Guidelines for
Safe Automation
of Chemical Processes

INTER-
SCIENCE

CENTER FOR CHEMICAL PROCESS SAFETY
of the
AMERICAN INSTITUTE OF CHEMICAL ENGINEERS
345 East 47th Street, New York, New York 10017
This page intentionally left blank
Guidelines for Safe Automation of Chemical Processes
Publications Available from the CENTER FOR CHEMICAL PROCESS SAFETY of the AMERICAN INSTITUTE OF CHEMICAL ENGINEERS

Guidelines for Safe Automation of Chemical Processes
Guidelines for Engineering Design for Process Safety
Guidelines for Auditing Process Safety Management Systems
Guidelines for Investigating Chemical Process Incidents
Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples
Plant Guidelines for Technical Management of Chemical Process Safety
Guidelines for Technical Management of Chemical Process Safety
Guidelines for Chemical Process Quantitative Risk Analysis
Guidelines for Process Equipment Reliability Data, with Data Tables
Guidelines for Vapor Release Mitigation
Guidelines for Safe Storage and Handling of High Toxic Hazard Materials
Guidelines for Use of Vapor Cloud Dispersion Models
Workbook of Test Cases for Vapor Cloud Source Dispersion Models
Proceedings of the International Conference on Vapor Cloud Modeling, 1987
1991 CCPS/AICHE Directory of Chemical Process Safety Services
Audiotapes and Materials from Workshops at the International Conference on Chemical Process Safety Management, 1991
Electronic Chemical Process Quantitative Risk Analysis Bibliography
Guidelines for Safe Automation of Chemical Processes

INTER-SCIENCE

CENTER FOR CHEMICAL PROCESS SAFETY
of the
AMERICAN INSTITUTE OF CHEMICAL ENGINEERS
345 East 47th Street, New York, New York 10017
# CONTENTS

List of Figures .......................... ix
List of Tables ............................ xiii
Preface .................................. xv
Glossary .................................. xix
Acronyms ................................ xxiii

## 1. INTRODUCTION

1.0 Objective .......................... 1
1.1 Scope ................................ 1
1.2 Limitations ......................... 2
1.3 Overview of the Contents .......... 2

## 2. THE PLACE OF AUTOMATION IN CHEMICAL PLANT SAFETY. . .A DESIGN PHILOSOPHY

2.0 Chemical Plant Operations in Transition ........................................ 7
2.1 Plant Automation .......................... 9
2.2 A Framework for Chemical Process Safety ....................................... 13
2.3 Chemical Plant Safety System Development ..................................... 18
2.4 Safety System Design Philosophy .................................................. 33
2.5 References ................................ 35

## 3. TECHNIQUES FOR EVALUATING INTEGRITY OF PROCESS CONTROL SYSTEMS

3.0 Introduction .......................... 37
3.1 Safety and Integrity Evaluation Techniques ...................................... 44
3.2 Typical Process Hazard Review Activities and Outputs .................... 70
3.3 System Integrity Evaluation Criteria and Certification Methods .......... 72
3.4 Emerging Documents .................... 77
3.5 References ................................ 78
## 4. SAFETY CONSIDERATIONS IN THE SELECTION AND DESIGN OF BASIC PROCESS CONTROL SYSTEMS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0 Introduction</td>
<td>81</td>
</tr>
<tr>
<td>4.1 BPCS Technology Selection</td>
<td>86</td>
</tr>
<tr>
<td>4.2 Signals</td>
<td>90</td>
</tr>
<tr>
<td>4.3 Field Measurements</td>
<td>97</td>
</tr>
<tr>
<td>4.4 Final Control Elements</td>
<td>109</td>
</tr>
<tr>
<td>4.5 Process Controllers</td>
<td>118</td>
</tr>
<tr>
<td>4.6 Operator/Control System Interfaces</td>
<td>130</td>
</tr>
<tr>
<td>4.7 Communication Considerations in typical PES Architectures</td>
<td>148</td>
</tr>
<tr>
<td>4.8 Electrical Power Distribution Systems</td>
<td>151</td>
</tr>
<tr>
<td>4.9 Control-System Grounding for Personnel and Signal Protection</td>
<td>157</td>
</tr>
<tr>
<td>4.10 Batch Control with Regulatory and Discrete Control</td>
<td>163</td>
</tr>
<tr>
<td>4.11 Software Design and Data Structures</td>
<td>177</td>
</tr>
<tr>
<td>4.12 Advanced Computer-Control Strategies</td>
<td>188</td>
</tr>
<tr>
<td>4.13 Administrative Actions</td>
<td>191</td>
</tr>
<tr>
<td>4.14 References</td>
<td>193</td>
</tr>
</tbody>
</table>

## 5. SAFETY CONSIDERATIONS IN THE SELECTION AND DESIGN OF SAFETY INTERLOCK SYSTEMS (SISs)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0 Introduction</td>
<td>197</td>
</tr>
<tr>
<td>5.1 SIS Design Issues</td>
<td>200</td>
</tr>
<tr>
<td>5.2 Perform SIS Requirements Analysis</td>
<td>225</td>
</tr>
<tr>
<td>5.3 SIS Technology Selection</td>
<td>226</td>
</tr>
<tr>
<td>5.4 Select SIS Architecture</td>
<td>228</td>
</tr>
<tr>
<td>5.5 Select SIS Equipment</td>
<td>244</td>
</tr>
<tr>
<td>5.6 Perform SIS DESIGN</td>
<td>244</td>
</tr>
<tr>
<td>5.7 References</td>
<td>252</td>
</tr>
</tbody>
</table>

## 6. ADMINISTRATIVE ACTIONS TO ENSURE CONTROL SYSTEM INTEGRITY

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0 Introduction</td>
<td>255</td>
</tr>
<tr>
<td>6.1 Communication of Procedures</td>
<td>256</td>
</tr>
<tr>
<td>6.2 Maintenance Facilities Planning</td>
<td>270</td>
</tr>
<tr>
<td>6.3 Testing Bpcs Hardware And Software</td>
<td>276</td>
</tr>
<tr>
<td>6.4 SIS and Alarm Test Procedures</td>
<td>278</td>
</tr>
<tr>
<td>6.5 Testing Frequency Requirements</td>
<td>282</td>
</tr>
<tr>
<td>6.6 Installed Test Connections and Necessary Bypasses</td>
<td>284</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>6.7 Plant Operations Training with Installed Controls</td>
<td>284</td>
</tr>
<tr>
<td>6.8 Documentation of the BPCS and SIS</td>
<td>287</td>
</tr>
<tr>
<td>6.9 Audit Program to Keep Emphasis on BPCS/SIS Maintenance and</td>
<td>289</td>
</tr>
<tr>
<td>Documentation Activities</td>
<td></td>
</tr>
<tr>
<td>6.10 Simulation</td>
<td>290</td>
</tr>
<tr>
<td>6.11 Process Control Organization and Staffing</td>
<td>292</td>
</tr>
<tr>
<td>6.12 References</td>
<td>294</td>
</tr>
<tr>
<td>7.0 Introduction</td>
<td>295</td>
</tr>
<tr>
<td>7.1 Project Definition</td>
<td>296</td>
</tr>
<tr>
<td>7.2 Hazard Identification</td>
<td>299</td>
</tr>
<tr>
<td>7.3 Process Design Strategy</td>
<td>304</td>
</tr>
<tr>
<td>7.4 SIS Integrity Level Selection</td>
<td>309</td>
</tr>
<tr>
<td>7.5 Design of the BPCS</td>
<td>323</td>
</tr>
<tr>
<td>7.6 Risk Assessment and Control</td>
<td>326</td>
</tr>
<tr>
<td>7.7 Design And Validation of the SIS</td>
<td>328</td>
</tr>
<tr>
<td>7.8 Installation and Testing</td>
<td>330</td>
</tr>
<tr>
<td>7.9 Administrative Procedures to Maintain Integrity</td>
<td>332</td>
</tr>
<tr>
<td>7.10 Approach for Automation of an Existing Facility</td>
<td>335</td>
</tr>
<tr>
<td>7.11 References</td>
<td>335</td>
</tr>
<tr>
<td>8.0 Introduction</td>
<td>337</td>
</tr>
<tr>
<td>8.1 Governmental Regulations and Industry Initiatives</td>
<td>338</td>
</tr>
<tr>
<td>8.2 Management Expectations and Changing Workplace Factors</td>
<td>344</td>
</tr>
<tr>
<td>8.3 Measurement, Control, and Communication Technologies of the</td>
<td>347</td>
</tr>
<tr>
<td>1990s</td>
<td></td>
</tr>
<tr>
<td>8.4 Summary</td>
<td>363</td>
</tr>
<tr>
<td>8.5 References</td>
<td>363</td>
</tr>
<tr>
<td>Appendix A SIS TECHNOLOGIES</td>
<td>365</td>
</tr>
<tr>
<td>A.1 Pneumatic/Hydraulic</td>
<td>365</td>
</tr>
<tr>
<td>A.2 Electrical Logic Technology</td>
<td>365</td>
</tr>
<tr>
<td>A.3 PES Technology</td>
<td>370</td>
</tr>
<tr>
<td>A.4 Hybrid Systems</td>
<td>371</td>
</tr>
</tbody>
</table>
Appendix B SEPARATION 372

Appendix C TYPICAL WATCHDOG TIMER CIRCUITS 376

C.1 Internal Watchdog Timers 376
C.2 External Watchdog Timers 376

Appendix D COMMUNICATIONS 383

D.1 Common Communications Techniques 384
D.2 I/O Communications 385

Appendix E SENSOR FAIL-SAFE CONSIDERATIONS 387

Appendix F SIS EQUIPMENT SELECTION CONSIDERATIONS 389

F.1 Separation Application Guidelines 390
F.2 Diversity Application Guidelines 391
F.3 Software Application Matrix 392
F.4 Diagnostics Application Matrix 394
F.5 Communications Application Guidelines 394

Appendix G POTENTIAL PES FAILURE MODES 398

Appendix H FACTORY ACCEPTANCE TEST GUIDELINES 402

H.1 Purpose of the FAT 402
H.2 Participants in the FAT 402
H.3 Preparation for the FAT 403
H.4 General Procedure 403
H.5 Responsibilities 404
H.6 FAT Schedule 405
H.7 Documents 405
H.8 Test Equipment 406
H.9 Detailed Test Procedure 407
H.10 Equipment Acceptance 407
H.11 FAT Preparation Document 407

INDEX 409
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Typical control system including BPCS and SIS components</td>
<td>12</td>
</tr>
<tr>
<td>2.2</td>
<td>Layers of protection found in modern chemical processing plants</td>
<td>14</td>
</tr>
<tr>
<td>2.3</td>
<td>Major steps in the development of safe process designs</td>
<td>19</td>
</tr>
<tr>
<td>2.3.1</td>
<td>Process hazards definition</td>
<td>20</td>
</tr>
<tr>
<td>2.3.2</td>
<td>Hazards and risk assessment</td>
<td>22</td>
</tr>
<tr>
<td>2.3.3</td>
<td>Risk mitigation and control</td>
<td>24</td>
</tr>
<tr>
<td>2.3.4</td>
<td>System integrity validation</td>
<td>25</td>
</tr>
<tr>
<td>2.4</td>
<td>Process risk ranking model</td>
<td>26</td>
</tr>
<tr>
<td>2.5</td>
<td>Examples of SIS structures</td>
<td>28</td>
</tr>
<tr>
<td>2.6</td>
<td>Linkage of process risk to SIS integrity classifications.</td>
<td>30</td>
</tr>
<tr>
<td>2.7</td>
<td>Application of the SIS integrity classification methodology</td>
<td>31</td>
</tr>
<tr>
<td>3.1</td>
<td>Anatomy of an incident</td>
<td>38</td>
</tr>
<tr>
<td>3.2</td>
<td>Process hazards analysis team activities during the process life cycle.</td>
<td>39</td>
</tr>
<tr>
<td>3.3</td>
<td>Relationship of hazard analysis techniques to process life cycle.</td>
<td>41</td>
</tr>
<tr>
<td>3.4</td>
<td>Capability assessment example. Response of a plant and its proactive system (Ref 3.9)</td>
<td>54</td>
</tr>
<tr>
<td>3.5</td>
<td>Example of a fault tree</td>
<td>57</td>
</tr>
<tr>
<td>3.6</td>
<td>Example of an event tree</td>
<td>59</td>
</tr>
<tr>
<td>3.7</td>
<td>Example of a reliability block diagram.</td>
<td>61</td>
</tr>
<tr>
<td>3.8</td>
<td>Example of a risk profile. Total societal risk for an example fractionating system. (Ref. 3.3)</td>
<td>62</td>
</tr>
<tr>
<td>3.9</td>
<td>Example of a Markov model (Ref 3.20).</td>
<td>64</td>
</tr>
<tr>
<td>3.10</td>
<td>Sequence of steps in establishing SIS requirements.</td>
<td>69</td>
</tr>
<tr>
<td>4.1</td>
<td>Total control system includes basic process control system</td>
<td>82</td>
</tr>
<tr>
<td>4.2</td>
<td>A general BPCS design strategy</td>
<td>85</td>
</tr>
<tr>
<td>4.3</td>
<td>Comparison of (a) distributed control system (DCS) and (b) direct-digital-control system.</td>
<td>89</td>
</tr>
<tr>
<td>4.4</td>
<td>Block diagram of typical power distribution system for computers, analyzers, and miscellaneous instruments that do not require an uninterruptable power supply.</td>
<td>153</td>
</tr>
<tr>
<td>4.5</td>
<td>Block diagram of typical power distribution system for BPCS and SIS when an uninterruptable power supply is required.</td>
<td>156</td>
</tr>
</tbody>
</table>
Figure 4.6  Typical electrical grounding system for computers and miscellaneous instruments that do not require an uninterruptable power supply.  
Figure 4.7  Typical electrical grounding system for PESs and instruments that require an uninterruptable power supply.  
Figure 4.8  Typical instrument system signal shielding and grounding practices.  
Figure 4.9  Batch control activities.  
Figure 4.10  Relationship among levels.  
Figure 4.11  Manual operation.  
Figure 5.1  Relationship of other chapters to Chapter 5.  
Figure 5.2  Scope of coverage for SIS hardware/software.  
Figure 5.3  Scope of SIS design.  
Figure 5.4  Verify safety integrity.  
Figure 5.5  Redundancy possibilities in a SIS.  
Figure 5.6  Passive diagnostics.  
Figure 5.7  Active diagnosis.  
Figure 5.8  Double-block-and-bleed valves.  
Figure 5.9  Integrity Level 1 SIS structure and block diagram.  
Figure 5.10  Integrity Level 2 SIS structure and block diagram.  
Figure 5.11  Pressure sensor installation connection diversity.  
Figure 5.12  Integrity Level 3 SIS structure and block diagram.  
Figure 5.13  Logic diagram for Integrity Level 3 SIS with BPCS mirroring.  
Figure 5.14. A Passive diagnostic implementation of the SIS from Figure 5.12.  
Figure 5.15  Integrity Level 3 hybrid structure and block diagram.  
Figure 5.16  Dual solenoid method (series) to implement output redundancy.  
Figure 5.17  Dual solenoid method (parallel) to implement output redundancy.  
Figure 5.18  High logic solver reliability using TMR.  
Figure 5.19  High reliability SIS using quad-redundant processors.  
Figure 6.1  Typical information for functional test checklists.  
Figure 7.1  Simplified flow diagram: the PVC Process.  
Figure 7.2  Example of P&ID for PVC reactor unit.  
Figure 7.3  Linkage of process risk to SIS integrity classifications.  
Figure 7.4  Safety interlock system for the VCM reactor.  
Figure A.1  Direct-wired logic system. (a) Block diagram format. (b) Schematic diagram format.  
Figure A.2  Direct-wired logic interconnected with a BPCS (or SIS).  
Figure B.2  Separation—direct-wired connectivity.  
Figure B.1  Separation—no interconnectivity.
Figure B.3 Separation—serial communication (read/write). 373
Figure B.4 Separation—serial communication (read only). 373
Figure B.5 Separation—"soft" read only. 374
Figure B.6 Separation—SIS with embedded BPCS functions. 375
Figure C.1 Application program for use with the external WDT. 377
Figure C.2 Watchdog timer application program (square wave generator). 378
Figure C.3 WDT timing diagram. 379
Figure C.4 WDT schematic. 380
Figure C.5 Auxiliary schematics 381
Figure D.1 Local I/O. 383
Figure D.2 Remote I/O 384
Figure D.3 SIS–SIS or BCPS–BCPS communications 384
Figure D.4 Electromechanical logic to PES communications. 385
Figure E.1 Two types of ultrasonic point level switches 387
Figure F.1 Typical system architecture. 389
This page intentionally left blank
LIST OF TABLES

Table 2.1 SIS Interlock Design Structure for Each Integrity Level 28
Table 3.1 Failure Contributors to 17 Incidents Observed during the 4 Years of Operation in PES-Controlled Plants in the Netherlands 42
Table 3.2 Breakdown of Causes of the 17 Incidents (Ref. 3.1) 43
Table 4.1 A Checklist for the Operator Interface in the BPCS 147
Table 4.2 Possible Sources of Data Errors 184
Table 4.3 Levels of Data Access and Manipulation 188
Table 5.1 Logic Structures 201
Table 5.2 SIS Technology Selection Matrix 227
Table 5.3 SIS Technology Selection—Prescriptive Methodology 228
Table 7.1 Some Physical Properties of Vinyl Chloride 300
Table 7.2 Partial Summary of Preliminary Hazard Assessment Information for Development of Safety Interlock Strategy 308
Table 7.3 A Framework for System Risk/Evaluation/Documentation and SIS Integrity Level Selection 311
Table 7.4 VCM Reactor Example: Risk-Based SIS Integrity Level 314
Table 7.5 Sample HAZOP Sheet from PHA Team Review 327
Table F.1 Diversity Application Matrix for a Single SIS with Redundant Paths 392
Table F.2 Software Application Matrix 393
Table F.3 Diagnostics Application Matrix for a Single SIS with Redundant Paths 395
Table F.4 Communications Matrix 396
Table F.5 I/O Communication Application Matrix 397
Table H.1 Possible Testing Scenarios 404
This page intentionally left blank
PREFACE

The American Institute of Chemical Engineers (AIChE) has a 30-year history of involvement with process safety for chemical processing plants. Through its strong ties with process designers, builders, operators, safety professionals and academia, the AIChE has enhanced communication and fostered improvement in the high safety standards of the industry. AIChE publications and symposia have become an information resource for the chemical engineering profession on the causes of accidents and means of prevention.

The Center for Chemical Process Safety (CCPS) was established in 1985 by the AIChE to develop and disseminate technical information for use in the prevention of major chemical accidents. The CCPS is supported by a diverse group of industrial sponsors in the chemical process industry and related industries who provide the necessary funding and professional guidance for its projects. The CCPS Technical Steering Committee and the individual technical subcommittees overseeing individual projects are staffed by representatives of sponsoring companies. The first CCPS/AIChE project was the preparation of Guidelines for Hazard Evaluation Procedures. Since that time, a number of other Guidelines have been produced. One of the projects initiated in 1987 has led to the publication of this book, Guidelines for Safe Automation of Chemical Processes.

The chemical industry today is becoming increasingly automated with the advent of programmable electronic systems for measurement and control. While increased automation, including alarm systems, controls and interlocks, reduces the potential for operator error, new types of faults may occur in the automated control system. The complexity of computer-based instrumentation systems increases the potential for design and maintenance errors. To ensure a high level of safety, plant management, experienced operations personnel, process specialists, safety professionals and electrical/instrumentation/control design specialists must all collaborate intelligently and with a general knowledge of the key safety philosophies and issues. The goal of this book is to provide the designers and operators of chemical process facilities with a general philosophy and approach to the safe automation of chemical processes.

While these Guidelines for Safe Automation of Chemical Processes are intended for use by control system specialists, they also include important information on how control system design and operation is integrated with process design, safety evaluations and plant management. Further, we expect that those
primarily concerned with process design or with safety assessments will also gain from this book a better understanding of the strengths and pitfalls associated with chemical process automation. The engineer who needs a deeper understanding of the details of the discipline can consult the literature cited in the chapter references.

These Guidelines are a technical document intended for use by engineers and other persons familiar with the manufacture and use of chemicals. They are not a standard and make no attempt to cover the detailed legal requirements that apply to the construction and operation of chemical processing facilities. Meeting such requirements is a minimum basis for design and operation of all facilities and for satisfying general good practices reflected in industry and corporate standards. Over and above minimal compliance with safety regulations, each organization ultimately has the responsibility for developing its own safety philosophy and practices; thus, there are many alternate routes to achieving a high level of safety.

The CCPS Process Control Safety Subcommittee has co-authored these Guidelines, attempting to represent the spectrum of practices used by leading companies in the industry. The final draft of the book has been reviewed by CCPS sponsor organizations.

ACKNOWLEDGMENTS

The American Institute of Chemical Engineers (AIChE) wishes to thank the Center for Chemical Process Safety (CCPS) and those involved in its operation, including its many sponsors whose funding and technical support made this project possible. Particular thanks are due to the members of the CCPS Process Control Subcommittee who collaborated to write this book. Their dedicated efforts, technical contributions and guidance in the preparation of this book are sincerely appreciated.

The members of the Process Control Safety Subcommittee are:

Thomas G. Lagana, CHAIR, Hercules Incorporated
Suzanne M. Kleinhaus, VICE-CHAIR, Merck and Company
Elio A. Comello, Esso Chemical Canada/Exxon Chemical Company
Thomas G. Fisher, The Lubrizol Corporation
Dallas L. Green, Rohm and Haas Company
Charles D. Hardin, Hoechst Celanese Chemical Group
Victor J. Maggioli, E. I. du Pont de Nemours and Company (retired)
Richard F. Palas, Amoco Corporation
Clark Thurston, Union Carbide Chemicals and Plastics Company, Inc.
Stanley Weiner, Monsanto Chemical Company (retired)
Former members were:

Lynn W. Craig,  *Rohm and Haas Company*

Richard J. Lasher,  *Exxon Chemicals USA*

Ronnie L. Powell,  *Union Carbide Corporation*

Chris Smith,  *PAST CHAIR, Rhône Poulenc Company*

Thomas W. Carmody, Edward L. Mullen and Elisabeth M. Drake (who also participated in the writing) of the AIChE/CCPS staff were responsible for the overall administration and coordination of this project.

The members of the CCPS Process Control Safety Subcommittee wish to thank their employers for providing time and support to participate in this project. Also, we thank many colleagues for their assistance as well as all those CCPS sponsors and members of the Technical Steering Committee who reviewed and critiqued this book prior to publication. Special thanks are due to the Du Pont Board for Process Control, to the Du Pont Technical editing team of R. J. Gardner, R. P. Grehofsky, W. H. Johnson Jr., C. G. Langford, and to Phyllis J. Drupieski who prepared the corrected final manuscript.

Russell H. Till managed production and design of the book.
GLOSSARY

ALPHA-TEST  The first functional test of a device or system.

AUDIT (PROCESS SAFETY AUDIT)  An inspection of plant/process unit, drawings, procedures, emergency plan, and/or management systems to verify compliance with safety standards.

AVAILABILITY  The probability that a system will be able to perform its designated function when required for use (e.g., that an IPL performs its protection function when a demand is placed on the IPL). Another term frequently used is Probability of Failure on Demand (PFD).

Availability = 1 - PFD.

BASIC PROCESS CONTROL SYSTEM (BPCS)  The control equipment and system which is installed to regulate normal production functions.

BPCS CONTROLLER  A controller dedicated to performing BPCS functions.

BETA-TEST  A device or system test comprising production components that have satisfactorily passed an alpha-test. The scale of the test is such that the equipment is installed in an operating environment and its operation is monitored to determine performance against expectations.

CHEMICAL PROCESS QUANTITATIVE RISK ANALYSIS (CPQRA)  The process of hazard identification followed by numerical evaluation of incident consequences and frequencies, and their combination into an overall measure of risk when applied to the chemical process industry.

COMMON MODE FAILURE  A single failure that directly affects multiple systems in ways that are not consequences of each other.

COMMON CAUSE FAILURE  A single condition (e.g., corrosive environment) that slowly degrades multiple systems in ways that may eventually lead to failures.

CONFIGURATION  (1) Interconnected equipment forming a system. (2) Application programming using vendor-embedded software.

DEMAND  A condition or event that requires a protective system or device to take appropriate action to prevent or mitigate a hazard.

DIAGNOSTIC PROGRAM  A troubleshooting program for identifying hardware or software malfunctions.

DIVERSITY  A number of independent and different means to perform the same overall protective function.

EMERGENCY SHUTDOWN SYSTEM  A term that is being superseded by Safety Interlock System.
FAIL-SAFE A concept that defines the failure direction of a component/system as a result of specific malfunctions. The failure direction is toward a safer or less hazardous condition.

FAIL-TO-DANGER An equipment fault which inhibits or delays actions to achieve a safe operational state should a demand occur. The fail-to-danger fault has a direct and detrimental effect on safety.

FAULT TOLERANCE That property of a system which permits it to carry out its assigned function in the presence of one or more faults in the hardware or software.

FINAL CONTROL ELEMENT A device that manipulates a process variable to achieve control.

HAZARD A chemical or physical condition that has the potential for causing damage to people, property, or the environment.

HUMAN ERROR Mistakes by people, such as designers, engineers, operators, maintenance personnel, or managers that may contribute to or result in undesired events.

HUMAN/MACHINE INTERFACE (HMI) The operators’ windows to monitoring and keys, knobs, switches, etc. for making adjustments in the process.

INDEPENDENT PROTECTION LAYER (IPL) A system or subsystem specifically designed to reduce the likelihood or severity of the impact of an identified hazardous event by a large factor, i.e. at least by a 100 fold reduction in likelihood. An IPL must be independent of other protection layers associated with the identified hazardous event, as well as dependable, and auditable. (See Section 2.2.2.)

INTEGRITY LEVEL An indicator of SIS performance as measured by PFD (i.e., 1 - availability). (See Section 2.3.4.2.)

INTERLOCK SYSTEM A system that, in response to a predetermined condition, initiates or prevents a predefined action.

LOGIC SOLVER The portion of the SIS that performs the logic function (electromechanical relays, the CPU of a PES, etc.).

MAN/MACHINE INTERFACE (MMI) See Human/Machine Interface.

MITIGATION SYSTEM A system designed to respond to a hazardous event sequence by reducing its impact consequences.

OPERATOR'S WORKSTATION A device that allows the operator to communicate with the PES. It can be used to enter information, to request and display stored data, to actuate various preprogrammed command routines, etc. (See HMI).

PROBABILITY OF FAILURE ON DEMAND (PFD) See Integrity Level.

PROCESS HAZARDS ANALYSIS TEAM (PHA team) The group of operational, process, instrument/electrical/control, and safety specialists who are responsible for the safety and integrity evaluation of the process from its inception through its implementation and transfer to plant operations, to meet corporate safety guidelines.
PROGRAMMABLE ELECTRONIC SYSTEM (PES) A computer-based system connected to sensors and final control elements for the purpose of control, protection, or monitoring.

PROGRAMMABLE ELECTRONIC SYSTEM (PES) CONTROLLER A distributed control system controller, PLC system controller, single loop controller, etc.

PROGRAMMABLE LOGIC CONTROLLER (PLC) A computer, hardened for an industrial environment, for implementing specific functions such as logic, sequencing, timing, counting, and control. Although these are more commonly called Programmable Controllers, the acronym PLC is used in this book because PC is more commonly used in referring to a personal computer.

PROTECTION LAYER (PL) Protection layers typically involve special process designs, process equipment, administrative procedures, the basic process control system (BPCS) and/or planned responses to imminent adverse process conditions; and these responses may be either automated or initiated by human actions.

QUALITATIVE METHODS Methods of design and evaluation developed through experience.

QUANTITATIVE METHODS Methods of design and evaluation based on theory and mathematical analysis.

REDUNDANCY The employment of two or more devices, each performing the same function, in order to improve reliability.

RELIABILITY Probability that a component or system will function correctly under stated conditions for a stated period of time (for an IPL, it is reflected in the impact of spurious shutdowns; for a BPCS, it is reflected in the mean successful operating period).

RISK A measure of potential human injury, environmental damage, or economic loss in terms of both incident likelihood and the magnitude of the consequent potential injury, damage, or loss.

RISK ANALYSIS The development of a risk estimate based on engineering evaluation, and mathematical techniques for combining estimates of incident consequences and frequencies.

RISK ASSESSMENT The process of making risk estimates and using the results to make decisions.

SAFETY INTERLOCK SYSTEM (SIS) An instrumented IPL whose purpose is to take the process to a safe state when predetermined conditions are violated.

SAFETY INTERLOCK SYSTEM CONTROLLER A controller dedicated to performing SIS functions.

SAFETY LAYER See Independent Protection Layer.

SAFETY REQUIREMENT SPECIFICATION The SRS is a compilation of information found in the PHA report, logic diagram, process technology docu-
ments, P&ID, etc., including both functional requirements and safety integrity requirements.

**SEPARATION**  The physical and functional isolation of all hardware and software elements. Physical separation is defined as the requirement that the basic process control function (regulatory control—BPCS) and the safety interlock function (SIS) be performed in different logic solvers. Functional separation is achieved through the elimination of common-mode failures in execution of the BPCS and the SIS functions. This may require the separation of BPCS and SIS sensors, final elements, I/O components, the logic solvers, the software operating systems, and the application programs. Some communication may be allowed between separate components and systems as long as no common mode failures can occur. (See Appendix B)

**SOFTWARE LIFE CYCLE**  The activities occurring during a period of time that starts when the software is conceived and ends when the software is no longer supportable for use. The software life cycle typically includes a requirements phase, development phase, test phase, integration phase, installation phase, and a maintenance phase. (See IEC/TC 65A: Software for computers in the application of industrial safety-related systems.)

**SUPERVISORY CONTROL COMPUTER**  A computer, with HMI display and input devices, designed for accepting BPCS status inputs and either reporting data to the operator for process manipulation or indirectly regulating the process by manipulating setpoints in the BPCS. Process computer applications realize advanced levels of control, such as economic optimization, constraint control, model-based control, override control, multivariable control, statistical process control, etc.

**USER-APPROVED (UA)**  Refers to PES equipment status. (See Section 3.3.2.1).

**USER-APPROVED SAFETY (UAS)**  Refers to PES equipment status. (See Section 3.3.2.2).

**VIDEO DISPLAY UNIT (VDU)**  Any of several types of HMI that use video technology.

**WATCH DOG TIMER (WDT)**  A timer implemented to prevent the system from looping endlessly, providing inaccurate communications, or becoming idle because of program errors or equipment faults.
ACRONYMS

AIChE American Institute of Chemical Engineers
API American Petroleum Institute
ASME American Society of Mechanical Engineers
BPCS Basic Process Control System
CSA Canadian Standards Association
CCPS Center for Chemical Process Safety
CMA Chemical Manufacturers Association (U.S.)
CPI Chemical Process Industry
CPU Central Processing Unit
CPQRA Chemical Process Quantitive Risk Analysis
DCS Distributed Control System
DCSC Distributed Control System Controller
DDC Direct Digital Control
DIN Deutsches Institut für Normung e.V. (The Standards Institution of Germany)
EMI Electromagnetic Interference
ESD Emergency Shutdown (see SIS)
ETA Event Tree Analysis
FAT Factory Acceptance Test
FDT Fractional Dead Time (see PFD)
FM Factory Mutual, Inc. (U.S.)
FMEA Failure Modes and Effects Analysis
FMECA Failure Modes Effect and Criticality Analysis
FSSL Fail-Safe Solid State Logic
FTA Fault Tree Analysis
HAZOP Hazard and Operability Study
HMI Human/Machine Interface
HSE Health & Safety Executive (U.K.)
IEC International Electrotechnical Commission (Switzerland)
IEEE Institute of Electrical and Electronic Engineers (U.S.)
I/O Input/Output
IPL Independent Protection Layer
ISA Instrument Society of America
ISO International Organization for Standardization (Switzerland)
LAN Local Area Network
LEL Lower Explosion Limit
MMI Man/Machine Interface (see HMI)
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTBF</td>
<td>Mean Time between Failures</td>
</tr>
<tr>
<td>MTDF</td>
<td>Mean Time to Detect Failure</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time to Failure</td>
</tr>
<tr>
<td>MTTR</td>
<td>Mean Time to Repair</td>
</tr>
<tr>
<td>NDFIT</td>
<td>Nondestructive Fault Insertion Testing</td>
</tr>
<tr>
<td>NEC</td>
<td>National Electric Code (U.S.)</td>
</tr>
<tr>
<td>NEMA</td>
<td>National Electrical Manufacturers' Association (U.S.)</td>
</tr>
<tr>
<td>NFPA</td>
<td>National Fire Protection Association, Inc. (U.S.)</td>
</tr>
<tr>
<td>OSHA</td>
<td>Occupational Safety and Health Administration (U.S.)</td>
</tr>
<tr>
<td>PES</td>
<td>Programmable Electronic System</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of Failure on Demand</td>
</tr>
<tr>
<td>PHA</td>
<td>Process Hazard Analysis</td>
</tr>
<tr>
<td>PI</td>
<td>Proportional-Integral</td>
</tr>
<tr>
<td>PID</td>
<td>Proportional-Integral-Derivative</td>
</tr>
<tr>
<td>P&amp;ID</td>
<td>Piping and Instrumentation Diagram</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>QRA</td>
<td>Quantitative Risk Assessment</td>
</tr>
<tr>
<td>RBD</td>
<td>Reliability Block Diagram</td>
</tr>
<tr>
<td>RFI</td>
<td>Radiofrequency Interference</td>
</tr>
<tr>
<td>RTD</td>
<td>Resistance-Temperature-Detectors</td>
</tr>
<tr>
<td>SIS</td>
<td>Safety Interlock System</td>
</tr>
<tr>
<td>SRS</td>
<td>Safety Requirements Specification</td>
</tr>
<tr>
<td>SSSC</td>
<td>Single Station Digital Controller</td>
</tr>
<tr>
<td>SLC</td>
<td>Single Loop Controller</td>
</tr>
<tr>
<td>TÜV</td>
<td>Technischer Überwachungs-Verein e.V. (Technical Inspection Association of Germany)</td>
</tr>
<tr>
<td>UA</td>
<td>User Approved</td>
</tr>
<tr>
<td>UAS</td>
<td>User Approved Safety</td>
</tr>
<tr>
<td>UL</td>
<td>Underwriters Laboratory, Inc. (U.S.)</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>VDU</td>
<td>Video Display Unit</td>
</tr>
<tr>
<td>WDT</td>
<td>Watchdog Timer</td>
</tr>
</tbody>
</table>
1

INTRODUCTION

1.0 OBJECTIVE

The preparation of this document was sponsored by the American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS) as a part of their continuing effort to improve the safety performance of the chemical processing industry (CPI) through education of engineers and others who design, start-up, operate, maintain, and manage chemical processing plants. In particular, this book provides guidelines for the safe application of automation systems to the control of chemical/petrochemical processes.

1.1 SCOPE

This book is directed not only toward those responsible for the design, installation, use, and maintenance of process control systems, but also to the broader community of engineers who are responsible for the safe design, operation, and management of chemical processes. In the past, instrumentation and process control systems were designed by specialists who often were not full participants in process design development. As control systems become increasingly automated and more complex, it is even more important to safe design and operation that process design engineers and instrumentation and control specialists understand each other's disciplines and work together to provide facilities where instrumentation and control systems are fully integrated with process design to provide inherently safe facilities.

These guidelines provide current information to improve safety in the application of both the Basic Process Control System (BPCS) and the Safety Interlock System (SIS). The primary emphasis is on application of Programmable Electronic Systems (PESs), but the principles may be applied to all types of control system hardware. The term "PES" applies to all types of digital control systems: Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Single-Station Digital Controllers (SSDCs), and other microprocessor-based equipment that may be used for control applications.

The complete control system is covered, from the field-mounted process sensors through the control modules, the Human–Machine Interface (HMI), and the final control elements. The guidelines are applicable to both new and existing process control systems.
1. INTRODUCTION

1.2 LIMITATIONS

The discussion of safety issues in this book is limited to the direct or indirect applications of instrumentation and control devices that can prevent and/or mitigate identified unacceptable process conditions. The focus of this book is on human and environmental safety and does not stress the issue of property loss. These guidelines are not intended for the nuclear industry, nor the military. The special safety concerns related to the discrete parts manufacturing industry, materials handling industry, or the packaging industry are not addressed in this book even though they may have some applicability in the chemical/petrochemical industry. Neither do these Guidelines cover fire protection systems. This book does not provide guidelines for the identification of potentially hazardous conditions nor does it address application of prevention and/or mitigation techniques that do not involve automation. This book suggests guidelines for how to determine whether or not you need an SIS and provides guidelines for how to design one if it is needed. The reader is referred to other CCPS publications as well as other texts and standards for information covering these other topics, namely, Guidelines for Technical Management of Chemical Process Safety, Guidelines for Chemical Process Quantitative Risk Analysis, Guidelines for Hazard Evaluation Procedures, and Guidelines for Safe Storage and Handling of High Toxic Hazard Materials.

These Guidelines were written by a group of experts who are leaders in the safe automation of chemical processes. The book also has been reviewed by more than a dozen sponsor companies and organizations who support CCPS. Thus, the Guidelines in this book represent a spectrum of the current practices of industry leaders in this area.

1.3 OVERVIEW OF THE CONTENTS

Each of the seven chapters following this introduction addresses a phase of the automation process. While some elements of sound process control and automation are presented as a starting point, primary emphasis is on specific issues that impact safety, rather than operability and reliability.

There are many good references addressing basic considerations in the selection of instrumentation and application to the control of chemical processes. References are listed at the end of each chapter. The reader is encouraged to use additional sources in applying sound engineering practices to the application of automation systems.

A brief description of each chapter follows.
1.3.1 Chapter 2—The Place of Automation in Chemical Plant Safety...

A Design Philosophy

The chemical processing industry is in transition due to worldwide competition, increasing governmental regulations, and customer demands for product consistency and purity. These changing conditions require the use of more automation and less dependence on the human element in day-to-day operations. Rapid technological changes in control systems are also introducing additional pressures and opportunities that become important considerations. The impact of these factors on the application of automation to chemical processes is discussed.

Proper application of control systems improves safety in the operation of chemical processes. The use of modern technology offers additional enhancements if properly applied. Chapter 2 offers guidelines to accomplish this for both the Basic Process Control Systems (BPCSs) and the Safety Interlock Systems (SISs). The need to integrate these systems into an overall automation system is discussed.

A model is presented that steps through the different phases that should be included in the design of automation systems. It emphasizes the need for conducting hazard analysis, performing risk assessments, and identifying the various means that will be used to prevent and/or mitigate any hazards identified. Since both the BPCS and the SIS play important roles in this effort, the factors that are recommended for consideration in their selection, design, and application are discussed. Specific details covered in succeeding chapters of the text are referenced.

The concepts of "protection layer" and "Independent Protection Layer" are introduced. Guidelines are presented for identifying and evaluating if protection layers qualify as "Independent Protection Layers" (IPLs) using a set of specific criteria. Once the protection layers are defined and the need for additional protection in the form of automated protection layers is identified, a means for determining the design criteria for the required SIS IPL is presented. The need for each company to develop specific criteria in this area is emphasized, since decisions involve judgments of acceptable risk.

Finally, this chapter presents a summary of a safety design philosophy. The guidelines contained in the following chapters are based on this philosophy.

The approach presented in this chapter illustrates how a qualitative technique can be utilized if more rigorous quantitative techniques are not appropriate.

Readers are cautioned to satisfy their own guidelines or criteria when classifying systems (i.e., establishing SIS design requirements) and to use these guidelines in making distinctions among classifications.
1.3.2 Chapter 3—Techniques for Evaluating Integrity of Process Control Systems

This chapter discusses the importance of analyzing failure modes that may exist in control system components. It also covers the various techniques that can be utilized in evaluating the effects of these failures on the overall safety of the process. While both qualitative and quantitative techniques are presented, the reader is referred to other references for specific details.

The role of a Process Hazards Analysis (PHA) team is described and a framework for risk assessment and control throughout the life cycle of a process is presented. Particular emphasis is placed on the integration of process control system safety evaluations with overall risk review and control activities.

The types of safety reviews conducted during the evolution of a process design are described with emphasis on how automated process control system safety is integrated with overall process risk mitigation.

A technique for the certification or approval of equipment for particular applications within the automation process is suggested. A procedure to accomplish this is presented and both the benefits and shortcomings are discussed.

An extensive list of references is provided for the user.

1.3.3 Chapter 4—Safety Considerations in the Selection and Design of Basic Process Control Systems

Chapter 4 gives guidance in the application of control system technology, field instrumentation (process sensors and final control elements), operator/control system interface considerations, and process controllers in the Basic Process Control System (BPCS).

The safety impact of process sensors is discussed. Safety considerations in applying single-loop (pneumatic, analog, and digital) and distributed control system controllers are discussed. The application of varying types of final-control elements (e.g., control valves) is also presented. Emphasis is on the safety aspects rather than on general application and selection guidelines, since these can be found in other texts and references.

Operator/control system interface considerations are covered from the viewpoint of information overload or adequacy of information available to the operator. Guidelines are presented for selecting and supporting various types of hardware in the BPCS.

Information is also provided relating to safety concerns in power supply, grounding and distribution systems, installation of specific components, communication considerations between systems, and the use of advanced control techniques.