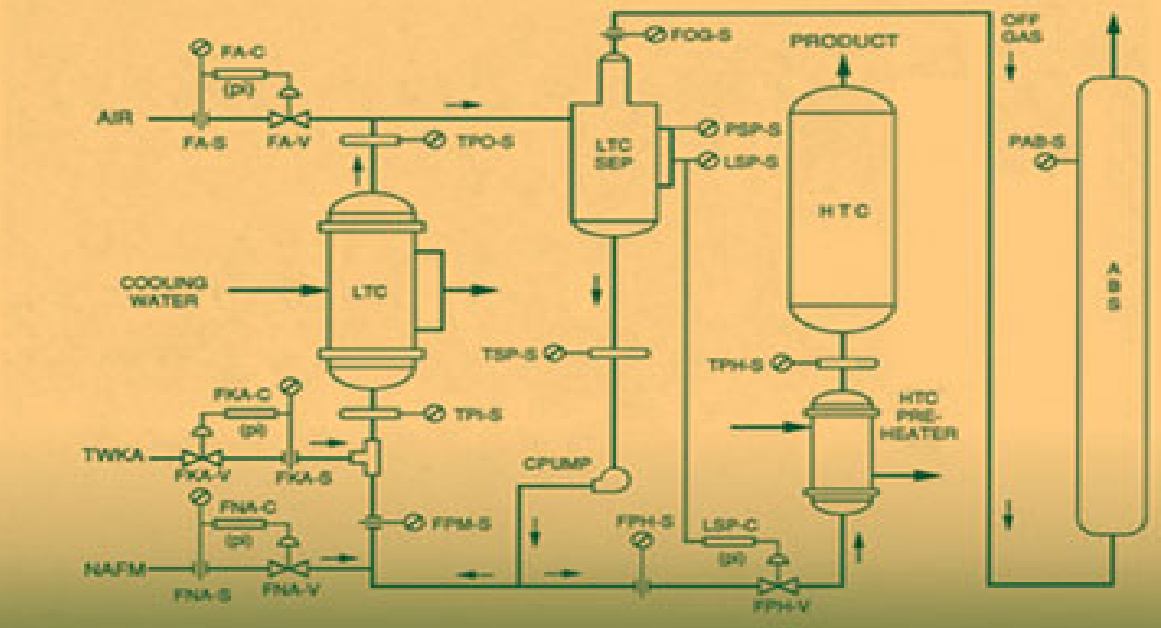
Optimal Automated Process Fault Analysis

Richard J. Fickelscherer and Daniel L. Chester



WILEY

AIChE

Contents

OPTIMAL AUTOMATED PROCESS FAULT ANALYSIS

Richard J. Fickelscherer

FALCONEER Technologies

Daniel L. Chester

FALCONNER Technologies and
Department of Computer and Information Sciences
University of Delaware

AIChE

WILEY

A JOHN WILEY & SONS, INC., PUBLICATION

Cover design: John Wiley & Sons, Inc.
Cover image: Courtesy of Richard J. Fickelscher

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at 877-762-2974, outside the United States at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Cataloging-in-Publication Data:

Fickelscherer, Richard J.
Optimal automated process fault analysis / by Richard J. Fickelscherer, Ph.D., P.E. co-founder, Falconeer Technologies, LLC & Daniel L. Chester, Ph.D. co-founder, Falconeer Technologies, LLC & associate chair, Department of Computer & Information Sciences, University of Delaware.
pages cm
Includes index.
ISBN 978-1-118-37231-9 (cloth)
1. Chemical process control–Data processing. 2. Fault location (Engineering)–Data processing. I. Chester, Daniel L. II. Title.
TP155.75.F527 2013
660′.2815–dc23

2012023637

R.J.F.: I dedicate this book to my loving wife, Pat, for all her encouragement and help, and for always believing in me. I am very fortunate to have found her and to have her at the center of my life.

D.L.C.: I dedicate this book to my parents, Fred and Della, for all the guidance they gave me over the years, and for making it possible for me to get the training and develop the skills that led to my contributions to this book. Their encouragement has always been appreciated.

FOREWORD

It is an honor to be asked to write the foreword to Rich and Dan's book on diagnostic reasoning for process plants. The story of the FALCON diagnostic system goes back to when I first joined MIT as a young faculty member in the early 1980s. In those days computing meant numerical computation in Fortran or C, mainframes and minicomputers ruled, and personal computers were underpowered novelties. Process control had begun a slow transition from pneumatic to digital instrumentation, but the first digital controllers were modeled unimaginatively after the PID loops they were replacing.

But Metcalfe's law was in full exponential ascent, and the world was rapidly changing, not only in terms of faster numerical methods. New ideas from artificial intelligence were flooding across the MIT campus, upending the very foundation of computing by means of an entirely new synthesis of symbolic, object-oriented, neural, and rule-based computing. Touching off a great intellectual ferment in chemical engineering, virtually every aspect of process operations was being transformed. Gauges transformed into graphical operator interfaces, fixed threshold alarms into intelligent monitoring and diagnosis, and steady-state operation into dynamic economic optimization.

The University of Delaware was one of the leaders in this exploration, especially in the area of process monitoring and fault diagnosis. Undertaking a joint project with Foxboro and DuPont in the early 1980s, Delaware spearheaded the first industrial application of an expert system, FALCON (fault analysis consultant), for online fault diagnosis of the DuPont adipic acid plant in Victoria, Texas. A key idea, expounded

further in this book, was the synthesis of logical (pattern or rule) analysis and quantitative mathematical modeling.

This period of creative experimentation reached its zenith in 1995, at the First International Conference on Intelligent Systems in Process Engineering in Snowmass, Colorado. By that time, I had moved to an MIT spin-off, Gensym Corporation, developers of the G2 real-time expert system development environment. G2 was that generation's ultimate synthesis of graphical UI, structured natural language, object-oriented programming, and rule-based processing. The conference showcased innovative knowledge-based systems ranging from product design to intelligent control, optimization, and diagnostics. Flush with the success of building and deploying hundreds of expert systems to solve real industrial problems, few of us realized just how quickly another revolution, the Internet, was going to overturn everything, yet again.

Throughout these many changes, some determined individuals have persevered to bring the vision of intelligent operations closer to reality. In this book, Rich and Dan explain how they transformed the art of the diagnostic expert system into a practical and reproducible system, implemented in FALCONEER™ IV to increase the operating safety and reliability of process systems. Their system captures many lessons learned during the rapid and often convulsive change of the past 25 years. I wish them the very best.

Mark A. Kramer, Ph.D.

Winchester, Massachusetts
February 2012

PREFACE

Process fault analyzers are computer programs that can monitor process operations to identify the underlying cause(s) of operating problems. A general method for creating process fault analyzers for chemical and nuclear processing plants has been sought ever since the incorporation of computers into process control. The motivation has been the enormous potential for improving process plant operations in terms of safety and productivity. Automated process fault analysis should help process operators (1) prevent catastrophic operating disasters such as explosions, fires, meltdowns, and toxic chemical releases; (2) reduce downtime after emergency process shutdowns; (3) eliminate unnecessary process shutdowns; (4) maintain better quality control of process products; and (5) ultimately, allow both higher process efficiency and higher production levels.

A wide variety of logically viable diagnostic strategies now exist for automating process fault analysis. However, automated fault analysis is currently still not widely used within the processing industries. This is due mainly to the following limitations: (1) the prohibitively large development, verification, implementation, or maintenance costs of these programs; (2) an inability to operate a program based on a given diagnostic strategy continuously online or in realtime; and (3) an inability to model process behavior at the desired level of detail, thus leading to unreliable or highly ambiguous diagnoses. Subsequently, a method for efficient production of automated process fault analyzers is still being actively sought. It is our contention that evaluating engineering models of normal process operation with current process data is the most promising

and powerful means of directly identifying underlying process operating problems. Doing so generates an unimpeachable source from which to logically infer the current state of the process being modeled. Performing this inference automatically online enables these programs to perform *intelligent supervision* of the daily operations of their associated process systems. It makes possible a fundamental understanding of a given process system's design and operation to be utilized in evaluating its current operating conditions.

The *method of minimal evidence* (**MOME**) is a model-based diagnostic strategy for developing optimal automated process fault analyzers. It was derived at the University of Delaware while developing the **FALCON** (fault analysis consultant) ***system***, a real-time online process fault analyzer for a commercial-scale adipic acid plant formerly owned and operated by DuPont in Victoria, Texas. It provides a uniform framework for examining both models of normal process operation and their corresponding associated modeling assumptions that are required to build such fault analyzers. MOME can be used directly to correctly diagnose both single- and multiple-fault situations, to determine the strategic placement of process sensors to facilitate fault analysis, and to determine the shrewd division of a large process system for distributing fault analyzers.

The MOME diagnostic strategy was again demonstrated to be effective in a commercial-scale persulfate plant owned and operated by FMC in Tonawanda, New York. Versions of two *knowledge-based systems* (**KBSs**) developed using MOME have been running online at this plant since February 2001. In the current implementation, these KBSs [a.k.a. **FALCONEER™ IV** (**FALCON** via engineering equation residuals IV)] diligently perform automated sensor validation and fault analysis of both FMC's electrolytic sodium persulfate and liquid ammonium persulfate processes in

realtime. The development effort for these two FALCONEER IV applications was more than two orders of magnitude less than that required for the original FALCON system, with even better performance to date. This impressive improvement in the development and maintenance effort required was possible because FALCONEER IV contains a compiler program that automatically generates the *sensor validation and proactive fault analysis* (**SV&PFA**) *diagnostic logic* required to perform competent fault analysis directly from the underlying engineering models of normal process operation. Since the MOME diagnostic strategy is a systematic procedure, creating an algorithm based on it and then codifying that algorithm proved to be straightforward. This treatment describes both the underlying logic of MOME and the fuzzy logic algorithm based on it. It is meant to be a study guide for those who wish to develop such fault analyzers for their own process systems.

Motivations for automating process fault analysis are described in detail in Chapter 1. Our patented methodology for automating process fault analysis (MOME and its associated fuzzy logic algorithm) is then discussed in detail in Chapters 2 to 5. The logic behind model-based reasoning in general and MOME in particular is described in Chatper 2. The MOME logic for performing single- and multiple-fault diagnosis is described in Chapter 3. Also discussed in Chapter 3 are the motivations behind the creation of process fault analyzers based on MOME automatically via the SV&PFA diagnostic rule logic compiler program contained in FALCONEER™ IV. The fuzzy logic algorithm automating MOME as implemented in this compiler is described in Chapter 4. In Chapter 5 the criteria for shrewdly distributing process fault analyzers throughout a large processing plant are described. Some general guidelines for the strategic placement of process sensors for directly facilitating fault diagnosis are also discussed.

Chapter 6 covers the need to augment process fault analysis with trend analysis of the various process sensor measurements and *key performance indicators* (**KPIs**) via the *virtual statistical process control* (**virtual SPC**) technique of calculating and analyzing *exponentially weighted moving averages* (**EWMAs**).

The need to first determine the current overall operating state of the process undergoing automated fault analysis in discussed in Chapter 7. Such determinations provide the proper context required for the fault analyzer to make legitimate diagnoses.

Chapter 8 summarizes the benefits derived and lessons learned when employing FALCONEER™ IV in actual process applications. A systematic procedure to follow when creating such applications is also described. The chapter concludes by summarizing the advantages of distilling the raw information contained in typical process sensor data continuously into value-added knowledge concerning the current state of process operations and having that knowledge be instantaneously available for *intelligent supervision* of those operations.

For completeness, four appendixes have been added to this treatment as background information. A number of the other various possible diagnostic strategies also used to automate process fault analysis and their limitations are reviewed briefly in Appendix A. Appendix B describes DuPont's adipic acid plant and the original automated process fault analyzer (i.e., the FALCON system) developed for it. The lessons learned from the development of this real-world fault analyzer are discussed in detail. The advantages of using the knowledge-based system paradigm for solving problems, especially those that led directly to the creation of the MOME diagnostic strategy, are also discussed. As described throughout the book, this strategy has since been codified into FALCONEER™ IV. Appendix C outlines the logic

that was used by the original hand-compiled FALCONEER system to determine the current process state in FMC's electrolytic sodium persulfate plant. This logic has since been simplified, generalized, and codified in the current implementation of FALCONEER™ IV. Finally, Appendix D describes two downloadable FALCONEER™ IV demos provided to accompany this treatment.

Richard J. Fickelscherer
Daniel L. Chester

ACKNOWLEDGMENTS

First, we would like to thank the other two key chief investigators at the University of Delaware on the original FALCON project, Professors Prasad S. Dhurjati and David E. Lamb, along with many student research assistants, including Oliver J. Smith IV, George M. A'zary, Larry Kramer, Dave Mooney, Lisa Laffend, Kathy Cebulka, Apperson Johnson, and Bob Varrin, Jr. We would also like to thank DuPont and its employees Duncan Rowan, Rick Taylor, John Hale, Robert Wagner, Bob Gardener, and Tim Cole, and especially our domain expert, the late Steve Matusevich. At Foxboro Inc., we would like to thank Dick Shirley, Dave Fortin, and the late Terry Rooney. Further, we thank Oliver J. Smith IV and Duncan Rowan for reviewing earlier versions of this treatment; their comments about ways to improve it were invaluable.

We also thank the FMC Corporation for its support in developing the various FALCONEER and FALCONEER™ IV KBS program applications, especially Doug Lenz, John Rovison, Charlie Lymburner, Weidong An, Don Lapham III, John Helieko, Don Stockhausen, and Jim Kaylor. As a cofounder of FALCONEER Technologies LLC, Doug Lenz strongly advocated including virtual SPC capabilities in FALCONEER™ IV; we would like to acknowledge the programming efforts of Lee Daniels required to accomplish both this and the streamlined state identification capability also currently included in FALCONEER™ IV.

Feel free to contact either of us if you would like to find out more about the FALCONEER™ IV software and our company's services. Following is the contact information:

Dr. Richard J. Fickelscherer, PE
Tonawanda, New York
falconeertech@verizon.net

Prof. Daniel Chester
Newark, Delaware
chester@cis.udel.edu

1

MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

1.1 INTRODUCTION

Economic competition within the *chemical process industry* (CPI) has led to the construction and operation of larger, highly integrated, and more automated production plants. As a result, the primary functions performed by the process operators in these plants have changed. An unfortunate consequence of such changes is that the operators' ability to perform process fault management has been diminished. The underlying reasons for this problem and the methods currently used to counteract it are discussed here.

1.2 CPI TRENDS TO DATE

The CPI constitutes one of the largest and most important segments of the global economy. While developing into its current, relatively stable position, competition for market share among the various chemical producers has greatly intensified. This competition has, in turn, created continuously downward pressure on the market price, and hence the associated profit margin, of most commodity chemical products. Several major trends within the CPI in the operation of production plants have resulted.

One of these trends exploits the economies of scale inherent in chemical manufacturing as a means to reduce costs. This has led to the construction and operation of

plants with ever-larger production capacities. While such facilities represent enormous capital investments, fixed costs per unit of production have been reduced substantially. Moreover, operating these larger plants has also reduced the direct labor costs because relatively fewer process operators are required per unit of production. As a result of this trend, most commodity chemicals are currently produced at facilities known as *world-class* plants.

Another major trend within the CPI has been the automation of the various process operations, especially process control functions. The motivation for automating process control functions is that it results in applying the best available process control strategies more accurately in a continuous, consistent, and dependable manner [1,2]. This automation has been made possible by advances in both computer technology and process control theory. Such advances have made automated control more economically feasible, reliable, and available [1]. Process computers have also provided a significant means for dealing with the diverse and complex information required to operate a modern production plant effectively [2]. Together with advances in electronic instrumentation, these developments have led to centralized control rooms that require considerably fewer personnel to operate [1].

A third major trend designed to reduce production costs has resulted from attempts to use energy more efficiently. These have included the application of traditional conservation measures, such as adequately insulating process equipment, and various measures designed to recover and reutilize energy more effectively. The latter measures have been a direct cause of greater process system integration. This has, in turn, increased functional coupling among the various process subsystems, thereby making the operation of these subsystems highly interdependent. These interdependencies complicate

operation of the overall process system, making it more difficult to start up, shut down, and control during production runs. It also opens up the possibility that a malfunction in one subsystem will cause malfunctions in other subsystems connected to them functionally.

A similar situation has resulted from the trend toward maintaining smaller inventories of raw materials and intermediate products. This complicates process operation in two ways. Since smaller buffers exist between the process subsystems, the effects of a malfunction in one subsystem can more easily migrate to other subsystems. In addition, if one subsystem is shut down for a prolonged period, it may force subsystems connected to it to be shut down. The trend toward greater process system integration and that toward limited storage facilities have a common consequence: They both make effective operation of the overall process system more critically dependent on the coordinated, faultless operation of its process subsystems.

A final trend for reducing production costs has been to maximize the availability of the plant for production. This is typically accomplished by optimally scheduling the production runs and by minimizing the effects of unexpected production disruptions. A variety of methods are in use to either eliminate or minimize the severity of unexpected production disruptions. Nonetheless, as the complexity of the plants has increased, making plants available for production has become much more difficult because the number of potential operating problems has also increased [3]. This tends to increase the frequency of unexpected production disruptions. Consequently, maximizing plant availability for efficient process operation has become more dependent on effective management of its various potential operating problems [4].

1.3 THE CHANGING ROLE OF PROCESS OPERATORS IN PLANT OPERATIONS

The process operators' main task in plant operation is to assess the process state continuously [1] and then, based on that assessment, to react appropriately. Process operators thus have three primary responsibilities [5]. The first is to monitor the performance of the various control loops to make sure that the process is operating properly. The second is to make adjustments to the process operating conditions whenever product quality or production efficiency falls outside predefined tolerance limits. The operators' third, and by far most important, responsibility is to respond properly to emergency situations: in other words, carry out effective and reliable process fault management. Such management requires that the operators detect, identify, and then implement the correct counteractions required to eliminate the process fault or faults that are causing the emergency situation. If process fault management is performed incorrectly, accidents can occur, as they have on many occasions.

The biggest change in the functions performed by process operators has been caused by the increased automation of process control. Operators now monitor and supervise process operations rather than controlling them manually. Moreover, increasingly, such functions are accomplished with interface technology designed to centralize control and information presentation [6]. As a result, their duties have become less interesting and their ability to carry out manual process control has diminished. Both situations have increased the job dissatisfaction experienced by process operators [6] and have diminished the operators' ability to perform process fault management.

A second change in the functions performed by operators in modern plants has resulted from having fewer operators present. Each operator has become responsible for a larger portion of the overall process system. This increases the risk of accidents because relatively fewer operators are available at any given time to notice the development of emergency situations or help prevent such situations from causing major accidents. In addition to the increased risk, the potential severity of accidents has also increased because larger quantities of reactive materials and energy are being processed. This makes the operators' ability to perform process fault management much more critical for ensuring safe operation of a plant.

One method used to help reduce the risk of a major accident has been the addition to the overall process control system of emergency interlock systems. Such systems are designed to shut the process down automatically during emergency situations, thereby reducing the likelihood of accidents that could threaten human and environmental well-being or damage process equipment. Emergency interlock systems therefore help ensure that a process operation is safe during emergency situations by decreasing the effects of human error [7]. Eliminating such accidents also protects the operational integrity of the process system, which in turn allows it to be restarted more quickly after emergency shutdowns.

However, the widespread use of emergency interlock systems has caused the operators' primary focus in plant operations to change from that of process safety to that of economic optimization [8]. In emergency situations, operators are now more concerned with taking the corrective actions required to keep the process system operating rather than those that will shut it down safely. They rely on the interlock system to handle emergency shutdowns, trusting that it will take over once operating

conditions become too dangerous to let production continue.

A potential problem with this strategy is that to keep the process system operating, operators may take actions that counteract the symptoms of a fault situation without correcting the situation itself [9]. Such behavior by the operators may cause them inadvertently to circumvent protection of the emergency interlock system, thereby creating an emergency situation which they falsely believe to be within that protection. Another potential problem of this strategy is that the interlock system may fail, which again will create a situation in which the operators falsely believe that the process system is protected by the emergency interlock system. These potential problems can be reduced by (1) prudent design of the interlock system, (2) being certain to add sufficient redundancy to detect critically dangerous situations [7], (3) establishing a formal policy by which particular interlocks can be bypassed during process operation [10], and (4) adequate maintenance of the interlock system [11].

In summary, the automation of process control duties and of emergency process shutdowns has shifted the operators' main activities away from direct process control to that of passive process monitoring. Moreover, automation has also tended to shift their primary emphasis away from process safety to that of economic optimization. As a result of these changes, the operators' ability to perform process fault management has been reduced. Unfortunately, this reduction has occurred during a period when such management has become more critical to both the safe and economical operation of the production plants. In response, various methods have been developed to help counteract this decline in human capability with process fault management.

1.4 METHODS CURRENTLY USED TO PERFORM PROCESS FAULT MANAGEMENT

A variety of methods have been developed either to reduce the occurrence of process faults or to help operators perform process fault management more effectively when it is required. The methods currently used to reduce the occurrence of process faults include (1) designing process systems with greater operational safety in mind; (2) constructing process plants that have better quality, and therefore more reliable, process equipment; (3) implementing comprehensive programs of preventive maintenance; and (4) establishing standard operating procedures and following them strictly. The direct methods currently used to help operators perform process fault management include (1) extensive training of operators in process fault management, (2) adding alarm systems to process control systems, (3) adding emergency interlock systems to process control systems, and (4) designing better control consoles and human–machine interfaces. Each of the eight methods, along with their associated shortcomings, is discussed below.

It is useful first, though, to examine how the failures in chemical plant operations are distributed by frequency. A survey of chemical plant failures [12] in the past has shown that operational failures account for 49% of the total number of failures, while human failures account for another 32% of that total. Equipment failures account for approximately one-half of all operational failures. The remaining failures are caused by defects in process design, process equipment manufacturing, or plant construction (15.5%), and by external events or natural causes (3.5%). A survey conducted by Mashiguchi of chemical plant failures

in Japan has shown a similar distribution [13]. Venkatasubramanium [14] cites studies which state that human error may account for up to as much as 70% of industrial accidents. Although highly anecdotal in nature, such failure distributions do provide a good indication of the classes of failures that are not being addressed properly by current fault management measures. Nimmo cites studies which estimate that the results of abnormal process operations (including inadequate process fault management) cost the U.S. petrochemical industry alone $20 billion per year [15].

The first, and most effective way to eliminate potential process faults is to keep them out of the process system design. As Lees [16] states: “The safety of the plant is determined primarily by the quality of the basic design rather than by the addition of special safety features.” Correspondingly, to identify potential operating safety problems, hazardous operation (HAZOP) studies [17] are now commonly performed during the design and construction of both new process systems and process retrofits. Such studies systematically examine alternative designs for potential safety problems, thereby allowing these designs to be compared on a common basis of potential operating risk. They are also very useful tools for determining how that risk will be affected by a particular process system improvement or operating failure. Software tools that perform online risk analysis are also now becoming available [18-31]. Such tools should allow operators to keep apprised of the relative levels of risk associated with operating a process in partially failed modes.

Nonetheless, it will never be possible to totally eliminate the risk inherent in chemical plant operations. The best that can be done is to reduce this risk below an acceptable limit. Moreover, risk analysis studies can be performed

improperly, either by overlooking some potential process faults or by using poor estimates of the risk factors associated with particular faults [32-34].

Constructing process plants with higher-quality equipment and employing comprehensive preventive maintenance programs are two methods designed to improve the reliability of process equipment during production runs. Both methods reduce the likelihood that a particular system component will malfunction, thus forcing an emergency process shutdown or causing an accident. Additionally, preventive maintenance sometimes uncovers incipient problems before they develop into major equipment failures that cause long process downtimes. This allows appropriate corrective actions to be taken well before such situations occur. Determining optimal scheduling of preventive maintenance shutdowns is a problem currently under active research [35-38].

Regardless, because of the stochastic nature of equipment failure, accurate prediction of when a particular process system component will malfunction is impossible. Preventive maintenance can therefore not be used to eliminate all process equipment failures. A very good example of this can be seen in the production of ammonia [39,40]. An average ammonia plant is out of service for preventive maintenance approximately 20 days a year. These plants are still out of service for a similar period of time due to unpredicted or sporadic equipment failures.

The final method of reducing the occurrence of process faults is the establishment of standard operating procedures. Establishing and then following such procedures strictly represents the most straightforward way to reduce process faults caused by human errors. This is because such procedures provide operators with simple guidelines for proper operation of a process system. Distilled from past operating experience and from safety considerations of

which the operators may not even be aware, such procedures specify the sequence of actions that have been proven to control process operation effectively and safely. By following such predetermined procedures, the various operators' responses to particular situations will be more predictable, more consistent, and consequently, more reliable.

However, there are several potential problems that can result from relying too heavily on standard operating procedures for safe process operation. These arise from the requirement that the operator remember all of the procedures, together with their exceptions, and then use them in the appropriate situations. For a given situation, operators may not apply the proper procedures because they either have never fully learned or have forgotten the correct procedures. Another problem is that they may misinterpret the situation and apply incorrect procedures. A third potential problem is that operators may be confronted with a situation for which either predetermined procedures do not exist or for which those that do exist are not appropriate. Another potential problem is that operators may ignore predetermined procedures and attempt to devise their own, thereby defeating the purpose of having standard operating procedures. The final potential problem is that they may blindly follow a predetermined procedure even though it leads directly to the development of an emergency situation.

Comprehensively training operators in effective process fault management is the best way to overcome the problems noted above. Training is designed to develop three critical cognitive abilities in operators [41]. The first is to give them knowledge of what the system will do by itself to recover from abnormal operating conditions and what operators are required to do; the second is to give operators knowledge of how a system will respond to unwarranted