

Seguridad para los sistemas de automatización y control industrial

Parte 4-2: Requisitos técnicos de seguridad para componentes IACS

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 62443-4-2

UNE-EN IEC 62443-4-2

Seguridad para los sistemas de automatización y control industrial
Parte 4-2: Requisitos técnicos de seguridad para componentes IACS

Security for industrial automation and control systems. Part 4-2: Technical security requirements for IACS components.

Sécurité des systèmes d'automatisation et de commande industrielles. Partie 4-2: Exigences de sécurité technique des composants IACS.

Esta norma es la versión oficial, en español, de la Norma Europea EN IEC 62443-4-2:2019, que a su vez adopta la Norma Internacional IEC 62443-4-2:2019.

EXTRACTO DEL DOCUMENTO UNE-EN IEC 62443-4-2

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
Depósito legal: M 37013:2019

© UNE 2019

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	14
Declaración.....	14
Prólogo	15
Introducción.....	17
1 Objeto y campo de aplicación.....	20
2 Normas para consulta.....	20
3 Términos, definiciones, abreviaturas, acrónimos y convenciones	21
3.1 Términos y definiciones.....	21
3.2 Términos abreviados y acrónimos.....	27
3.3 Convenciones	30
4 Restricciones comunes relacionadas con la seguridad de los componentes.....	31
4.1 Visión de conjunto.....	31
4.2 CCSC 1: Admisión de funciones esenciales	31
4.3 CCSC 2: Contramedidas compensatorias.....	31
4.4 CCSC 3: Privilegio mínimo	31
4.5 CCSC 4: Proceso de desarrollo de software	32
5 FR 1 - Control de identificación y autenticación.....	32
5.1 Propósito y descripciones del SL-C(IAC).....	32
5.2 Justificación	32
5.3 CR 1.1 - Identificación y autenticación de usuarios humanos	33
5.3.1 Requisito.....	33
5.3.2 Justificación y directrices adicionales	33
5.3.3 Mejoras de los requisitos.....	33
5.3.4 Niveles de seguridad	34
5.4 CR 1.2 - Identificación y autenticación de procesos de software y dispositivos.....	34
5.4.1 Requisito.....	34
5.4.2 Justificación y directrices adicionales	34
5.4.3 Mejoras de los requisitos.....	35
5.4.4 Niveles de seguridad	35
5.5 CR 1.3 - Gestión de cuentas.....	35
5.5.1 Requisito.....	35
5.5.2 Justificación y directrices adicionales	35
5.5.3 Mejoras de los requisitos.....	35
5.5.4 Niveles de seguridad	35
5.6 CR 1.4 - Gestión de identificadores.....	36
5.6.1 Requisito.....	36
5.6.2 Justificación y directrices adicionales	36
5.6.3 Mejoras de los requisitos.....	36
5.6.4 Niveles de seguridad	36
5.7 CR 1.5 - Gestión de autenticadores.....	36
5.7.1 Requisito.....	36
5.7.2 Justificación y directrices adicionales	37
5.7.3 Mejoras de los requisitos.....	38
5.7.4 Niveles de seguridad	38
5.8 CR 1.6 - Gestión de acceso inalámbrico.....	38

5.9	CR 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	CR 1.8 – Certificados de infraestructura de clave pública	39
5.10.1	Requisito.....	39
5.10.2	Justificación y directrices adicionales	39
5.10.3	Mejoras de los requisitos.....	39
5.10.4	Niveles de seguridad	40
5.11	CR 1.9 – Fortaleza de la autenticación basada en clave pública	40
5.11.1	Requisito.....	40
5.11.2	Justificación y directrices adicionales	40
5.11.3	Mejoras de los requisitos.....	41
5.11.4	Niveles de seguridad	41
5.12	CR 1.10 – Retroalimentación del autenticador	41
5.12.1	Requisito.....	41
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	CR 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	CR 1.12 – Notificación 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	CR 1.13 – Acceso a través de redes que no son de confianza	44
5.16	CR 1.14 – Fortaleza de la autenticación basada en clave simétrica.....	44
5.16.1	Requisito.....	44
5.16.2	Justificación y directrices adicionales	45
5.16.3	Mejoras de los requisitos.....	45
5.16.4	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	CR 2.1 – Aplicación de la autorización	46
6.3.1	Requisito.....	46
6.3.3	Mejoras de los requisitos.....	47
6.3.4	Niveles de seguridad	47
6.4	CR 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	CR 2.3 – Control de uso para dispositivos portátiles y móviles	48
6.6	CR 2.4 – Código móvil	49
6.7	CR 2.5 – Bloqueo de sesión.....	49
6.7.1	Requisito.....	49
6.7.2	Justificación y directrices adicionales	49
6.7.3	Mejoras de los requisitos.....	49

6.7.4	Niveles de seguridad	49
6.8	CR 2.6 – Terminación de sesión remota	49
6.8.1	Requisito.....	49
6.8.2	Justificación y directrices adicionales	50
6.8.3	Mejoras de los requisitos.....	50
6.8.4	Niveles de seguridad	50
6.9	CR 2.7 – Control de sesiones simultáneas.....	50
6.9.1	Requisito.....	50
6.9.2	Justificación y directrices adicionales	50
6.9.3	Mejoras de los requisitos.....	50
6.9.4	Niveles de seguridad	50
6.10	CR 2.8 – Eventos auditables	51
6.10.1	Requisito.....	51
6.10.2	Justificación y directrices adicionales	51
6.10.3	Mejoras de los requisitos.....	51
6.10.4	Niveles de seguridad	51
6.11	CR 2.9 – Capacidad de almacenamiento de los datos de auditoría.....	52
6.11.1	Requisito.....	52
6.11.2	Justificación y directrices adicionales	52
6.11.3	Mejoras de los requisitos.....	52
6.11.4	Niveles de seguridad	52
6.12	CR 2.10 – Respuesta a los fallos de procesamiento de auditorías	53
6.12.1	Requisito.....	53
6.12.2	Justificación y directrices adicionales	53
6.12.3	Mejoras de los requisitos.....	53
6.12.4	Niveles de seguridad	53
6.13	CR 2.11 – Marcas de tiempo	53
6.13.1	Requisito.....	53
6.13.2	Justificación y directrices adicionales	54
6.13.3	Mejoras de los requisitos.....	54
6.13.4	Niveles de seguridad	54
6.14	CR 2.12 – No rechazo	54
6.14.1	Requisito.....	54
6.14.2	Justificación y directrices adicionales	54
6.14.3	Mejoras de los requisitos.....	55
6.14.4	Niveles de seguridad	55
6.15	CR 2.13 – Uso de interfaces físicas de diagnóstico y ensayo	55
7	FR 3 – Integridad del sistema.....	55
7.1	Propósito y descripciones del nivel de seguridad de capacidad SL-C(SI)	55
7.2	Justificación	56
7.3	CR 3.1 – Integridad de la comunicación.....	56
7.3.1	Requisito.....	56
7.3.2	Justificación y directrices adicionales	56
7.3.3	Mejoras de los requisitos.....	57
7.3.4	Niveles de seguridad	57
7.4	CR 3.2 – Protección contra código malicioso	57
7.5	CR 3.3 – Verificación de la funcionalidad de la seguridad	57
7.5.1	Requisito.....	57
7.5.2	Justificación y directrices adicionales	58
7.5.3	Mejoras de los requisitos.....	58
7.5.4	Niveles de seguridad	58
7.6	CR 3.4 – Integridad del software y de la información.....	59
7.6.1	Requisito.....	59
7.6.2	Justificación y directrices adicionales	59

7.6.3	Mejoras de los requisitos.....	59
7.6.4	Niveles de seguridad	59
7.7	CR 3.5 - Validación de entrada	59
7.7.1	Requisito.....	59
7.7.2	Justificación y directrices adicionales	60
7.7.3	Mejoras de los requisitos.....	60
7.7.4	Niveles de seguridad	60
7.8	CR 3.6 - Salida determinista	60
7.8.1	Requisito.....	60
7.8.2	Justificación y directrices adicionales	60
7.8.3	Mejoras de los requisitos.....	61
7.8.4	Niveles de seguridad	61
7.9	CR 3.7 - Tratamiento de errores.....	61
7.9.1	Requisito.....	61
7.9.2	Justificación y directrices adicionales	61
7.9.3	Mejoras de los requisitos.....	61
7.9.4	Niveles de seguridad	61
7.10	CR 3.8 - Integridad de la sesión.....	62
7.10.1	Requisito.....	62
7.10.2	Justificación y directrices adicionales	62
7.10.3	Mejoras de los requisitos.....	62
7.10.4	Niveles de seguridad	62
7.11	CR 3.9 - Protección de la información de auditoría.....	63
7.11.1	Requisito.....	63
7.11.2	Justificación y directrices adicionales	63
7.11.3	Mejoras de los requisitos.....	63
7.11.4	Niveles de seguridad	63
7.12	CR 3.10 - Soporte para actualizaciones.....	63
7.13	CR 3.11 - Resistencia a la manipulación física y mecanismos de detección	63
7.14	CR 3.12 - Provisión de raíces de confianza de los proveedores de productos	63
7.15	CR 3.13 - Provisión de raíces de confianza del propietario del activo	64
7.16	CR 3.14 - Integridad del proceso de arranque.....	64
8	FR 4 - Confidencialidad de los datos	64
8.1	Propósito y descripciones del SL-C(DC)	64
8.2	Justificación	64
8.3	CR 4.1 - Confidencialidad de la información	64
8.3.1	Requisito.....	64
8.3.2	Justificación y directrices adicionales	65
8.3.3	Mejoras de los requisitos.....	65
8.3.4	Niveles de seguridad	65
8.4	CR 4.2 - Persistencia de la información	65
8.4.1	Requisito.....	65
8.4.2	Justificación y directrices adicionales	65
8.4.3	Mejoras de los requisitos.....	66
8.4.4	Niveles de seguridad	66
8.5	CR 4.3 - Uso de criptografía	66
8.5.1	Requisito.....	66
8.5.2	Justificación y directrices adicionales	67
8.5.3	Mejoras de los requisitos.....	67
8.5.4	Niveles de seguridad	67
9	FR 5 - Flujo de datos restringido	67
9.1	Propósito y descripciones del SL-C(RDF)	67

9.2	Justificación	68
9.3	CR 5.1 – Segmentación de la red.....	68
9.3.1	Requisito.....	68
9.3.2	Justificación y directrices adicionales	68
9.3.3	Mejoras de los requisitos.....	69
9.3.4	Niveles de seguridad	69
9.4	CR 5.2 – Protección de los límites de zona.....	69
9.5	CR 5.3 – Restricciones de comunicación entre personas de carácter general.....	69
9.6	CR 5.4 – Partición de aplicaciones.....	69
10	FR 6 – Respuesta apropiada a los acontecimientos	69
10.1	Propósito y descripciones del SL-C(TRE).....	69
10.2	Justificación	70
10.3	CR 6.1 – Accesibilidad de los registros de auditoría	70
10.3.1	Requisito.....	70
10.3.2	Justificación y directrices adicionales	70
10.3.3	Mejoras de los requisitos.....	70
10.3.4	Niveles de seguridad	70
10.4	CR 6.2 – Supervisión continua.....	71
10.4.1	Requisito.....	71
10.4.2	Justificación y directrices adicionales	71
10.4.3	Mejoras de los requisitos.....	71
10.4.4	Niveles de seguridad	71
11	FR 7 – Disponibilidad de recursos.....	72
11.1	Propósito y descripciones del SL-C(RA).....	72
11.2	Justificación	72
11.3	CR 7.1 – Protección contra denegación de servicio.....	72
11.3.1	Requisito.....	72
11.3.2	Justificación y directrices adicionales	72
11.3.3	Mejoras de los requisitos.....	72
11.3.4	Niveles de seguridad	73
11.4	CR 7.2 – Gestión de recursos.....	73
11.4.1	Requisito.....	73
11.4.2	Justificación y directrices adicionales	73
11.4.3	Mejoras de los requisitos.....	73
11.4.4	Niveles de seguridad	73
11.5	CR 7.3 – Copia de seguridad del sistema de control.....	73
11.5.1	Requisito.....	73
11.5.2	Justificación y directrices adicionales	74
11.5.3	Mejoras de los requisitos.....	74
11.5.4	Niveles de seguridad	74
11.6	CR 7.4 – Recuperación y reconstitución del sistema de control.....	74
11.6.1	Requisito.....	74
11.6.2	Justificación y directrices adicionales	74
11.6.3	Mejoras de los requisitos.....	75
11.6.4	Niveles de seguridad	75
11.7	CR 7.5 – Alimentación de emergencia	75
11.8	CR 7.6 – Ajustes de configuración de red y seguridad.....	75
11.8.1	Requisito.....	75
11.8.2	Justificación y directrices adicionales	75
11.8.3	Mejoras de los requisitos.....	75
11.8.4	Niveles de seguridad	75
11.9	CR 7.7 – Funcionalidad mínima	76
11.9.1	Requisito.....	76

11.9.2	Justificación y directrices adicionales	76
11.9.3	Mejoras de los requisitos.....	76
11.9.4	Niveles de seguridad	76
11.10	CR 7.8 – Inventario de componentes del sistema de control	76
11.10.1	Requisito.....	76
11.10.2	Justificación y directrices adicionales	76
11.10.3	Mejoras de los requisitos.....	76
11.10.4	Niveles de seguridad	77
12	Requisitos para las aplicaciones de software	77
12.1	Propósito	77
12.2	SAR 2.4 – Código móvil.....	77
12.2.1	Requisito.....	77
12.2.2	Justificación y directrices adicionales	77
12.2.3	Mejoras de los requisitos.....	78
12.2.4	Niveles de seguridad	78
12.3	SAR 3.2 – Protección contra código malicioso	78
12.3.1	Requisito.....	78
12.3.2	Justificación y directrices adicionales	78
12.3.3	Mejoras de los requisitos.....	78
12.3.4	Niveles de seguridad	78
13	Requisitos de los dispositivos integrados	79
13.1	Propósito	79
13.2	EDR 2.4 – Código móvil	79
13.2.1	Requisito.....	79
13.2.2	Justificación y directrices adicionales	79
13.2.3	Mejoras de los requisitos.....	79
13.2.4	Niveles de seguridad	79
13.3	EDR 2.13 – Uso de interfaces físicas de diagnóstico y ensayo	80
13.3.1	Requisito.....	80
13.3.2	Justificación y directrices adicionales	80
13.3.3	Mejoras de los requisitos.....	80
13.3.4	Niveles de seguridad	80
13.4	EDR 3.2 – Protección contra código malicioso.....	80
13.4.1	Requisito.....	80
13.4.2	Justificación y directrices adicionales	81
13.4.3	Mejoras de los requisitos.....	81
13.4.4	Niveles de seguridad	81
13.5	EDR 3.10 – Soporte para actualizaciones.....	81
13.5.1	Requisito.....	81
13.5.2	Justificación y directrices adicionales	81
13.5.3	Mejoras de los requisitos.....	82
13.5.4	Niveles de seguridad	82
13.6	EDR 3.11 – Resistencia a la manipulación física y mecanismos de detección	82
13.6.1	Requisito.....	82
13.6.2	Justificación y directrices adicionales	82
13.6.3	Mejoras de los requisitos.....	82
13.6.4	Niveles de seguridad	83
13.7	EDR 3.12 – Provisión de raíces de confianza de los proveedores de productos	83
13.7.1	Requisito.....	83
13.7.2	Justificación y directrices adicionales	83
13.7.3	Mejoras de los requisitos.....	83
13.7.4	Niveles de seguridad	83

13.8	EDR 3.13 – Provisión de raíces de confianza del propietario del activo.....	84
13.8.1	Requisito.....	84
13.8.2	Justificación y directrices adicionales	84
13.8.3	Mejoras de los requisitos.....	84
13.8.4	Niveles de seguridad	85
13.9	EDR 3.14 – Integridad del proceso de arranque	85
13.9.1	Requisito.....	85
13.9.2	Justificación y directrices adicionales	85
13.9.3	Mejoras de los requisitos.....	85
13.9.4	Niveles de seguridad	85
14	Requisitos para los dispositivos host.....	86
14.1	Propósito	86
14.2	HDR 2.4 – Código móvil	86
14.2.1	Requisito.....	86
14.2.2	Justificación y directrices adicionales	86
14.2.3	Mejoras de los requisitos.....	86
14.2.4	Niveles de seguridad	86
14.3	HDR 2.13 – Uso de interfaces físicas de diagnóstico y ensayo.....	87
14.3.1	Requisito.....	87
14.3.2	Justificación y directrices adicionales	87
14.3.3	Mejoras de los requisitos.....	87
14.3.4	Niveles de seguridad	87
14.4	HDR 3.2 – Protección contra códigos maliciosos	88
14.4.1	Requisito.....	88
14.4.2	Justificación y directrices adicionales	88
14.4.3	Mejoras de los requisitos.....	88
14.4.4	Niveles de seguridad	88
14.5	HDR 3.10 – Soporte para actualizaciones	88
14.5.1	Requisito.....	88
14.5.2	Justificación y directrices adicionales	88
14.5.3	Mejoras de los requisitos.....	89
14.5.4	Niveles de seguridad	89
14.6	HDR 3.11 – Resistencia a la manipulación física y mecanismos de detección	89
14.6.1	Requisito.....	89
14.6.2	Justificación y directrices adicionales	89
14.6.3	Mejoras de los requisitos.....	89
14.6.4	Niveles de seguridad	90
14.7	HDR 3.12 – Provisión de raíces de confianza de los proveedores de productos	90
14.7.1	Requisito.....	90
14.7.2	Justificación y directrices adicionales	90
14.7.3	Mejoras de los requisitos.....	90
14.7.4	Niveles de seguridad	90
14.8	HDR 3.13 – Provisión de raíces de confianza del propietario del activo.....	91
14.8.1	Requisito.....	91
14.8.2	Justificación y directrices adicionales	91
14.8.3	Mejoras de los requisitos.....	91
14.8.4	Niveles de seguridad	92
14.9	HDR 3.14 – Integridad del proceso de arranque.....	92
14.9.1	Requisito.....	92
14.9.2	Justificación y directrices adicionales	92
14.9.3	Mejoras de los requisitos.....	92

14.9.4	Niveles de seguridad	92
15	Requisitos de los dispositivos de red	93
15.1	Propósito	93
15.2	NDR 1.6 – Gestión de acceso inalámbrico	93
15.2.1	Requisito.....	93
15.2.2	Justificación y directrices adicionales	93
15.2.3	Mejoras de los requisitos.....	93
15.2.4	Niveles de seguridad	93
15.3	NDR 1.13 – Acceso a través de redes que no son de no confianza.....	93
15.3.1	Requisito.....	93
15.3.2	Justificación y directrices adicionales	94
15.3.3	Mejoras de los requisitos.....	94
15.3.4	Niveles de seguridad	94
15.4	NDR 2.4 – Código móvil.....	94
15.4.1	Requisito.....	94
15.4.2	Justificación y directrices adicionales	95
15.4.3	Mejoras de los requisitos.....	95
15.4.4	Niveles de seguridad	95
15.5	NDR 2.13 – Uso de interfaces físicas de diagnóstico y ensayo.....	95
15.5.1	Requisito.....	95
15.5.2	Justificación y directrices adicionales	96
15.5.3	Mejoras de los requisitos.....	96
15.5.4	Niveles de seguridad	96
15.6	NDR 3.2 – Protección contra códigos maliciosos	96
15.6.1	Requisito.....	96
15.6.2	Justificación y directrices adicionales	96
15.6.3	Mejoras de los requisitos.....	97
15.6.4	Niveles de seguridad	97
15.7	NDR 3.10 – Soporte para actualizaciones	97
15.7.1	Requisito.....	97
15.7.2	Justificación y directrices adicionales	97
15.7.3	Mejoras de los requisitos.....	97
15.7.4	Niveles de seguridad	97
15.8	NDR 3.11 – Resistencia a la manipulación física y mecanismos de detección	98
15.8.1	Requisito.....	98
15.8.2	Justificación y directrices adicionales	98
15.8.3	Mejoras de los requisitos.....	98
15.8.4	Niveles de seguridad	98
15.9	NDR 3.12 – Provisión de raíces de confianza de los proveedores de productos	98
15.9.1	Requisito.....	98
15.9.2	Justificación y directrices adicionales	99
15.9.3	Mejoras de los requisitos.....	99
15.9.4	Niveles de seguridad	99
15.10	NDR 3.13 – Provisión de raíces de confianza del propietario del activo.....	99
15.10.1	Requisito.....	99
15.10.2	Justificación y directrices adicionales	100
15.10.3	Mejoras de los requisitos.....	100
15.10.4	Niveles de seguridad	100
15.11	NDR 3.14 – Integridad del proceso de arranque	101
15.11.1	Requisito.....	101
15.11.2	Justificación y directrices adicionales	101
15.11.3	Mejoras de los requisitos.....	101

15.11.4 Niveles de seguridad	101
15.12 NDR 5.2 – Protección de los límites de la zona	101
15.12.1 Requisito.....	101
15.12.2 Justificación y directrices adicionales	102
15.12.3 Mejoras de los requisitos.....	102
15.12.4 Niveles de seguridad	102
15.13 NDR 5.3 – Restricciones de comunicaciones entre personas de propósito general.....	103
15.13.1 Requisito.....	103
15.13.2 Justificación y directrices adicionales	103
15.13.3 Mejoras de los requisitos.....	103
15.13.4 Niveles de seguridad	103
Anexo A (Informativo) Categorías de dispositivos.....	104
A.1 Generalidades.....	104
A.2 Categoría de dispositivo: dispositivo integrado.....	104
A.2.1 Controlador lógico programable (PLC)	104
A.2.2 Dispositivo electrónico inteligente (IED)	105
A.3 Categoría de dispositivo: dispositivo de red	105
A.3.1 Conmutador.....	105
A.3.2 Terminador de red privada virtual (VPN).....	106
A.4 Categoría de dispositivo: dispositivo/aplicación host.....	106
A.4.1 Estaciones de trabajo del operador	106
A.4.2 Historiador de datos.....	107
Anexo B (Informativo) Asignación de requisitos de los componentes (CR) y mejoras de los requisitos (RE) a los requisitos fundamentales (FR) de niveles de seguridad SL 1-4.....	108
B.1 Visión de conjunto.....	108
B.2 Tabla de asignación de los niveles de seguridad (SL)	108
Bibliografía	114
Anexo ZA (Normativo) Otras normas internacionales citadas en esta norma con las referencias de las normas europeas correspondientes.....	116
Figura 1 – Partes de la serie de Normas IEC 62443.....	19
Tabla B.1 – Asignación de CR (requisitos del componente) y RE (mejoras de los requisitos) a los requisitos fundamentales (FR) de niveles de seguridad SL 1-4.....	109

1 Objeto y campo de aplicación

Esta parte de la Norma IEC 62443 indica los requisitos técnicos de los componentes (CR) detallados de un sistema de control asociados con los siete requisitos fundamentales (FR) descritos en la Especificación Técnica IEC TS 6-2443-1-1, incluida la definición de los requisitos relativos a los niveles de seguridad de capacidad del sistema de control y sus componentes, SL-C (componente).

Tal como se define en la Especificación Técnica IEC TS 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).

Estas siete FR son la base para definir los niveles de capacidad de seguridad de los sistemas de control. La definición de los niveles de capacidad de seguridad para el componente del sistema de control es la meta y el objetivo de este documento, a diferencia de los SL-T o los SL (SL-A) alcanzados, que están fuera del campo de aplicación.

NOTA 1 Véase la Norma IEC 62443-2-1 [1] para un conjunto equivalente de requisitos de capacidad no técnicos, relacionados con el programa, necesarios para lograr plenamente un SL-T (sistema de control).

NOTA 2 Las marcas y nombres comerciales mencionados en este documento se dan para la conveniencia de los usuarios de este documento. Esta información no constituye una aprobación por parte de la IEC de los productos mencionados.

2 Normas para consulta

En el texto se hace referencia a los siguientes documentos de manera que parte o la totalidad de su contenido constituyen requisitos 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 esta).

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

IEC 62443-3-3:2013, *Seguridad para los sistemas de automatización y control industrial. Parte 3-3: Requisitos de seguridad del sistema y niveles de seguridad.*

IEC 62443-4-1, *Seguridad para los sistemas de automatización y control industrial. Parte 4-1: Requisitos del ciclo de vida del desarrollo seguro del producto.*