CONTENTS

1 Purpose 15
2 Introduction 15
3 Existing SIS 16
4 Overview 17
4.1 Life-cycle approach 18
4.2 Define a risk-management strategy 18
4.3 Implement the strategy 20
4.3.1 Independence 20
4.3.2 Programmable logic controllers (PLC) 21
4.3.3 User-approved devices 21
4.3.4 Response time 21
4.3.5 Support system considerations 21
4.3.6 Verification 22
4.3.7 Proof testing 22
4.4 Validate, startup, operate, and maintain the strategy 22
4.5 Manage changes to the strategy 24
5 Acronyms and abbreviations 25
Annex A Example Methods for Evaluating the Existing SIS 29
Annex B Alarms and Alerts from the SIS 35
Annex C Management of Functional Safety: Organization and Resources 45
Annex D Verification, Validation, and Functional Safety Assessments 51
Annex E Functional Safety Management System Audits 63
Annex F BPCS and its Relationship to the SIS 75
Annex G Failures – Types, Classifications, Sources and Strategy for Defense 85
Annex H SIF versus Interlocks, Permissives, and Inhibits 97
Annex I Continuous, High, and Low Demand Mode 103
Annex J SIL 4 versus Inherently Safer Design 111
Annex K Fault Tolerance Topics 113
Annex L Device Selection 119
Annex M General Purpose versus Safety Logic Solvers 139
Annex N Design Guidance 143
Annex O Application Programming 157
Annex P Response to Detection of a Dangerous Fault 161
Annex Q Instrumented Safeguard Setpoint Guidance 169
Annex R Key Performance Indicators 187
Annex S Safety Manual 191
Annex T References 195

Copyright 2020 ISA. All rights reserved.

Figures

Figure 1.1 – SIS safety lifecycle (modified ANSI/ISA-61511-1:2018 Figure 7) 8
Figure B.1 – Example of safety alarm system architecture 39
Figure B.2 – Safety alarm system for increasing process variable with operator action via HMI 42
Figure B.3 – Detail of safety alarm for increasing process variable and manual final control element 43
Figure D.1 – Relative cost of design changes as a function of project phase 53
Figure F.1 – Protection layers (ANSI/ISA-61511-1:2018, Figure 9) 77
Figure F.2 – Comparative risk reduction for shared field devices. Lower PFD values provide more risk reduction 84
Figure G.1 – Breakdown of failure classifications 87
Figure G.2 – Venn diagram of failure classifications 88
Figure G.3 – Venn diagram showing the probability of failure on demand for each failure classification 90
Figure G.4 – Venn diagram showing the probability of failure on demand for each failure classification 90
Figure G.5 – Primary cause of failure by lifecycle phase 92
Figure G.6 – Improving the overall quality, the configuration, and the availability of a safety protection layer can help to reduce systematic and random failures 94
Figure H.1 – Definition of safety instrumented system and safety instrumented function 100
Figure I.1 – Case 1 example graphic 107
Figure I.2 – Case 2 example graphic 108
Figure I.3 – Case 3 example graphic 108
Figure I.4 – Case 4 example graphic 109
Figure L.1 – Work process for selecting devices 123
Figure L.2 – Evidence supporting user approval 130
Figure Q.1 – IPL operating region with overall safety factor 171
Figure Q.2 – IPL response time with IPL safety factors 172
Figure Q.3. – Elements of sensor response time 173
Figure Q.4. – Elements of logic solver response time 174
Figure Q.5. – Elements of final control element response time with automatic actuation 175
Figure Q.6 – Result of not adjusting design for process lag 176
Figure Q.7 – Adjusting final element closure limit for process lag 177
Figure Q.8 – Adjusting final element closure limit for process lag and TSU 178
Figure Q.9 – Applying response time safety factor and determining MSP 179
Figure Q.10 – Setpoint specification relationships 180
Figure S.1 – Types of information forming safety manual content 191

Copyright 2020 ISA. All rights reserved.

Tables

Table 1-1– SIS Safety Life Cycle overview (modified ANSI/ISA-61511-1:2018 Table 2) 9
Table A.1 – Example of mapping prior design practice classification to SIL 32
Table C.1 — Example roles and responsibilities matrix 47
Table C.2 – Examples of experience or skills for the disciplines in Table C.1 49
Table D.1 – Purpose of relative timing of FSAs 53
Table E.1 – Functional safety audit focus topics and key input documents 65
Table E.2 – Example functional safety audit interview questions 67
Table G.1 – Key differences between random and systematic failures 86
Table J.1 – Checklist for evaluating feasibility of SIL 4 SIS 112
Table L.1 – Equipment approval form 134
Table N.1 – Fault types 147
Table N.2 – Diagnostic tests for programmable electronics 149
Table R.1 – Example indicators related to safety instrumented systems (SIS) 188

Copyright 2020 ISA. All rights reserved.