

CONTENTS

PREFACE	3
FOREWORD	10
0 Introduction	11
0.1 Overview.....	11
0.2 Purpose and intended audience	12
0.3 Usage within other parts of the ISA - 62443 series	12
1 Scope	15
2 Normative references	15
3 Terms, definitions, abbreviated terms, acronyms, and conventions	15
3.1 Terms and definitions.....	15
3.2 Abbreviated terms and acronyms	21
3.3 Conventions.....	23
4 Common control system security constraints	24
4.1 Overview.....	24
4.2 Support of essential functions	24
4.3 Compensating countermeasures	24
4.4 Least privilege	25
5 FR 1 – Identification and authentication control	25
5.1 Purpose and SL-C(IAC) descriptions.....	25
5.2 Rationale	25
5.3 SR 1.1 – Human user identification and authentication.....	25
5.4 SR 1.2 – Software process and device identification and authentication	27
5.5 SR 1.3 – Account management	28
5.6 SR 1.4 – Identifier management.....	28
5.7 SR 1.5 – Authenticator management	29
5.8 SR 1.6 – Wireless access management	30
5.9 SR 1.7 – Strength of password-based authentication	31
5.10 SR 1.8 – Public key infrastructure (PKI) certificates	32
5.11 SR 1.9 – Strength of public key authentication	33
5.12 SR 1.10 – Authenticator feedback	34
5.13 SR 1.11 – Unsuccessful login attempts	34
5.14 SR 1.12 – System use notification.....	35
5.15 SR 1.13 – Access via untrusted networks.....	35
6 FR 2 – Use control	36
6.1 Purpose and SL-C(UC) descriptions.....	36
6.2 Rationale	36
6.3 SR 2.1 – Authorization enforcement	37
6.4 SR 2.2 – Wireless use control	38
6.5 SR 2.3 – Use control for portable and mobile devices	39
6.6 SR 2.4 – Mobile code	39

6.7	SR 2.5 – Session lock	40
6.8	SR 2.6 – Remote session termination	40
6.9	SR 2.7 – Concurrent session control	41
6.10	SR 2.8 – Auditable events	41
6.11	SR 2.9 – Audit storage capacity	42
6.12	SR 2.10 – Response to audit processing failures	43
6.13	SR 2.11 – Timestamps	43
6.14	SR 2.12 – Non-repudiation	44
7	FR 3 – System integrity	45
7.1	Purpose and SL-C(SI) descriptions	45
7.2	Rationale	45
7.3	SR 3.1 – Communication integrity	45
7.4	SR 3.2 – Malicious code protection	46
7.5	SR 3.3 – Security functionality verification	47
7.6	SR 3.4 – Software and information integrity	48
7.7	SR 3.5 – Input validation	49
7.8	SR 3.6 – Deterministic output	49
7.9	SR 3.7 – Error handling	50
7.10	SR 3.8 – Session integrity	50
7.11	SR 3.9 – Protection of audit information	51
8	FR 4 – Data confidentiality	52
8.1	Purpose and SL-C(DC) descriptions	52
8.2	Rationale	52
8.3	SR 4.1 – Information confidentiality	52
8.4	SR 4.2 – Information persistence	53
8.5	SR 4.3 – Use of cryptography	54
9	FR 5 – Restricted data flow	55
9.1	Purpose and SL-C(RDF) descriptions	55
9.2	Rationale	55
9.3	SR 5.1 – Network segmentation	55
9.4	SR 5.2 – Zone boundary protection	56
9.5	SR 5.3 – General purpose person-to-person communication restrictions	57
9.6	SR 5.4 – Application partitioning	58
10	FR 6 – Timely response to events	58
10.1	Purpose and SL-C(TRE) descriptions	58
10.2	Rationale	59
10.3	SR 6.1 – Audit log accessibility	59
10.4	SR 6.2 – Continuous monitoring	59
11	FR 7 – Resource availability	60
11.1	Purpose and SL-C(RA) descriptions	60
11.2	Rationale	61
11.3	SR 7.1 – Denial of service protection	61
11.4	SR 7.2 – Resource management	61
11.5	SR 7.3 – Control system backup	62

11.6	SR 7.4 – Control system recovery and reconstitution	62
11.7	SR 7.5 – Emergency power	63
11.8	SR 7.6 – Network and security configuration settings	63
11.9	SR 7.7 – Least functionality	64
11.10	SR 7.8 – Control system component inventory	64
Annex A (informative) Discussion of the SL vector		67
A.1	Introduction.....	67
A.2	Security levels	67
A.3	SL vector	72
Annex B (informative) Mapping of SRs and REs to FR SL levels 1-4		75
B.1	Overview.....	75
B.2	SL mapping table	75
BIBLIOGRAPHY		80
Figure 1 – ISA-62443 Work Products		13
Figure A.1 – High-level process-industry example showing zones and conduits.....		69
Figure A.2 – High-level manufacturing example showing zones and conduits		70
Figure A.3 – Schematic of correlation of the use of different SL types		71
Table B.1 – Mapping of SRs and REs to FR SL levels 1-4		75