CONTENTS

PREFACE 3
CONTENTS 5
0 Introduction 9
1 Scope 11
2 References 11
3 Terms, definitions, abbreviated terms, acronyms, and conventions 11
3.1 Terms and definitions 11
3.2 Abbreviated terms and acronyms 11
4 Management of functional safety (Clause 5) 12
5 Hazard and risk analysis (Clause 8) 13
6 Allocation of safety functions to protection layers (Clause 9) 14
7 Safety requirements specification (SRS) for the safety instrumented system (Clauses 10 and 12) 15
8 Design and engineering of safety instrumented system (Clauses 11 and 12) 15
8.1 Independence and segregation 15
8.2 Access 16
8.3 Security concept 17
9 Design and development of other means of risk reduction (Clause 9) 17
10 Installation, commissioning and validation (Clauses 14 and 15) 18
10.1 Overview 18
10.2 Documentation 18
11 Operation and maintenance (Clause 16) 19
11.1 Security events 19
Any events associated with the SIS security countermeasures should be logged and continuously monitored. 19
11.2 Normal maintenance 19
11.3 Mechanical integrity 19
11.4 Inspection/Audit 19
11.5 Remote access 20
11.6 Bypasses 21
11.7 Tools 21
12 Modification (Clause 17) 21
13 Decommissioning (Clause 18) 22
Annex A (Informative) Example SIS interfaces to the enterprise network 25
A.1 Overview 25
A.2 Air-gapped 25
A.3 Interfaced 28
A.4 Integrated 2 zone 30
A.5 Integrated 1 zone 32
BIBLIOGRAPHY 34

Figure 1 – Graphical representation of the Safety Life Cycle 9
Figure A.1 – Example Network Security Architecture with Air-Gapped SIS..... 27
Figure A.2 – Example Network Security Architecture with Interfaced SIS 29
Figure A.3 – Example Network Security Architecture with Integrated 2 Zone SIS 31
Figure A.4 – Example Network Security Architecture with Integrated 1 Zone SIS 33