CONTENTS

UNITED STATES NATIONAL FOREWORD 11
IEC FOREWORD 11
INTRODUCTION 13
1 Scope 16
2 Normative references 21
3 Abbreviations and definitions 22
3.1 Abbreviations 22
3.2 Definitions 23
4 Conformance to this International Standard 38
5 Management of functional safety 38
5.1 Objective 38
5.2 Requirements 38
6 Safety life-cycle requirements 43
6.1 Objectives 43
6.2 Requirements 43
7 Verification 45
7.1 Objective 45
8 Process hazard and risk assessment 46
8.1 Objectives 46
8.2 Requirements 46
9 Allocation of safety functions to protection layers 47
9.1 Objectives 47
9.2 Requirements of the allocation process 47
9.3 Additional requirements for safety integrity level 4 49
9.4 Requirements on the basic process control system as a protection layer 49
9.5 Requirements for preventing common cause, common mode and dependent failures 50
10 SIS safety requirements specification 51
10.1 Objective 51
10.2 General requirements 51
10.3 SIS safety requirements 51
11 SIS design and engineering 52
11.1 Objective 52
11.2 General requirements 52
11.3 Requirements for system behaviour on detection of a fault 54
11.4 Requirements for hardware fault tolerance 55
11.5 Requirements for selection of components and subsystems 56
11.6 Field devices 59
11.7 Interfaces 60
11.8 Maintenance or testing design requirements 62
11.9 SIF probability of failure 62
12 Requirements for application software, including selection criteria for utility software 63
12.1 Application software safety life-cycle requirements 64
12.2 Application software safety requirements specification 70

Copyright 2004 ISA. All rights reserved.

12.3 Application software safety validation planning 72
12.4 Application software design and development 72
12.5 Integration of the application software with the SIS subsystem 77
12.6 FPL and LVL software modification procedures 78
12.7 Application software verification 79
13 Factory acceptance testing (FAT) 80
13.1 Objectives 80
13.2 Recommendations 80
14 SIS installation and commissioning 81
14.1 Objectives 81
14.2 Requirements 81
15 SIS safety validation 82
15.1 Objective 82
15.2 Requirements 82
16 SIS operation and maintenance 85
16.1 Objectives 85
16.2 Requirements 85
16.3 Proof testing and inspection 87
17 SIS modification 87
17.1 Objectives 87
17.2 Requirements 88
18 SIS decommissioning 88
18.1 Objectives 88
18.2 Requirements 89
19 Information and documentation requirements 89
19.1 Objectives 89
19.2 Requirements 89
Annex A (informative) Differences 91
A.1 Organizational differences 91
A.2 Terminology 91

Figure 1 – Overall framework of this standard 15
Figure 2 – Relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) and IEC 61508 18
Figure 3 – Relationship between ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) and IEC 61508 (see 1.2) 19
Figure 4 – Relationship between safety instrumented functions and other functions 20
Figure 5 – Relationship between system, hardware, and software of ~~IEC 61511-1~~ ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) 21
Figure 6 – Programmable electronic system (PES): structure and terminology 31
Figure 7 – Example SIS architecture 34
Figure 8 – SIS safety life-cycle phases and functional safety assessment stages 41
Figure 9 – Typical risk reduction methods found in process plants 50
Figure 10 – Application software safety life cycle and its relationship to the SIS safety life cycle 64

Copyright 2004 ISA. All rights reserved.

Figure 11 – Application software safety life cycle (in realization phase) 66
Figure 12 – Software development life cycle (the V-model) 67
Figure 13 – Relationship between the hardware and software architectures of SIS 70

Table 1 – Abbreviations used in ~~IEC 61511~~ ANSI/ISA-84.00.01-2004 (IEC 61511 Mod) 22
Table 2 – SIS safety life-cycle overview 44
Table 3 – Safety integrity levels: probability of failure on demand 48
Table 4 – Safety integrity levels: frequency of dangerous failures of the SIF 48
Table 5 – Minimum hardware fault tolerance of PE logic solvers 55
Table 6 – Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers 56
Table 7 – Application software safety life cycle: overview 68

Copyright 2004 ISA. All rights reserved.