# TABLE OF CONTENTS

**LIST OF FIGURES**  
**LIST OF TABLES**  
**ABBREVIATIONS**  
**GLOSSARY**  
**ACKNOWLEDGEMENTS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PROCESS SAFETY AND SAFE AUTOMATION</td>
<td>1</td>
</tr>
<tr>
<td>1.1 OBJECTIVE</td>
<td>7</td>
</tr>
<tr>
<td>1.2 SCOPE</td>
<td>9</td>
</tr>
<tr>
<td>1.3 LIMITATIONS</td>
<td>9</td>
</tr>
<tr>
<td>1.4 TARGET AUDIENCE</td>
<td>11</td>
</tr>
<tr>
<td>1.5 INCIDENTS THAT DEFINE SAFE AUTOMATION</td>
<td>13</td>
</tr>
<tr>
<td>1.6 OVERVIEW OF THE CONTENTS</td>
<td>18</td>
</tr>
<tr>
<td>1.7 KEY DIFFERENCES</td>
<td>21</td>
</tr>
<tr>
<td>2 THE ROLE OF AUTOMATION IN PROCESS SAFETY</td>
<td>23</td>
</tr>
<tr>
<td>2.1 PROCESS OPERATIONS</td>
<td>23</td>
</tr>
<tr>
<td>2.2 PLANT AUTOMATION</td>
<td>33</td>
</tr>
<tr>
<td>2.3 A FRAMEWORK FOR PROCESS SAFETY</td>
<td>42</td>
</tr>
<tr>
<td>2.4 RISK-BASED DESIGN</td>
<td>54</td>
</tr>
<tr>
<td>2.5 RISK MANAGEMENT OF EXISTING FACILITY</td>
<td>78</td>
</tr>
<tr>
<td>3 AUTOMATION SPECIFICATION</td>
<td>83</td>
</tr>
<tr>
<td>3.1 PROCESS AUTOMATION LIFECYCLE</td>
<td>83</td>
</tr>
<tr>
<td>3.2 FUNCTIONAL SPECIFICATION</td>
<td>91</td>
</tr>
<tr>
<td>3.3 DESIGNING FOR OPERATING OBJECTIVES</td>
<td>92</td>
</tr>
<tr>
<td>3.4 INHERENTLY SAFER PRACTICES</td>
<td>104</td>
</tr>
<tr>
<td>3.5 DESIGNING FOR CORE ATTRIBUTES</td>
<td>107</td>
</tr>
<tr>
<td>3.6 CONTROL AND SAFETY SYSTEM INTEGRATION</td>
<td>133</td>
</tr>
<tr>
<td>4 DESIGN AND IMPLEMENTATION OF PROCESS CONTROL SYSTEMS</td>
<td>153</td>
</tr>
<tr>
<td>4.1 INPUT AND OUTPUT FIELD SIGNAL TYPES</td>
<td>161</td>
</tr>
<tr>
<td>4.2 BASIC APPLICATION PROGRAM FUNCTIONS</td>
<td>162</td>
</tr>
<tr>
<td>4.3 PROCESS CONTROL OBJECTIVES</td>
<td>165</td>
</tr>
<tr>
<td>4.4 PROCESS CONTROLLER TECHNOLOGY SELECTION</td>
<td>172</td>
</tr>
<tr>
<td>4.5 DETAILED APPLICATION PROGRAM DESIGN</td>
<td>194</td>
</tr>
<tr>
<td>5 DESIGN AND IMPLEMENTATION OF SAFETY CONTROLS, ALARMS, AND INTERLOCKS (SCAI)</td>
<td>211</td>
</tr>
<tr>
<td>5.1 SCAI CLASSIFICATION</td>
<td>215</td>
</tr>
<tr>
<td>5.2 DESIGN CONSIDERATIONS</td>
<td>220</td>
</tr>
<tr>
<td>5.3 SCAI TECHNOLOGY SELECTION</td>
<td>244</td>
</tr>
<tr>
<td>6 ADMINISTRATIVE CONTROLS AND MONITORING</td>
<td>265</td>
</tr>
<tr>
<td>6.1 INTRODUCTION</td>
<td>265</td>
</tr>
<tr>
<td>6.2 AUTOMATION ORGANIZATION MANAGEMENT</td>
<td>266</td>
</tr>
<tr>
<td>6.3 PROCESS SAFETY INFORMATION</td>
<td>269</td>
</tr>
<tr>
<td>6.4 OPERATING PROCEDURES</td>
<td>273</td>
</tr>
<tr>
<td>6.5 MAINTENANCE PLANNING</td>
<td>291</td>
</tr>
<tr>
<td>6.6 HUMAN AND SYSTEMATIC FAILURE MANAGEMENT</td>
<td>303</td>
</tr>
<tr>
<td>6.7 MANAGEMENT OF CHANGE</td>
<td>316</td>
</tr>
</tbody>
</table>

vii
6.8 AUDITING, MONITORING AND METRICS

APPENDIX A. CONTROL SYSTEM CONSIDERATIONS
A.1 CONTROL SYSTEM TECHNOLOGIES
A.2 ADDITIONAL CONSIDERATIONS FOR PROCESS CONTROL APPLICATIONS

APPENDIX B. POWER, GROUNDING, AND SHIELDING
B.1 POWER SUPPLY AND DISTRIBUTION
B.2 GROUNDING FOR SAFE, RELIABLE OPERATIONS
B.3 SIGNAL SHIELDING AND GROUNDING PRACTICES
B.4 SPECIAL SCAI CONSIDERATIONS

APPENDIX C. COMMUNICATIONS
C.1 COMMUNICATION CLASSIFICATIONS
C.2 COMMON COMMUNICATION NETWORK TOPOLOGIES
C.3 COMMUNICATION BETWEEN DEVICES
C.4 WIRELESS COMMUNICATION
C.5 COMMON COMMUNICATION CONFIGURATIONS
C.6 COMMON DATA COMMUNICATION ISSUES
C.7 PROCESS CONTROL AND SAFETY SYSTEM COMMUNICATIONS
C.8 SCAI COMMUNICATIONS

APPENDIX D. ALARM MANAGEMENT
D.1 ALARMS
D.2 STANDARDS AND RESOURCES
D.3 ALARM MANAGEMENT
D.4 MANAGING THE SAFETY ASPECTS OF ALARMS
D.5 ALARM SYSTEM PERFORMANCE BENCHMARKING
D.6 ALARM MANAGEMENT SOFTWARE

APPENDIX E. FIELD DEVICE CONSIDERATIONS
E.1 GENERAL SIGNAL SAFETY
E.2 FIELD DEVICE SELECTION
E.3 FLOW MEASUREMENT
E.4 PRESSURE MEASUREMENT
E.5 LEVEL MEASUREMENT
E.6 TEMPERATURE MEASUREMENT
E.7 ON-STREAM PROCESS ANALYSIS
E.8 AUTOMATED VALVES
E.9 ELECTRIC MOTORS
E.10 STEAM TURBINE VARIABLE SPEED DRIVES

APPENDIX F. SIS EQUIPMENT SELECTION
F.1 SELECTION BASIS
F.2 ADDITIONAL CONSIDERATIONS

APPENDIX G. HUMAN MACHINE INTERFACE DESIGN
G.1 GENERAL
G.2 OPERATOR INTERFACE STANDARDS AND RESOURCES
G.3 INSTRUMENT PANELS
G.4 CONFIGURABLE OPERATOR WORKSTATIONS
G.5 PROCESS ALARMS
G.6 SIS IMPACT ON HMI
<table>
<thead>
<tr>
<th>TABLE OF CONTENTS</th>
<th>ix</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.7 CONTROL-CENTER ENVIRONMENT</td>
<td>545</td>
</tr>
<tr>
<td>G.8 VIDEO</td>
<td>546</td>
</tr>
<tr>
<td>G.9 OPERATOR INTERFACES OF FUTURE</td>
<td>546</td>
</tr>
<tr>
<td>G.10 HMI CONSIDERATIONS CHECKLIST</td>
<td>547</td>
</tr>
<tr>
<td>APPENDIX H. APPLICATION PROGRAMMING</td>
<td>551</td>
</tr>
<tr>
<td>H.1 SOFTWARE TYPES</td>
<td>551</td>
</tr>
<tr>
<td>H.2 APPLICATION PROGRAM DEVELOPMENT</td>
<td>552</td>
</tr>
<tr>
<td>H.3 APPLICATION PROGRAMMING LANGUAGES</td>
<td>554</td>
</tr>
<tr>
<td>H.4 APPLICATION PROGRAM DEVELOPMENTAL MODELS</td>
<td>556</td>
</tr>
<tr>
<td>H.5 PROCESS CONTROL APPLICATION PROGRAM</td>
<td>557</td>
</tr>
<tr>
<td>H.6 SCAI APPLICATION PROGRAM</td>
<td>563</td>
</tr>
<tr>
<td>APPENDIX I. INSTRUMENT RELIABILITY PROGRAM</td>
<td>565</td>
</tr>
<tr>
<td>I.1 INTRODUCTION</td>
<td>565</td>
</tr>
<tr>
<td>I.2 TRACKING FAILURE</td>
<td>566</td>
</tr>
<tr>
<td>I.3 DATA TAXONOMY</td>
<td>568</td>
</tr>
<tr>
<td>I.4 DATA COLLECTION EFFORTS</td>
<td>569</td>
</tr>
<tr>
<td>I.5 FAILURE INVESTIGATION</td>
<td>571</td>
</tr>
<tr>
<td>I.6 CALCULATION OF FAILURE RATE</td>
<td>572</td>
</tr>
<tr>
<td>I.7 VERIFICATION</td>
<td>576</td>
</tr>
<tr>
<td>APPENDIX J. ACCEPTANCE TESTING GUIDELINES</td>
<td>581</td>
</tr>
<tr>
<td>J.1 ACCEPTANCE TESTING</td>
<td>581</td>
</tr>
<tr>
<td>J.2 STANDARDS</td>
<td>581</td>
</tr>
<tr>
<td>J.3 FACTORY ACCEPTANCE TEST</td>
<td>582</td>
</tr>
<tr>
<td>J.4 SITE ACCEPTANCE TEST (SAT)</td>
<td>589</td>
</tr>
<tr>
<td>INDEX</td>
<td>597</td>
</tr>
</tbody>
</table>