ISO 8102-20:2022-08 (E)

Electrical requirements for lifts, escalators and moving walks - Part 20: Cybersecurity

Contents

Page

Foreword v

Introduction vi

1 Scope 1

2 Normative references 2

3 Terms,definitionsandabbreviatedterms 2
3.1 Terms and definitions 2
3.2 Abbreviated terms 3

4 Secure development lifecycle for lifts, escalators and moving walks 3
4.1 General 3
4.2 Security management 4
4.2.1 Development process 4
4.2.2 Identification of responsibilities 4
4.2.3 Identification of applicability 4
4.2.4 Security expertise 4
4.2.5 Process scoping 4
4.2.6 File integrity 4
4.2.7 Development environment security 4
4.2.8 Controls for private keys 4
4.2.9 Security requirements for externally provided components 4
4.2.10 Custom developed components from third-party suppliers 4
4.2.11 Assessing and addressing security-related issues 5
4.2.12 Process verification 5
4.2.13 Continuous improvement 5
4.3 Specification of security requirements 5
4.3.1 Product security context 5
4.3.2 Threat model 5
4.3.3 Product security requirements 5
4.3.4 Product security requirements content 5
4.3.5 Security requirements review 5
4.4 Secure by design 5
4.4.1 Secure design principles 5
4.4.2 Defense in depth design 5
4.4.3 Security design review 5
4.4.4 Secure design best practices 5
4.5 Secure implementation 6
4.5.1 Security implementation review 6
4.5.2 Secure coding standards 6
4.6 Security verification and validation testing 6
4.6.1 Security requirements testing 6
4.6.2 Threat mitigation testing 6
4.6.3 Vulnerability testing 6
4.6.4 Penetration testing 6
4.6.5 Independence of testers 6
4.7 Management of security-related issues 6
4.7.1 Receiving notifications of security-related issues 6
4.7.2 Reviewing security-related issues 6
4.7.3 Assessing security-related issues 6

4.7.4 Addressing security-related issues 6
4.7.5 Disclosing security-related issues 7
4.7.6 Periodic review of security defect management practice 7
4.8 Security update management 7
4.8.1 Security update qualification 7
4.8.2 Security update documentation 7
4.8.3 Dependent component or operating system security update documentation 7
4.8.4 Security update delivery 7
4.8.5 Timely delivery of security patches 7
4.9 Security guidelines 7
4.9.1 Product defense in depth 7
4.9.2 Defense in depth measures expected in the environment 7
4.9.3 Security hardening guidelines 7
4.9.4 Secure disposal guidelines 8
4.9.5 Secure operation guidelines 8
4.9.6 Account management guidelines 8
4.9.7 Documentation review 8

5 Security requirements 8
5.1 General 8
5.2 Foundational requirements 8
5.3 Domains of the EUC functions 8
5.4 EUC security level requirements 10
5.5 Selection of security controls and countermeasures 10
5.6 Common security constraints 11
5.6.1 General 11
5.6.2 Support of essential functions 11
5.6.3 Compensating countermeasures 11
5.6.4 Least privilege 11
5.6.5 Software development process 11

6 Information for use 11

Annex A (informative) Additional information on secure development lifecycle for lifts, escalators and moving walks 13

Annex B (informative) Additional information on how to apply the general method of risk assessments 25

Annex C (informative) List of security practices 29

Annex D (informative) Guidance for application of zones and conduits 31

Bibliography 34