortiManager, FortiSOAR, Fabric-Ready Partner Solutions**		
FR 7 – SRs & REs	**Security Levels**				**Relevance**	**Compliance**	**Solution Description**
	SL1	**SL2**	**SL3**	**SL4**	**IACS/ Fortinet**	**Full/Partial/ None**	**(P: Product, C: Configuration, N: Note)**
SR 7.7 – Least functionality	✓	✓	✓	✓	Both	Full	P: FortiGate, FortiEDR, FortiClient C: Product(s) integration and implementation of security policies to restrict unnecessary functions/ports/protocols/services.
SR 7.8 – Control system component inventory		✓	✓	✓	Both	Full	P: FortiGate, FortiAnalyzer, FortiSOAR, Fabric-Ready Partner Solutions C: Product(s) integration.

More details can be found in the [Effective ICS Cybersecurity Using the IEC 62443 Standard](#) white paper published in partnership with the SANS Institute.

FORTINET

www.fortinet.com