# Guidelines for Preventing Human Error in Process Safety

Center for Chemical Process Safety
of the
American Institute of Chemical Engineers
345 East 47th Street, New York, NY 10017

*To the Memory of John Embrey, 1937–1993*



**Library of Congress Cataloging-in Publication Data**
Guidelines for preventing human error in process safety.
p. cm.
Includes bibliographical references and index.
ISBN 0–8169–0461–8
1. Chemical processes—Safety measures. 2. Human engineering.
I. American Institute of Chemical Engineers. Center for Chemical Process Safety.
TP155.5.G778 1994
660' .2804—dc20 94–2481
CIP

**This book is available at a special discount when ordered in bulk quantities. For information, contact the Center for Chemical Process Safety of the American Institute of Chemical Engineers at the address shown above.**

# Preface

The Center for Chemical Process Safety (CPS) was established in 1985 by the American Institute of Chemical Engineers (AIChE) for the express purpose of assisting the Chemical and Hydrocarbon Process Industries in avoiding or mitigating catastrophic chemical accidents. To achieve this goal, CCPS has focused its work on four areas:

- establishing and publishing the latest scientific and engineering guidelines (not standards) for prevention and mitigation of incidents involving toxic and/or reactive materials;
- encouraging the use of such information by dissemination through publications, seminars, symposia and continuing education programs for engineers;
- advancing the state-of-the-art in engineering practices and technical management through research in prevention and mitigation of catastrophic events; and
- developing and encouraging the use of undergraduate education curricula that will improve the safety knowledge and awareness of engineers.

It is readily acknowledged that human errors at the operational level are a primary contributor to the failure of systems. It is often not recognized, however, that these errors frequently arise from failures at the management, design, or technical expert levels of the company. This book aims to show how error at all of these levels can be minimized by the systematic application of tools, techniques and principles from the disciplines of human factors, ergonomics, and cognitive psychology. The book is the result of a project in which a group of volunteer professionals from CCPS sponsor companies prepared a project proposal and then worked with the successful contractor, Dr. David Embrey of Human Reliability Associates, to produce this book. The ensuing dialogue has resulted in a book that not only provides the underlying principles and theories of the science of human factors, but also goes on to show their application to process safety problems and to the CCPS technical management of process safety system.

## 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 made this project possible; the members of its Technical Steering Committee who conceived of and supported this *Guidelines* project and the members of its Human Reliability Subcommittee for their dedicated efforts, technical contributions, and enthusiasm.

This book was written by Dr. David Embrey of Human Reliability Associates, with the assistance of the CCPS Human Reliability Subcommittee. Section 8.2, Managing Human Error by Design, which deals with the application of human factors principles in the process safety management system, was written by the Human Reliability Subcommittee.

- *The main authors of the text of the book were the following staff members of Human Reliability Associates:*
  Dr. David Embrey
  Dr. Tom Kontogiannis
  Mark Green
- *Other contributions from the following individuals are gratefully acknowledged:*
  Dr. Trevor Kletz
  Dr. Deborah Lucas
  Barry Kirwan
  Andrew Livingston
- *The members of the Human Reliability Subcommittee were:*
  Gary A. Page, American Cyanamid Co., (Chairman)
  Joseph Balkey, Union Carbide Corp.
  S. Barry Gibson, DuPont
  Mark D. Johnson, Eastman Kodak Co.
  Joseph B. Mettalia, Jr., CCPS Staff Consultant
  Gary Van Sciver, Rohm and Haas Co.
  Joseph C. Sweeney, ARCO Chemical Co.
- *Reviewers were:*
  Daniel A. Crowl, Mich. Tech. University
  Randolph A. Freeman, Monsanto Co.
  Thomas O. Gibson, The Dow Chemical Co.
  William N. Helmer, Hoechst Celanese Corp.
  Michele M. Houser, Martin Marietta Energy Systems
  Trevor A. Kletz, Process Safety Consultant
  Donald K. Lorenzo, Process Safety Institute
  Denise B. McCafferty, DNV Technica, Inc.
  Michael T. McHale, Air Products and Chemicals, Inc.
  David Meister, Consultant

Robert W. Ormsby, Air Products and Chemicals, Inc.
Wayne A. Pennycook, Exxon
John D. Snell, OxyChem
Marvin F. Specht, Hercules Incorporated
Donald Turner, CH2M Hill
Lester H. Wittenberg, CCPS

The Human Reliability Subcommittee wishes to express its appreciation to Lester Wittenberg, Thomas Carmody, and Bob G. Perry of CCPS for their enthusiastic support.

# Glossary and Acronyms

## GLOSSARY

*Active Errors* An active human error is an intended or unintended action that has an immediate negative consequence for the system.

*Cognitive "tunnel vision"* A characteristic of human performance under stress. Information is sought that confirms the initial hypothesis about the state of the process while disregarding information that contradicts the hypothesis.

*Encystment* A characteristic of human performance under stress. Encystment occurs when minor problems and details are focused on to excess while more important issues are ignored.

*External Error Mode* The observable form of an error, for example, an action omitted, as distinct from the underlying process

*Externals* Psychological classification of individuals who assume (when under stress), that the problem is out of their immediate control and therefore seek assistance.

*Human Error Probability* The probability that an error will occur during the performance of a particular job or task within a defined time period. *Alternative definition:* The probability that the human operator will fail to provide the required system function within the required time.

*Human Information-Processing* A view of the human operator as an information-processing system. Information-processing models are conventionally expressed in terms of diagrams which indicate the flow of information through stages such as perception, decision-making, and action.

*Human Reliability* The probability that a job will be successfully completed within a required minimum time.

*Human–Machine Interface* The boundary across which information is transmitted between the process and the worker, for example, analog displays, VDUs.

*Internal Error Mechanism* The psychological process (e.g., strong stereotype takeover) that underlies an external error mode.

*Internal Error Mode* The stage in the sequence of events preceding an external error mode at which the failure occurred (e.g., failed to detect the initial signal).

*Internals* Individuals who, when under stress, are likely to seek information about a problem and attempt to control it themselves.

*Knowledge-Based Level of Control* Information processing carried out consciously as in a unique situation or by an unskilled or occasional user

*Latent error* An erroneous action or decision for which the consequences only become apparent after a period of time when other conditions or events combine with the original error to produce a negative consequence for the system.

*Locus of Control* The tendency of individuals to ascribe events to external or internal causes, which affects the degree of control that they perceive they have over these events. (See also *Externals* and *Internals.*)

*Manual Variability* An error mechanism in which an action is not performed with the required degree of precision (e.g., time, spatial accuracy, force).

*Mindset Syndrome* A stress-related phenomenon in which information that does not support a person's understanding of a situation is ignored. (See also *Cognitive tunnel vision.*)

*Mistakes* Errors arising from a correct intentions that lead to incorrect action sequences. Such errors may arise, for example, from lack of knowledge or inappropriate diagnosis.

*Performance-Influencing Factors* Factors that influence the effectiveness of human performance and hence the likelihood of errors.

*Population Stereotype* Expectations held by a particular population with regard to the expected movement of a control or instrument indicator and the results or implications of this movement

*Reactance* Occurs when a competent worker attempts to prove that his or her way of doing things is superior in response to being reassigned to a subordinate position.

*Recovery Error* Failure to correct a human error before its consequences occur.

*Risk Assessment* A methodology for identifying the sources of risk in a system and for making predictions of the likelihood of systems failures.

*Risk Homeostasis* The theory that an operator will attempt to maintain a stable perception of risk following the implementation of new technology that increases the safety of a human–machine system. The theory predicts that operators will take greater risks where more safety devices are incorporated into the system.

*Role Ambiguity* Exists when an individual has inadequate information about his or her roles or duties.

*Role Conflict* Exists when there is the simultaneous occurrence of two or more sets of responsibilities or roles such that compliance with one is not compatible with compliance with the other(s).

*Root Causes* The combinations of conditions or factors that underlie accidents or incidents.

*Rule-Based Level of Control* In the context of chemical industry tasks, the type of human information processing in which diagnoses are made and actions are formulated on the basis of rules (e.g., "if the symptoms are X then the problem is Y").

*Rule Book Culture* An organization in which management or workers believe that all safety problems can be resolved by rigid adherence to a defined set of rules.

*Skill-Based Level of Control* A mode of information processing characterized by the smooth execution of highly practiced, largely physical actions requiring little conscious monitoring.

*Slips* Errors in which the intention is correct but failure occurs when carrying out the activity required. Slips occur at the skill-based level of information processing.

*Stereotype Fixation* Occurs when an individual misapplies rules or procedures that are usually successful.

*Stereotype Takeover* Occurs when an incorrect but highly practiced action is substituted for a correct but less frequently occurring action in a similar task. Also called a *strong habit intrusion.*

*Traditional Safety Engineering* A safety management policy that emphasizes individual responsibility for system safety and the control of error by the use of motivational campaigns and punishment.

*Vagabonding* Stress-related phenomenon in which a person's thoughts move rapidly and uncontrollably among issues, treating each superficially.

*Verbal Protocol Analysis* Technique in which the person is asked to give a "self-commentary" as he or she undertakes a task.

*Violation* An error that occurs when an action is taken that contravenes known operational rules, restrictions, and/or procedures. The definition of violations excludes actions taken to intentionally harm the system (i.e., sabotage).

## ACRONYMS

| | |
|---|---|
| *AT* | Area Technician |
| *CADET* | Critical Action and Decision Evaluation Technique |

| | |
|---|---|
| *CADs* | Critical Actions or Decisions |
| *CCPS* | Center for Chemical Process Safety |
| *CCR* | Central Control Room |
| *CCTV* | Closed-Circuit Television |
| *CHAP* | Critical Human Action Profile |
| *CPI* | Chemical Process Industry |
| *CPQRA* | Chemical Process Quantitative Risk Assessment |
| *CR* | Control Room |
| *CRT* | Cathode Ray Tube |
| *CSE* | Cognitive Systems Engineering |
| *CT* | Critical Tasks |
| *CTI* | Critical Task Identification |
| *CV* | Current Values |
| *DA chart* | Decision Action Chart |
| *ECFC* | Events and Causal Factors Charting |
| *ERS* | Error Reduction Strategies |
| *FMECA* | Failure Modes and Effects of Criticality Analysis |
| *GEMS* | Generic Error Modeling System |
| *HAZOP* | Hazard and Operability Study |
| *HEA* | Human Error Analysis |
| *HEP* | Human Error Probability |
| *HFAM* | Human Factors Assessment Methodology |
| *HFE/E* | Human Factors Engineering and Ergonomics Approach |
| *HMI* | Human–Machine Interface |
| *HPES* | Human Performance Evaluation System |
| *HPIP* | Human Performance Investigation Process |
| *HRA* | Human Reliability Analysis |
| *HRAM* | Human Reliability Assessment Method |
| *HRP* | Hazard Release Potential |
| *HSP* | Hazard Severity Potential |
| *HTA* | Hierarchical Task Analysis |
| *IDA* | Influence Diagram Approach |
| *IMAS* | Influence Modeling and Assessment System |
| *IRS* | Incident Reporting Systems |
| *ISRS* | International Safety Rating I Systems |
| *LTA* | Less Than Adequate |
| *MAST* | Memory and Search Test |

| | |
|---|---|
| *MORT* | Management Oversight and Risk Tree |
| *MSM* | Molecular Sieve Module |
| *NIOSH* | National Institute of Occupational Safety and Health |
| *NMRS* | Near Miss Reporting System |
| *NRC* | US Nuclear Regulatory Commission |
| *OAET* | Operator Action Event Tree |
| *OSD* | Operational Sequence Diagram |
| *P&ID* | Piping and Instrumentation Diagram |
| *PA* | Public Address |
| *PCS* | Process Control System |
| *PDCC* | Program Development and Coordination Committee |
| *PHEA* | Predictive Human Error Analysis |
| *PIF* | Performance Influencing Factors |
| *PORV* | Pilot-Operated Relief Valve |
| *PPE* | Personal Protective Equipment |
| *PRV* | Pressure Relief Valve |
| *PSA* | Probabilistic Safety Analysis |
| *PSF* | Performance Shaping Factors |
| *QRA* | Quantitative Risk Assessment |
| *RCAS* | Root Cause Analysis System |
| *RHT* | Risk Homeostasis Theory |
| *SFG* | Signal Flow Graphs |
| *SLI* | Success Likelihood Index |
| *SLIM* | Success Likelihood Index Method |
| *SM* | Separator Module |
| *SOP* | Standard Operating Procedure |
| *SORTM* | Stimulus Operation Response Team Performance |
| *SP* | Set Points |
| *SPEAR* | System for Predictive Error Analysis and Reduction |
| *SRK* | Skill–Rule–Knowledge-Based Model |
| *STAHR* | Sociotechnical Approach to Human Reliability |
| *STEP* | Sequentially Timed Events Plotting Procedure |
| *TA* | Task Analysis |
| *THERP* | Technique for Human Error Rate Prediction |
| *TQM* | Total Quality Management |
| *TSE* | Traditional Safety Engineering |
| *VDU* | Visual Display Unit |