CONTENTS

UNITED STATES NATIONAL FOREWORD 11
IEC FOREWORD 11
INTRODUCTION 13
1 Scope 17
2 Normative references 17
3 ~~Terms,~~ Definitions and abbreviations 17
4 Conformance to this International Standard 18
5 Management of functional safety 18
5.1 Objective 18
5.2 Requirements 18
6 Safety lifecycle requirements 24
6.1 Objectives 24
6.2 Requirements 25
7 Verification 25
7.1 Objective 25
8 Process hazard and risk assessment 25
8.1 Objectives 25
8.2 Requirements 26
9 Allocation of safety functions to protection layers 29
9.1 Objective 29
9.2 Requirements of the allocation process 29
9.3 Additional requirements for safety integrity level 4 31
9.4 Requirement on the basic process control system as a layer of protection 32
9.5 Requirements for preventing common cause, common mode and dependent failures 33
10 SIS safety requirements specification 34
10.1 Objective 34
10.2 General requirements 34
10.3 SIS safety requirements 34
11 SIS design and engineering 35
11.1 Objective 35
11.2 General requirements 36
11.3 Requirements for system behaviour on detection of a fault 40
11.4 Requirements for hardware fault tolerance 40
11.5 Requirements for selection of components and subsystems 41
11.6 Field devices 43
11.7 Interfaces 44
11.8 Maintenance or testing design requirements 47
11.9 SIF probability of failure 48
12 Requirements for application software, including selection criteria for utility software 50
12.1 Application software safety lifecycle requirements 50
12.2 Application software safety requirements specification 53

Copyright 2004 ISA. All rights reserved.

12.3 Application software safety validation planning 55
12.4 Application software design and development 56
12.5 Integration of the application software with the SIS subsystem 63
12.6 FPL and LVL software modification procedures 63
12.7 Application software verification 64
13 Factory acceptance testing (FAT) 66
13.1 Objectives 66
13.2 Recommendations 66
14 SIS installation and commissioning 66
14.1 Objectives 66
14.2 Requirements 66
15 SIS safety validation 67
15.1 Objective 67
15.2 Requirements 67
16 SIS operation and maintenance 68
16.1 Objectives 68
16.2 Requirements 68
16.3 Proof testing and inspection 68
17 SIS modification 69
17.1 Objective 69
17.2 Requirements 70
18 SIS decommissioning 70
18.1 Objectives 70
18.2 Requirements 70
19 Information and documentation requirements 70
19.1 Objectives 70
19.2 Requirements 70
Annex A (informative) Example of techniques for calculating the probability of failure on demand for a safety instrumented function 73
A.1 General 73
A.2 Reliability block diagram technique 73
A.3 Simplified equations technique 73
A.4 Fault tree analysis technique 73
A.5 Markov modelling technique 73
Annex B (informative) Typical SIS architecture development 75
B.1 Background 75
B.2 Work process 75
B.3 Example 1 77
B.4 Example 2 79
Annex C (informative) Application features of a safety PLC 81
C.1 System 81
C.2 Work process 82

Copyright 2004 ISA. All rights reserved.

Annex D (informative) Example of SIS logic solver application software development methodology 83
D.1 Summary of the overall system integration process 83
D.2 SIS logic solver application development software 84
D.3 Coding standards for the application programmer 85
D.4 Other requirements for configuration/programming and run-time systems for safety applications 86
D.5 Assumptions 86
Annex E (informative) Example of development of externally configured diagnostics for a safety-configured PE logic solver 89
E.1 Internally configured diagnostics 89
E.2 Externally configured diagnostics 89
E.3 Reference 90

Figure 1 – Overall framework of this standard 15
Figure 2 – BPCS function and initiating cause independence illustration 32
Figure 3 – Software development lifecycle (the V-model) 51
Figure C.1 – Logic solver 82
Figure E.1 – EWDT timing diagram 91

Table 1 – Typical safety manual organisation and contents 61

Copyright 2004 ISA. All rights reserved.