

S21 SEC

CYBERSECURITY
YOU CAN TRUST

Key Cyber Security Requirements for Wind Farms according to IEC 62443



SPEAKER



Elyoenai Egozcue

Head of ICS Cybersecurity Services

Mr. Elyoenai Egozcue received his M.Sc. in Telecommunications Engineer from the UPNA University of Pamplona, Spain undertaking his Master Thesis at the VUB University of Brussels, Belgium. He started his professional career as a cyber security researcher at S21sec Labs, dealing with open-source cyber intelligence, RFID security, Network security and biometrics. He is currently the head of cyber security services for industrial automation and control systems at S21sec and leads relevant projects in this field in sectors such as renewable power generation, power transmission and distribution, railway transportation, logistics, etc.



www.linkedin.com/in/eegozcue/

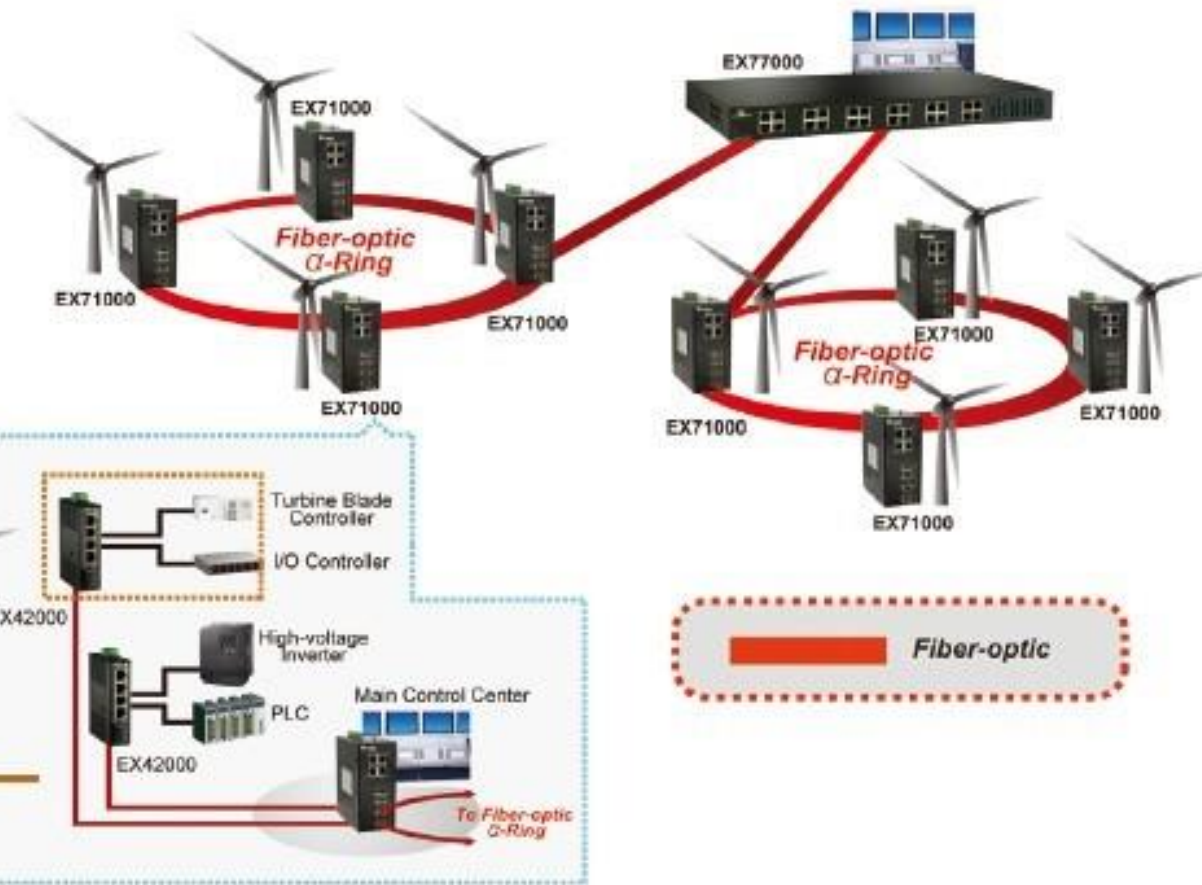


[@ElyoenaiEM](https://twitter.com/ElyoenaiEM)

INDEX

1. General concepts: SuC, FR, SL
2. Security requirements at system and component levels
3. Conclusions

IEC 62443 – System Under Consideration (SuC)



SYSTEM COMPONENTS:

Embedded Device (ED): PLC, IEDs (e.g. inverter), CMS, controller.

Network Device (ND): switches, routers, VPN terminator, firewalls.

Host: Linux Redhat, Windows XP, Windows 2000 Server, etc.

Software Application: Historian, SCADA, engineering station, etc.

IEC 62443 – Foundational Requirements (FR)

The IEC 62443 groups technical security controls into 7 categories

FR1 – Identification and Authentication Control (IAC)

FR2 – Use Control (UC)

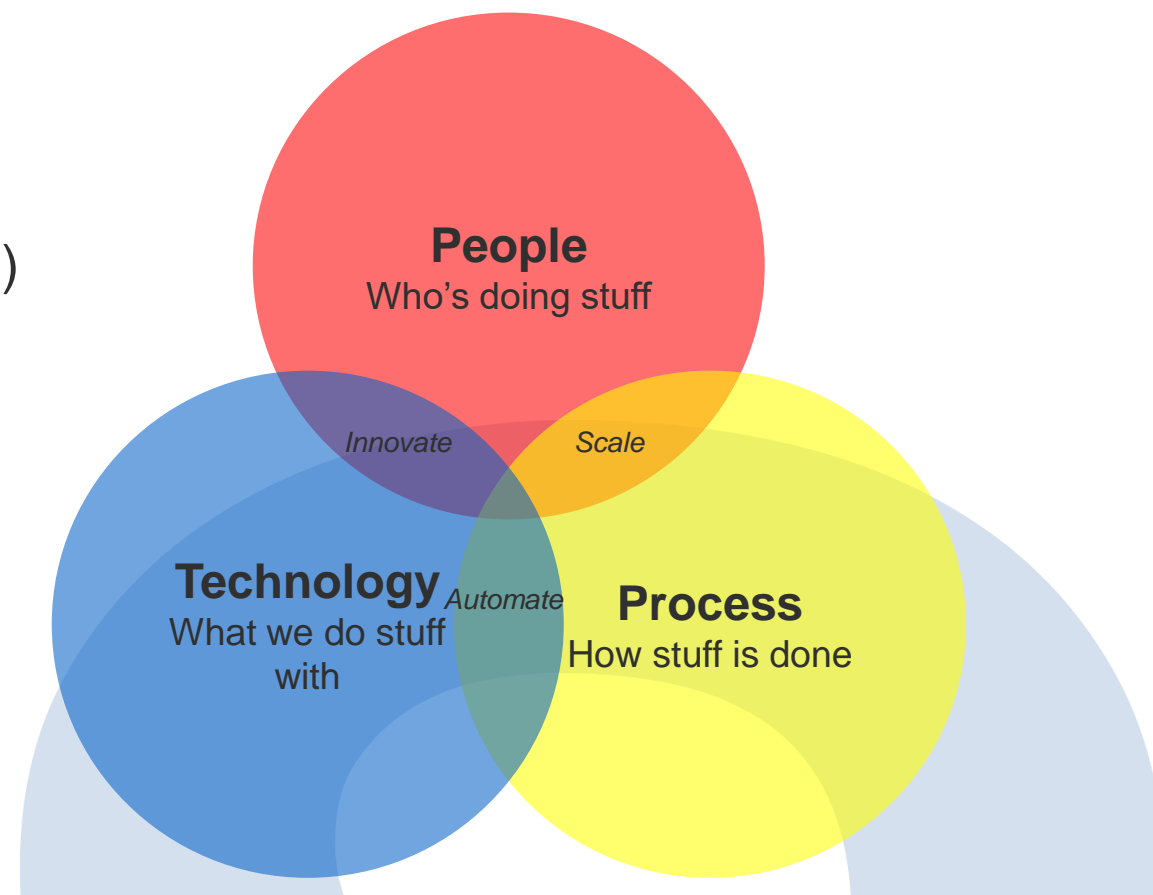
FR3 – System Integrity (SI)

FR4 – Data Confidentiality (DC)

FR5 – Restricted Data Flow (RDF)

FR6 – Timely Response to Events (TRE)

FR7 – Resource Availability (RA)



Technical security requirements are derived from FR and defined at system (SR) and component levels (CR). Component Requirements (CR) will vary sometimes depending on the component type: EDR, NDR, HR, SAR

IEC 62443 – Security Levels

Safety systems have used the concept of **Safety Integrity Levels (SIL)**.

SIL allowed integrity capability of components and systems to be represented by a number (e.g. SIL 2).

SIL Safety Integrity Level (per IEC 61508)	Safety Availability	PFD Probability of Failure on Demand 1 - Availability	RRF Risk Reduction Factor 1 / PFD
4	> 99.99%	< 0.0001 ($1E^{-4}$)	> 10,000
3	99.9 – 99.99%	0.001 – 0.0001 ($1E^{-3}$ to $1E^{-4}$)	1,000 – 10,000
2	99 – 99.9%	0.01 – 0.001 ($1E^{-2}$ to $1E^{-3}$)	100 – 1,000
1	90 – 99%	0.1 – 0.01 ($1E^{-1}$ to $1E^{-2}$)	10 - 100
0	Basic Process Control		

Security Levels provide a qualitative approach to addressing security for a zone, system, component

- **Target security level (SL-T):** desired level of security.
- **Achieved security level (SL-A):** the actual level of security for a particular system.
- **Capability security level (SL-C):** the security level that components or systems can provide.

SL	Definition of protection level
4	intentional violation using sophisticated means with extended resources, system specific skills and high motivation
3	intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivation
2	intentional violation using simple means with low resources, generic skills and low motivation
1	casual or coincidental violation
0	no especial security requirements for any FR

IEC 62443 – Security requirements: Human user identification and authentication

IEC 62443-3-3	IEC 62443-4-2	Real world examples
<p>SR 1.1 The control system shall provide the capability to identify and authenticate all human users on all interfaces that provide human user access to the control system.</p> <p>SR 1.1 RE 1 Uniquely identify and authenticate all human users</p> <p>SR 1.1 RE 2 Employ multifactor authentication for access via untrusted networks</p> <p>SR 1.1 RE 3 Multifactor authentication for all networks</p>	<p>CR 1.1 All human users need to be identified and authenticated for all access to components (e.g. applications and devices) on all interfaces. This includes access through network protocols HTTP, HTTPS, FTP, SFTP, and protocols used by device configuration tools.</p> <p>CR 1.1 RE 1 Unique identification and authentication</p> <p>CR 1.1 RE 2 Multifactor authentication for all interfaces of the component</p>	<p>Authentication methods: passwords, tokens, biometrics and a combination of them.</p> <p>Other factors: geographic location</p> <p>Role-based authentication can be used but it is not a unique identification.</p> <p>A system-level identification and authentication capability is preferred from a management perspective (i.e. AD, LDAP, Radius)</p>

Common types of 2FA



Note: Access controls (IAC and UC) shall not prevent the operation of essential functions

IEC 62443 – Security requirements: Zone boundary protection

IEC 62443-3-3	IEC 62443-4-2	Real world examples
<p>SR 5.2 The control system shall monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.</p> <p>SR 5.2 RE 1 Deny by default, allow by exception policy.</p> <p>SR 5.2 RE 2 Prevent communication through the control system boundary (Island mode)</p> <p>SR 5.2 RE 3 Fail close functionality</p>	<p>NDR 5.2 the network device shall monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.</p> <p>NDR 5.2 RE 1 Dany all, permit by exception</p> <p>NDR 5.2 RE 2 Island mode</p> <p>NDR 5.2 RE 3 Fail close</p>	<p>Boundary protection mechanisms: firewalls, routers, proxies, etc.</p> <p>Island mode is key to content security breaches when been detected within the control system, or when an attack is occurring at the enterprise level.</p> <p>When a hardware/power failure occurs at the boundary protection mechanism, the goal is to prevent any communications through the control system boundary (fail close)</p>

IEC 62443 – Security requirements: Zone boundary protection

IEC 62443

SR 5.2 The control system shall ensure the security of control communications to enforce the compartmentalization of the control system in the risk-based zones.

SR 5.2 RE 1 Deny by default all connections to the control system with exception policy.

SR 5.2 RE 2 Prevent compromise of the control system boundary.

SR 5.2 RE 3 Fail close.

Threat Prevention Engine Settings

General
Anti-Bot
Threat Emulation
Threat Extraction
UserCheck

Fail Mode
In case of internal system error
 Allow all connections (Fail-open)
 Block all connections (Fail-close)

Check Point Online Web Service
 Block connections when the web service is unavailable
Resource classification mode
 Background - requests are allowed until categorization is complete
 Hold - requests are blocked until categorization is complete
 Custom - configured different settings

Emulation Limits
Maximum file size for emulation (KB): 30000
Maximum emulation time (seconds): 60
Maximum file time in queue (minutes): 720
When limit is exceeded traffic is **accepted** with track: Log

Connection Unification
Session unification timeout (minutes): 60

HTTP Inspection
 Enable HTTP inspection on non standard ports

OK Cancel

Note: Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode

IEC 62443 – Security requirements: Control system backup

IEC 62443-3-3	IEC 62443-4-2	Real world examples
<p>SR 7.3 The control system shall support backups of user-level and system-level information (including system state information) without affecting normal plant operations. Information required for post-incident forensic activity (e.g. audit logs) should be included</p> <p>SR 7.3 RE 1 Capability to verify the reliability of backup mechanisms.</p> <p>SR 7.3 RE 2 Capability to automate the backup function based on a configurable frequency</p>	<p>CR 7.3 Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level info). The backup process shall not affect the normal component operations. Cryptographic keys should be included and recommended to backup separately as security requirements for protecting the backup are higher.</p> <p>CR 7.3 RE 1 Capability to validate the integrity of backed up information prior to the initiation of a restore</p>	<p>Techniques and tools:</p> <ul style="list-style-type: none">- NAS server with a file structure and a batch process- Proprietary solutions (e.g. Siemens TIA Portal)- Multivendor solutions: VersionDOG or MDT Autosave

IEC 62443 – Security requirements: Control system backup

IEC 62443-2-2	Company	IEC 62443-4-2	Real world examples
<p>SR 7.3 The control system shall supply backups of user-level and system-level information (including system state information) without affecting normal plant operations. Information required for post-incident forensic activity (e.g. audit logs) should be included.</p> <p>SR 7.3 RE 1 Capability to verify the reliability of backup mechanisms.</p> <p>SR 7.3 RE 2 Capability to automate the backup function based on a configurable frequency</p>		<p>Techniques and tools:</p> <ul style="list-style-type: none"> - NAS server with a file structure and a batch process - Proprietary solutions (e.g. Siemens TIA Portal) - Multivendor solutions: VersionDOG or MDT Autosave 	

IEC 62443 – Security requirements: Control system backup

Company

IEC 62443-2

IEC 62443-4-2

Real world examples

SR 7.3 The backups of information operations incident should be

SR 7.3 RE of backup

SR 7.3 RE backup frequency

The screenshot displays the AdminClient software interface for configuring and monitoring tasks. The main window is titled 'versiondog - AdminClient - Tareas'. The interface includes a menu bar (Inicio, Vista, Ayuda), a toolbar with various icons for file operations and task management, and a breadcrumb navigation path: Empresa > Planta 1 > Cocción > Máquina 1 > PLC1 > S-PLC1.

The 'Árbol de proyectos' (Project Tree) on the left shows a hierarchical structure of folders and files, including 'Su Empresa', 'Planta 1', 'Cocción', 'Máquina 1', 'PLC1', 'Doc-S-PLC1', 'S-PLC1', 'PLC2', 'Máquina 2', 'Fermentación', 'Línea de embotellado', 'Maduración', 'Malteado', 'Planta 2', 'Planta 3', and 'wINGELAN'.

The 'Tareas' (Tasks) table shows a single task configuration:

Estado de ejecución	Último inicio	Nombre de la tarea	Tipo de carga	Programación
Según programación	28/11/2018 9:54	PLC1	SIMATIC S7	Cada día, a las 01:00

The 'Resultados de tareas' (Task Results) table provides a detailed log of task executions:

Fecha y hora de la tarea (lc)	Versión	Copia de seguridad	Lugar de la ejecución
28/11/2018 9:54:54	13	20181126.003	Servidor de versiondog (INGELAN.DOG)
26/11/2018 11:35:50	13	20181126.003	Servidor de version...
26/11/2018 11:33:14	12	20181126.003	Servidor de version...
26/11/2018 11:31:20	12	20181126.002	Servidor de version...
26/11/2018 11:28:15	12	20181126.002	Servidor de version...
26/11/2018 9:29:44	11	20181126.001	Servidor de version...
26/11/2018 9:29:13	11	20181126.001	Servidor de version...

The 'Configuración de tareas' (Task Configuration) panel on the right shows the following settings:

- Tipo de carga: SIMATIC S7
- Aplicar: Según programación
- Nombre de la tarea: PLC1
- Componente: \DAMM\Planta 1\Cocción\Máquina 1\PLC1\S-PLC1
- Notificar: Administrador
- Advertir si la copia de seguridad tiene más de: Nunca advertir
- Programación: Cada día, a las 01:00
- En caso de error: Ninguna acción fue especificada
- Ejecución desde: Automático
- Id de tarea: 8F651CC239034EE58FCBC28CA35C599
- Id de componente: A8D90A33316444CC932F6DADD4846CC9

Buttons at the bottom of the configuration panel include 'Guardar', 'Eliminar', and 'Resetear'.

Conclusions

1. IEC 62443 defines technical requirements at system or component levels to achieve certain SL-C
2. Depending on the security level to be achieved, enhancements to requirements should be considered
3. Security measures shall not adversely affect essential functions of a high availability IACS
4. Both component vendors and system integrators have a major responsibility in achieving the SL-T

OFFICES

Madrid

C/Ramírez de Arellano,
21, CP 28043

Pamplona

P. E. La Muga, 11, 1ª Planta,
31160, Orkoien (Navarra)

Barcelona

C/Tarragona, 141-157,
Piso 14, CP 08014

Vitoria - Gasteiz

Edificio Azucarera Avda. de
los Huetos 75, oficina 38

Porto

Lugar do Espido, via norte
4470-177. Maia

San Sebastián

P.E. Zuatzu, Ed. Urgull, 2º,
CP 20018

León

Edificio CEBT, Calle Santos
Ovejero 1. Oficina PB08

Bilbao

C/ Camino de Laida
Edificio 207, Bloque B 1º
planta

Lisboa

Rua do Viriato, 13B, 4º
Andar. 1050-233, PT

Ciudad de Mexico

Calle Río Pánuco, 108. Colonia
Renacimiento, Ciudad de México



S21 SEC



facebook.com/pages/S21sec



linkedin.com/company/s21sec



twitter.com/@S21sec



instagram.com/s21_sec



www.s21sec.com