

Redes de comunicaciones industriales
Seguridad de la red y del sistema
Parte 3-3: Requisitos de seguridad del sistema y
niveles de seguridad

Esta norma ha sido elaborada por el comité técnico CTN 203 *Equipamiento eléctrico y sistemas automáticos para la industria*, cuya secretaría desempeña SERCOBE.



EXTRACTO DEL DOCUMENTO UNE-EN IEC 62443-3-3

UNE-EN IEC 62443-3-3

Redes de comunicaciones industriales
Seguridad de la red y del sistema
Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad

Industrial communication networks. Network and system security. Part 3-3: System security requirements and security levels.

Réseaux industriels de communication. Sécurité dans les réseaux et les systèmes. Partie 3: Exigences relatives à la sécurité dans les systèmes et niveaux de sécurité.

Esta norma es la versión oficial, en español, de las Normas Europeas EN IEC 62443-3-3:2019 y EN IEC 62443-3-3:2019/AC:2019-10, que a su vez adoptan las Normas Internacionales IEC 62443-3-3:2013 e IEC 62443-3-3:2013/COR1:2014.

EXTRACTO DEL DOCUMENTO UNE-EN IEC 62443-3-3

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización

Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

© UNE 2020

Prohibida la reproducción sin el consentimiento de UNE.

Todos los derechos de propiedad intelectual de la presente norma son titularidad de UNE.

Índice

Prólogo europeo	11
Declaración.....	11
Prólogo.....	12
0 Introducción.....	14
0.1 Visión de conjunto.....	14
0.2 Propósito y público al que está destinada la norma.....	15
0.3 Uso con otras partes de la serie de Normas IEC 62443.....	16
1 Objeto y campo de aplicación.....	18
2 Normas para consulta.....	18
3 Términos, definiciones, abreviaturas, acrónimos y convenciones	19
3.1 Términos y definiciones.....	19
3.2 Abreviaturas y acrónimos	24
3.3 Convenciones	27
4 Restricciones comunes en materia de seguridad del sistema de control	28
4.1 Visión de conjunto.....	28
4.2 Admisión de funciones esenciales.....	28
4.3 Contramedidas compensatorias	29
4.4 Privilegio mínimo.....	30
5 FR 1 - Control de identificación y autenticación.....	30
5.1 Propósito y descripciones del nivel de seguridad de capacidad SL-C(IAC).....	30
5.2 Justificación	30
5.3 SR 1.1 - Identificación y autenticación de usuarios humanos	31
5.3.1 Requisito.....	31
5.3.2 Justificación y directrices adicionales	31
5.3.3 Mejoras de los requisitos.....	31
5.3.4 Niveles de seguridad	32
5.4 SR 1.2 - Identificación y autenticación de procesos de software y dispositivos.....	32
5.4.1 Requisito.....	32
5.4.2 Justificación y directrices adicionales	32
5.4.3 Mejoras de los requisitos.....	33
5.4.4 Niveles de seguridad	33
5.5 SR 1.3 - Gestión de cuentas.....	33
5.5.1 Requisito.....	33
5.5.2 Justificación y directrices adicionales	34
5.5.3 Mejoras de los requisitos.....	34
5.5.4 Niveles de seguridad	34
5.6 SR 1.4 - Gestión de identificadores.....	34
5.6.1 Requisito.....	34
5.6.2 Justificación y directrices adicionales	35
5.6.3 Mejoras de los requisitos.....	35
5.6.4 Niveles de seguridad	35
5.7 SR 1.5 - Gestión de autenticadores	35
5.7.1 Requisito.....	35
5.7.2 Justificación y directrices adicionales	36

5.7.3	Mejoras de los requisitos.....	37
5.7.4	Niveles de seguridad	37
5.8	SR 1.6 – Gestión de acceso inalámbrico.....	37
5.8.1	Requisito.....	37
5.8.2	Justificación y directrices adicionales	37
5.8.3	Mejoras de los requisitos.....	38
5.8.4	Niveles de seguridad	38
5.9	SR 1.7 – Fortaleza de la autenticación basada en contraseña	38
5.9.1	Requisito.....	38
5.9.2	Justificación y directrices adicionales	38
5.9.3	Mejoras de los requisitos.....	39
5.9.4	Niveles de seguridad	39
5.10	SR 1.8 – Certificados de infraestructura de clave pública (PKI).....	39
5.10.1	Requisito.....	39
5.10.2	Justificación y directrices adicionales	40
5.10.3	Mejoras de los requisitos.....	40
5.10.4	Niveles de seguridad	40
5.11	SR 1.9 – Fortaleza de la autenticación de clave pública.....	40
5.11.1	Requisito.....	40
5.11.2	Justificación y directrices adicionales	41
5.11.3	Mejoras de los requisitos.....	41
5.11.4	Niveles de seguridad	41
5.12	SR 1.10 – Retroalimentación del autenticador	42
5.12.1	Requisito.....	42
5.12.2	Justificación y directrices adicionales	42
5.12.3	Mejoras de los requisitos.....	42
5.12.4	Niveles de seguridad	42
5.13	SR 1.11 – Intentos fallidos de inicio de sesión	42
5.13.1	Requisito.....	42
5.13.2	Justificación y directrices adicionales	43
5.13.3	Mejoras de los requisitos.....	43
5.13.4	Niveles de seguridad	43
5.14	SR 1.12 – Aviso de uso del sistema	43
5.14.1	Requisito.....	43
5.14.2	Justificación y directrices adicionales	43
5.14.3	Mejoras de los requisitos.....	44
5.14.4	Niveles de seguridad	44
5.15	SR 1.13 – Acceso a través de redes que no son de no confianza	44
5.15.1	Requisito.....	44
5.15.2	Justificación y directrices adicionales	44
5.15.3	Mejoras de los requisitos.....	45
5.15.4	Niveles de seguridad	45
6	FR 2 – Control de uso	45
6.1	Propósito y descripciones del nivel de seguridad de capacidad SL-C(UC)	45
6.2	Justificación	46
6.3	SR 2.1 – Aplicación de la autorización.....	46
6.3.1	Requisito.....	46
6.3.2	Justificación y directrices adicionales	46
6.3.3	Mejoras de los requisitos.....	47
6.3.4	Niveles de seguridad	47
6.4	SR 2.2 – Control de uso inalámbrico	48
6.4.1	Requisito.....	48
6.4.2	Justificación y directrices adicionales	48
6.4.3	Mejoras de los requisitos.....	48

6.4.4	Niveles de seguridad	48
6.5	SR 2.3 – Control de uso para dispositivos portátiles y móviles	49
6.5.1	Requisito.....	49
6.5.2	Justificación y directrices adicionales	49
6.5.3	Mejoras de los requisitos.....	49
6.5.4	Niveles de seguridad	49
6.6	SR 2.4 – Código móvil	50
6.6.1	Requisito.....	50
6.6.2	Justificación y directrices adicionales	50
6.6.3	Mejoras de los requisitos.....	50
6.6.4	Niveles de seguridad	50
6.7	SR 2.5 – Bloqueo de la sesión.....	51
6.7.1	Requisito.....	51
6.7.2	Justificación y directrices adicionales	51
6.7.3	Mejoras de los requisitos.....	51
6.7.4	Niveles de seguridad	51
6.8	SR 2.6 – Terminar una sesión remota	51
6.8.1	Requisito.....	51
6.8.2	Justificación y directrices adicionales	52
6.8.3	Mejoras de los requisitos.....	52
6.8.4	Niveles de seguridad	52
6.9	SR 2.7 – Control de sesiones simultáneas	52
6.9.1	Requisito.....	52
6.9.2	Justificación y directrices adicionales	52
6.9.3	Mejoras de los requisitos.....	52
6.9.4	Niveles de seguridad	52
6.10	SR 2.8 – Eventos auditables.....	53
6.10.1	Requisito.....	53
6.10.2	Justificación y directrices adicionales	53
6.10.3	Mejoras de los requisitos.....	53
6.10.4	Niveles de seguridad	54
6.11	SR 2.9 – Capacidad de almacenamiento de datos de auditoría	54
6.11.1	Requisito.....	54
6.11.2	Justificación y directrices adicionales	54
6.11.3	Mejoras de los requisitos.....	54
6.11.4	Niveles de seguridad	54
6.12	SR 2.10 – Respuesta a los fallos de procesamiento de auditorías.....	55
6.12.1	Requisito.....	55
6.12.2	Justificación y directrices adicionales	55
6.12.3	Mejoras de los requisitos.....	55
6.12.4	Niveles de seguridad	55
6.13	SR 2.11 – Marcas de tiempo	55
6.13.1	Requisito.....	55
6.13.2	Justificación y directrices adicionales	56
6.13.3	Mejoras de los requisitos.....	56
6.13.4	Niveles de seguridad	56
6.14	SR 2.12 – No rechazo.....	56
6.14.1	Requisito.....	56
6.14.2	Justificación y directrices adicionales	57
6.14.3	Mejoras de los requisitos.....	57
6.14.4	Niveles de seguridad	57
7	FR 3 – Integridad del sistema	57
7.1	Propósito y descripciones del nivel de seguridad de capacidad SL-C(SI)	57
7.2	Justificación	58

7.3	SR 3.1 – Integridad de la comunicación.....	58
7.3.1	Requisito.....	58
7.3.2	Justificación y directrices adicionales	58
7.3.3	Mejoras de los requisitos.....	59
7.3.4	Niveles de seguridad	59
7.4	SR 3.2 – Protección contra códigos maliciosos	59
7.4.1	Requisito.....	59
7.4.2	Justificación y directrices adicionales	60
7.4.3	Mejoras de los requisitos.....	60
7.4.4	Niveles de seguridad	60
7.5	SR 3.3 – Verificación de la funcionalidad de la seguridad	61
7.5.1	Requisito.....	61
7.5.2	Justificación y directrices adicionales	61
7.5.3	Mejoras de los requisitos.....	61
7.5.4	Niveles de seguridad	62
7.6	SR 3.4 – Integridad del software y de la información.....	62
7.6.1	Requisito.....	62
7.6.2	Justificación y directrices adicionales	62
7.6.3	Mejoras de los requisitos.....	62
7.6.4	Niveles de seguridad	63
7.7	SR 3.5 – Validación de entrada.....	63
7.7.1	Requisito.....	63
7.7.2	Justificación y directrices adicionales	63
7.7.3	Mejoras de los requisitos.....	63
7.7.4	Niveles de seguridad	63
7.8	SR 3.6 – Salida determinista	64
7.8.1	Requisito.....	64
7.8.2	Justificación y directrices adicionales	64
7.8.3	Mejoras de los requisitos.....	64
7.8.4	Niveles de seguridad	64
7.9	SR 3.7 – Tratamiento de errores	64
7.9.1	Requisito.....	64
7.9.2	Justificación y directrices adicionales	65
7.9.3	Mejoras de los requisitos.....	65
7.9.4	Niveles de seguridad	65
7.10	SR 3.8 – Integridad de la sesión.....	65
7.10.1	Requisito.....	65
7.10.2	Justificación y directrices adicionales	65
7.10.3	Mejoras de los requisitos.....	65
7.10.4	Niveles de seguridad	66
7.11	SR 3.9 – Protección de la información de auditoría	66
7.11.1	Requisito.....	66
7.11.2	Justificación y directrices adicionales	66
7.11.3	Mejoras de los requisitos.....	66
7.11.4	Niveles de seguridad	67
8	FR 4 – Confidencialidad de los datos	67
8.1	Propósito y descripciones del nivel de seguridad de capacidad SL-C(DC)	67
8.2	Justificación	67
8.3	SR 4.1 – Confidencialidad de la información	67
8.3.1	Requisito.....	67
8.3.2	Justificación y directrices adicionales	68
8.3.3	Mejoras de los requisitos.....	68
8.3.4	Niveles de seguridad	69
8.4	SR 4.2 – Persistencia de la información.....	69

8.4.1	Requisito.....	69
8.4.2	Justificación y directrices adicionales	69
8.4.3	Mejoras de los requisitos.....	69
8.4.4	Niveles de seguridad	70
8.5	SR 4.3 – Uso de criptografía	70
8.5.1	Requisito.....	70
8.5.2	Justificación y directrices adicionales	70
8.5.3	Mejoras de los requisitos.....	70
8.5.4	Niveles de seguridad	71
9	FR 5 – Flujo de datos restringido	71
9.1	Propósito y descripciones del nivel de seguridad de capacidad SL-C(RDF)	71
9.2	Justificación	71
9.3	SR 5.1 – Segmentación de red.....	71
9.3.1	Requisito.....	71
9.3.2	Justificación y directrices adicionales	72
9.3.3	Mejoras de los requisitos.....	72
9.3.4	Niveles de seguridad	73
9.4	SR 5.2 – Protección de los límites de la zona	73
9.4.1	Requisito.....	73
9.4.2	Justificación y directrices adicionales	73
9.4.3	Mejoras de los requisitos.....	73
9.4.4	Niveles de seguridad	74
9.5	SR 5.3 – Restricciones de comunicación entre personas de propósito general.....	74
9.5.1	Requisito.....	74
9.5.2	Justificación y directrices adicionales	74
9.5.3	Mejoras de los requisitos.....	75
9.5.4	Niveles de seguridad	75
9.6	SR 5.4 – Partición de aplicaciones	75
9.6.1	Requisito.....	75
9.6.2	Justificación y directrices adicionales	75
9.6.3	Mejoras de los requisitos.....	76
9.6.4	Niveles de seguridad	76
10	FR 6 – Respuesta oportuna a los incidentes.....	76
10.1	Propósito y descripciones del nivel de seguridad de capacidad SL-C(TRE).....	76
10.2	Justificación	76
10.3	SR 6.1 – Accesibilidad de los registros de auditoría	77
10.3.1	Requisito.....	77
10.3.2	Justificación y directrices adicionales	77
10.3.3	Mejoras de los requisitos.....	77
10.3.4	Niveles de seguridad	77
10.4	SR 6.2 – Supervisión continua.....	77
10.4.1	Requisito.....	77
10.4.2	Justificación y directrices adicionales	78
10.4.3	Mejoras de los requisitos.....	78
10.4.4	Niveles de seguridad	78
11	FR 7 – Disponibilidad de recursos.....	78
11.1	Propósito y descripciones del nivel de seguridad de capacidad SL-C(RA).....	78
11.2	Justificación	79
11.3	SR 7.1 – Protección contra la denegación de servicio	79
11.3.1	Requisito.....	79

11.3.2	Justificación y directrices adicionales	79
11.3.3	Mejoras de los requisitos.....	79
11.3.4	Niveles de seguridad	80
11.4	SR 7.2 – Gestión de recursos	80
11.4.1	Requisito.....	80
11.4.2	Justificación y directrices adicionales	80
11.4.3	Mejoras de los requisitos.....	80
11.4.4	Niveles de seguridad	80
11.5	SR 7.3 – Copia de seguridad del sistema de control	81
11.5.1	Requisito.....	81
11.5.2	Justificación y directrices adicionales	81
11.5.3	Mejoras de los requisitos.....	81
11.5.4	Niveles de seguridad	81
11.6	SR 7.4 – Recuperación y reconstitución del sistema de control	81
11.6.1	Requisito.....	81
11.6.2	Justificación y directrices adicionales	82
11.6.3	Mejoras de los requisitos.....	82
11.6.4	Niveles de seguridad	82
11.7	SR 7.5 – Alimentación de emergencia	82
11.7.1	Requisito.....	82
11.7.2	Justificación y directrices adicionales	82
11.7.3	Mejoras de los requisitos.....	82
11.7.4	Niveles de seguridad	82
11.8	SR 7.6 – Ajustes de configuración de red y seguridad	83
11.8.1	Requisito.....	83
11.8.2	Justificación y directrices adicionales	83
11.8.3	Mejoras de los requisitos.....	83
11.8.4	Niveles de seguridad	83
11.9	SR 7.7 – Funcionalidad mínima	83
11.9.1	Requisito.....	83
11.9.2	Justificación y directrices adicionales	84
11.9.3	Mejoras de los requisitos.....	84
11.9.4	Niveles de seguridad	84
11.10	SR 7.8 – Inventario de componentes del sistema de control	84
11.10.1	Requisito.....	84
11.10.2	Justificación y directrices adicionales	84
11.10.3	Mejoras de los requisitos.....	84
11.10.4	Niveles de seguridad	84
Anexo A (Informativo) Información sobre el vector SL.....		86
Anexo B (Informativo) Asignación de requisitos del sistema (SR) y mejoras de los requisitos (RE) a los requisitos fundamentales (FR) de los niveles de seguridad 1-4.....		96
Bibliografía		101
Anexo ZA (Normativo) Otras normas internacionales citadas en esta norma con las referencias de las normas europeas correspondientes.....		103
Figura 1 – Estructura de la serie de Normas IEC 62443		17
Figura A.1 – Ejemplo de un proceso industrial de alto nivel con zonas y conductos		89

Figura A.2 – Ejemplo de una planta de fabricación de alto nivel con zonas y conductos	90
Figura A.3 – Esquema de la correlación entre el uso de los distintos tipos de niveles de seguridad.....	91
Tabla B.1 – Asignación de requisitos del sistema (SR) y mejoras de los requisitos (RE) a los requisitos fundamentales (FR) de los niveles de seguridad 1-4	96

1 Objeto y campo de aplicación

Esta parte de la serie de Normas IEC 62443 detalla los requisitos técnicos de un sistema de control (SR) asociados con los siete requisitos fundamentales (FR) descritos en la Norma IEC 62443-1-1, incluyendo la definición de los requisitos relativos a los niveles de seguridad de capacidad del sistema de control, SL-C(sistema de control). Estos requisitos estarían destinados a varios miembros de la comunidad de los sistemas de automatización y control industrial (IACS), así como a las zonas y los conductos definidos para el sistema en consideración (SuC) a la hora de desarrollar el nivel de seguridad objetivo adecuado del sistema de control, SL-T(sistema de control), para un activo específico.

Tal como se define en la Norma IEC 62443-1-1, hay un total de siete requisitos fundamentales (FR):

- a) control de identificación y autenticación (IAC),
- b) control de uso (UC),
- c) integridad del sistema (SI),
- d) confidencialidad de los datos (DC),
- e) flujo de datos restringido (RDF),
- f) respuesta oportuna a los eventos (TRE), y
- g) disponibilidad de recursos (RA).

Estos siete requisitos son la base para los SL de capacidad del sistema de control, SL-C(sistema de control). La definición de la capacidad de seguridad para el sistema de control es la meta y el objetivo de esta norma, a diferencia de los SL objetivos (SL-T) o los SL alcanzados (SL-A), que están fuera de su campo de aplicación

Véase la Norma IEC 62443-2-1 para consultar un conjunto equivalente de SR de capacidad no técnicos, relacionados con el programa, necesarios para alcanzar plenamente un SL objetivo del sistema de control.

2 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, solo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluida cualquier modificación de ésta).

IEC 62443-1-1:2009, *Industrial communication networks. Network and system security. Part 1-1: Terminology, concepts and models.*

IEC 62443-2-1, *Redes de comunicaciones industriales. Seguridad de la red y del sistema. Parte 2-1: Establecimiento de un programa de seguridad del sistema de control y automatización industrial.*