

ICS 25.040

CCS N 10



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 42456-2023

**Security for industrial automation and control systems -
Technical security requirements for IACS components**

工业自动化和控制系统信息安全 IACS组件的安全技术要求

Issued on: March 17, 2023

Implemented on: October 1, 2023

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

1 Scope	1
2 Normative references	1
3 Terms, definitions, abbreviated terms and conventions	2
3.1 Terms and definitions	2
3.2 Abbreviated terms	7
3.3 Conventions	9
4 Common principles	10
4.1 Overview	10
4.2 CCSC 1: Support of basic functions	10
4.3 CCSC 2: Compensating countermeasures	10
4.4 CCSC 3: Least privilege	10
4.5 CCSC 4: Software development process	10
5 FR 1 - Identification and authentication control	10
5.1 Purpose and SL-C(IAC) description	10
5.2 Rationale	11
5.3 CR 1.1 - Human user identification and authentication	11
5.4 CR 1.2 - Software process and device identification and authentication	12
5.5 CR 1.3 - Account management	12
5.6 CR 1.4 - Identifier management	13
5.7 CR 1.5 - Authenticator management	14
5.8 CR 1.6 - Wireless access management	15
5.9 CR 1.7 - Strength of password-based authentication	15
5.10 CR 1.8 - Public key infrastructure (PKI) certificates	15
5.11 CR 1.9 - Strength of public key-based authentication	16
5.12 CR 1.10 - Authenticator feedback	17
5.13 CR 1.11 - Unsuccessful login attempts	17
5.14 CR 1.12 - System use notification	18
5.15 CR 1.13 - Access via untrusted networks	19
5.16 CR 1.14 - Strength of symmetric key-based authentication	19
6 FR 2 - Use control	20
6.1 Purpose and SL-C(UC) description	20
6.2 Rationale and supplemental guidance	20

6.3 CR 2.1 - Authorization enforcement	20
6.4 CR 2.2 - Wireless use control	21
6.5 CR 2.3 - Use control for portable and mobile devices	22
6.6 CR 2.4 - Mobile code	22
6.7 CR 2.5 - Session lock	22
6.8 CR 2.6 - Remote session termination	22
6.9 CR 2.7 - Concurrent session control	23
6.10 CR 2.8 - Auditable events	23
6.11 CR 2.9 - Audit storage capacity	24
6.12 CR 2.10 - Response to audit processing failures	25
6.13 CR 2.11 - Timestamps	25
6.14 CR 2.12 - Non-repudiation	26
6.15 CR 2.13 - Use of physical diagnostic and test interfaces	26
7 FR 3 - System integrity	26
7.1 Purpose and SL-C(SI) description	26
7.2 Basic principle	27
7.3 CR 3.1 - Communication integrity	27
7.4 CR 3.2 - Protection from malicious code	28
7.5 CR 3.3 - Security functionality verification	28
7.6 CR 3.4 - Software and information integrity	29
7.7 CR 3.5 - Input validation	29
7.8 CR 3.6 - Deterministic output	30
7.9 CR 3.7 - Error handling	30
7.10 CR 3.8 - Session integrity	31
7.11 CR 3.9 - Protection of audit information	32
7.12 CR 3.10 - Support for updates	32
7.13 CR 3.11 - Physical tamper resistance and detection	32
7.14 CR 3.12 - Provisioning product supplier roots of trust	32
7.15 CR 3.13 - Provisioning asset owner roots of trust	32
7.16 CR 3.14 - Integrity of the boot process	32
8 FR 4 - Data confidentiality	33
8.1 Purpose and SL-C(DC) description	33
8.2 Basic principle	33
8.3 CR 4.1 - Information confidentiality	33
8.4 CR 4.2 - Residual information	34

8.5 CR 4.3 - Use of cryptography	34
9 FR 5 - Restricted data flow	35
9.1 Purpose and SL-C(RDF) description	35
9.2 Basic principle	35
9.3 CR 5.1 - Network segmentation	35
9.4 CR 5.2 - Zone boundary protection	36
9.5 CR 5.3 - General purpose person-to-person communication restrictions	36
10 FR 6 - Timely response to events	36
10.1 Purpose and SL-C(TRE) description	36
10.2 Rationale and supplemental guidance	37
10.3 CR 6.1 - Audit log accessibility	37
10.4 CR 6.2 - Continuous monitoring	37
11 FR 7 - Resource availability	38
11.1 Purpose and SL-C(RA) description	38
11.2 Rationale	38
11.3 CR 7.1 - Denial of service protection	38
11.4 CR 7.2 - Resource management	39
11.5 CR 7.3 - Control system backup	39
11.6 CR 7.4 - Control system recovery and reconstitution	40
11.7 CR 7.5 - Emergency power	40
11.8 CR 7.6 - Network and security configuration settings	40
11.9 CR 7.7 - Least functionality	41
11.10 CR 7.8 - Control system component inventory	41
12 Software application requirements	42
12.1 Purpose	42
12.2 SAR 2.4 - Mobile code	42
12.3 SAR 3.2 - Protection from malicious code	43
13 Embedded device requirements	43
13.1 Purpose	43
13.2 EDR 2.4 - Mobile code	43
13.3 EDR 2.13 - Use of physical diagnostic and test interfaces	44
13.4 EDR 3.2 - Protection from malicious code	45
13.5 EDR 3.10 - Support for updates	45
13.6 EDR 3.11 - Physical tamper resistance and detection	46
13.7 EDR 3.12 - Provisioning product supplier roots of trust	46

13.8 EDR 3.13 - Provisioning asset owner roots of trust	47
13.9 EDR 3.14 - Integrity of the boot process	48
14 Host device requirements	48
14.1 Purpose	48
14.2 HDR 2.4 - Mobile code	48
14.3 HDR 2.13 - Use of physical diagnostic and test interfaces	49
14.4 HDR 3.2 - Protection from malicious code	50
14.5 HDR 3.10 - Support for updates	50
14.6 HDR 3.11 - Physical tamper resistance and detection	51
14.7 HDR 3.12 - Provisioning product supplier roots of trust	51
14.8 HDR 3.13 - Provisioning asset owner roots of trust	52
14.9 HDR 3.14 - Integrity of the boot process	53
15 Network device requirements	53
15.1 Purpose	53
15.2 NDR 1.6 - Wireless access management	54
15.3 NDR 1.13 - Access via untrusted networks	54
15.4 NDR 2.4 - Mobile code	55
15.5 NDR 2.13 - Use of physical diagnostic and test interfaces	56
15.6 NDR 3.2 - Protection from malicious code	56
15.7 NDR 3.10 - Support for updates	57
15.8 NDR 3.11 - Physical tamper resistance and detection	57
15.9 NDR 3.12 - Provisioning product supplier roots of trust	58
15.10 NDR 3.13 - Provisioning asset owner roots of trust	58
15.11 NDR 3.14 - Integrity of the boot process	59
15.12 NDR 5.2 - Zone boundary protection	60
15.13 NDR 5.3 - General purpose person-to-person communication restrictions	60
Annex A (informative) Device classification	62
A.1 Overview	62
A.2 Device classification: embedded devices	62
A.3 Device classification: network devices	63
A.4 Device classification: host devices and applications	63
Annex B (informative) Mapping of CRs and REs to FR SL 1 to 4	64
B.1 Overview	64
B.2 SL mapping tables	64
Bibliography	70