

CONTENTS

1	Scope	19
2	Normative references	19
3	Terms, definitions, abbreviated terms, acronyms, and conventions	19
3.1	Terms and definitions	19
3.2	Abbreviated terms and acronyms	24
3.3	Conventions	25
4	General principles	25
4.1	Concepts	25
4.2	Maturity model	26
5	Practice 1 – Security management	28
5.1	Purpose	28
5.2	SM-1: Development process	29
5.2.1	Requirement	29
5.2.2	Rationale and supplemental guidance	29
5.3	SM-2: Identification of responsibilities	29
5.3.1	Requirement	29
5.3.2	Rationale and supplemental guidance	29
5.4	SM-3: Identification of applicability	29
5.4.1	Requirement	29
5.4.2	Rationale and supplemental guidance	29
5.5	SM-4: Security expertise	30
5.5.1	Requirement	30
5.5.2	Rationale and supplemental guidance	30
5.6	SM-5: Process scoping	30
5.6.1	Requirement	30
5.6.2	Rationale and supplemental guidance	30
5.7	SM-6: File integrity	31
5.7.1	Requirement	31
5.7.2	Rationale and supplemental guidance	31
5.8	SM-7: Development environment security	31
5.8.1	Requirement	31
5.8.2	Rationale and supplemental guidance	31
5.9	SM-8: Controls for private keys	31
5.9.1	Requirement	31
5.9.2	Rationale and supplemental guidance	31
5.10	SM-9: Security requirements for externally provided components	31
5.10.1	Requirement	31
5.10.2	Rationale and supplemental guidance	32
5.11	SM-10: Custom developed components from third-party suppliers	32
5.11.1	Requirement	32
5.11.2	Rationale and supplemental guidance	33
5.12	SM-11: Assessing and addressing security-related issues	33

5.12.1	Requirement	33
5.12.2	Rationale and supplemental guidance	33
5.13	SM-12: Process verification.....	33
5.13.1	Requirement	33
5.13.2	Rationale and supplemental guidance	33
5.14	SM-13: Continuous improvement	33
5.14.1	Requirement	33
5.14.2	Rationale and supplemental guidance	33
6	Practice 2 – Specification of security requirements	34
6.1	Purpose	34
6.2	SR-1: Product security context.....	35
6.2.1	Requirement	35
6.2.2	Rationale and supplemental guidance	35
6.3	SR-2: Threat model.....	35
6.3.1	Requirement	35
6.3.2	Rationale and supplemental guidance	36
6.4	SR-3: Product security requirements	36
6.4.1	Requirement	36
6.4.2	Rationale and supplemental guidance	36
6.5	SR-4: Product security requirements content	37
6.5.1	Requirement	37
6.5.2	Rationale and supplemental guidance	37
6.6	SR-5: Security requirements review	37
6.6.1	Requirement	37
6.6.2	Rationale and supplemental guidance	37
7	Practice 3 – Secure by design.....	38
7.1	Purpose	38
7.2	SD-1: Secure design principles	38
7.2.1	Requirement	38
7.2.2	Rationale and supplemental guidance	38
7.3	SD-2: Defense in depth design.....	39
7.3.1	Requirement	39
7.3.2	Rationale and supplemental guidance	40
7.4	SD-3: Security design review	40
7.4.1	Requirement	40
7.4.2	Rationale and supplemental guidance	40
7.5	SD-4: Secure design best practices	40
7.5.1	Requirement	40
7.5.2	Rationale and supplemental guidance	41
8	Practice 4 – Secure implementation	41
8.1	Purpose	41
8.2	Applicability	41
8.3	SI-1: Security implementation review	41
8.3.1	Requirement	41

8.3.2	Rationale and supplemental guidance	42
8.4	SI-2: Secure coding standards	42
8.4.1	Requirement	42
8.4.2	Rationale and supplemental guidance	42
9	Practice 5 – Security verification and validation testing	42
9.1	Purpose	42
9.2	SVV-1: Security requirements testing	43
9.2.1	Requirement	43
9.2.2	Rationale and supplemental guidance	43
9.3	SVV-2: Threat mitigation testing	43
9.3.1	Requirement	43
9.3.2	Rationale and supplemental guidance	43
9.4	SVV-3: Vulnerability testing	44
9.4.1	Requirement	44
9.4.2	Rationale and supplemental guidance	44
9.5	SVV-4: Penetration testing	44
9.5.1	Requirement	44
9.5.2	Rationale and supplemental guidance	44
9.6	SVV-5: Independence of testers	45
9.6.1	Requirement	45
9.6.2	Rationale and supplemental guidance	45
10	Practice 6 – Management of security-related issues	46
10.1	Purpose	46
10.2	DM-1: Receiving notifications of security-related issues	46
10.2.1	Requirement	46
10.2.2	Rationale and supplemental guidance	46
10.3	DM-2: Reviewing security-related issues	46
10.3.1	Requirement	46
10.3.2	Rationale and supplemental guidance	47
10.4	DM-3: Assessing security-related issues	47
10.4.1	Requirement	47
10.4.2	Rationale and supplemental guidance	47
10.5	DM-4: Addressing security-related issues	48
10.5.1	Requirement	48
10.5.2	Rationale and supplemental guidance	48
10.6	DM-5: Disclosing security-related issues	49
10.6.1	Requirement	49
10.6.2	Rationale and supplemental guidance	49
10.7	DM-6: Periodic review of security defect management practice	50
10.7.1	Requirement	50
10.7.2	Rationale and supplemental guidance	50
11	Practice 7 – Security update management	50
11.1	Purpose	50
11.2	SUM-1: Security update qualification	50

11.2.1	Requirement	50
11.2.2	Rationale and supplemental guidance	50
11.3	SUM-2: Security update documentation	50
11.3.1	Requirement	50
11.3.2	Rationale and supplemental guidance	51
11.4	SUM-3: Dependent component or operating system security update documentation	51
11.4.1	Requirement	51
11.4.2	Rationale and supplemental guidance	51
11.5	SUM-4: Security update delivery	51
11.5.1	Requirement	51
11.5.2	Rationale and supplemental guidance	51
11.6	SUM-5: Timely delivery of security patches	52
11.6.1	Requirement	52
11.6.2	Rationale and supplemental guidance	52
12	Practice 8 – Security guidelines	52
12.1	Purpose	52
12.2	SG-1: Product defense in depth	52
12.2.1	Requirement	52
12.2.2	Rationale and supplemental guidance	53
12.3	SG-2: Defense in depth measures expected in the environment	53
12.3.1	Requirement	53
12.3.2	Rationale and supplemental guidance	53
12.4	SG-3: Security hardening guidelines	53
12.4.1	Requirement	53
12.4.2	Rationale and supplemental guidance	54
12.5	SG-4: Secure disposal guidelines	54
12.5.1	Requirement	54
12.5.2	Rationale and supplemental guidance	54
12.6	SG-5: Secure operation guidelines	54
12.6.1	Requirement	54
12.6.2	Rationale and supplemental guidance	55
12.7	SG-6: Account management guidelines	55
12.7.1	Requirement	55
12.7.2	Rationale and supplemental guidance	55
12.8	SG-7: Documentation review	55
12.8.1	Requirement	55
12.8.2	Rationale and supplemental guidance	55
Annex A	(informative) Possible metrics	57
Annex B	(informative) Table of requirements	59
Figure 1	– Parts of the ISA-62443 series	16
Figure 2	– Example scope of product life-cycle	17
Figure 3	– Defense in depth strategy is a key philosophy of the secure product life-cycle	26

Table 1 – Maturity levels	28
Table 2 – Example SDL continuous improvement activities.....	34
Table 3 – Required level of independence of testers from developers.....	45
Table B-1 – Summary of all requirements	59