IEC 62443-4-1

- 1 Scope
- 2 Normative references
- 3 Terms, definitions, abbreviated terms, acronyms and conventions
  - 3.1 Terms and definitions
  - 3.2 Abbreviated terms and acronyms
  - 3.3 Conventions
- 4 General principles
  - 4.1 Concepts
  - 4.2 Maturity model
- 5 Practice 1 – Security management
  - 5.1 Purpose
  - 5.2 SM-1: Development process
  - 5.3 SM-2: Identification of responsibilities
  - 5.4 SM-3: Identification of applicability
  - 5.5 SM-4: Security expertise
  - 5.6 SM-5: Process scoping
  - 5.7 SM-6: File integrity
  - 5.8 SM-7: Development environment security
  - 5.9 SM-8: Controls for private keys
  - 5.10 SM-9: Security requirements for externally provided components
  - 5.11 SM-10: Custom developed components from third-party suppliers
  - 5.12 SM-11: Assessing and addressing security-related issues
  - 5.13 SM-12: Process verification
  - 5.14 SM-13: Continuous improvement
- 6 Practice 2 – Specification of security requirements
  - 6.1 Purpose
  - 6.2 SR-1: Product security context
  - 6.3 SR-2: Threat model
  - 6.4 SR-3: Product security requirements
  - 6.5 SR-4: Product security requirements content
  - 6.6 SR-5: Security requirements review
- 7 Practice 3 – Secure by design
  - 7.1 Purpose
  - 7.2 SD-1: Secure design principles
  - 7.3 SD-2: Defense in depth design
  - 7.4 SD-3: Security design review
  - 7.5 SD-4: Secure design best practices
- 8 Practice 4 – Secure implementation
  - 8.1 Purpose
  - 8.2 Applicability
  - 8.3 SI-1: Security implementation review
  - 8.4 SI-2: Secure coding standards
- 9 Practice 5 – Security verification and validation testing
  - 9.1 Purpose
  - 9.2 SVV-1: Security requirements testing
  - 9.3 SVV-2: Threat mitigation testing
  - 9.4 SVV-3: Vulnerability testing
  - 9.5 SVV-4: Penetration testing
  - 9.6 SVV-5: Independence of testers
- 10 Practice 6 – Management of security-related issues
  - 10.1 Purpose
  - 10.2 DM-1: Receiving notifications of security-related issues
  - 10.3 DM-2: Reviewing security-related issues
  - 10.4 DM-3: Assessing security-related issues
  - 10.5 DM-4: Addressing security-related issues
  - 10.6 DM-5: Disclosing security-related issues
  - 10.7 DM-6: Periodic review of security defect management practice
- 11 Practice 7 – Security update management
  - 11.1 Purpose
  - 11.2 SUM-1: Security update qualification
  - 11.3 SUM-2: Security update documentation
  - 11.4 SUM-3: Dependent component or operating system security update documentation
  - 11.5 SUM-4: Security update delivery
  - 11.6 SUM-5: Timely delivery of security patches
- 12 Practice 8 – Security guidelines
  - 12.1 Purpose
  - 12.2 SG-1: Product defense in depth
  - 12.3 SG-2: Defense in depth measures expected in the environment
  - 12.4 SG-3: Security hardening guidelines
  - 12.5 SG-4: Secure disposal guidelines
  - 12.6 SG-5: Secure operation guidelines
  - 12.7 SG-6: Account management guidelines
  - 12.8 SG-7: Documentation review
- 13 Annexes
  - 13.1 Annex A (informative) Possible metrics
  - 13.2 Annex B (informative) Table of requirements