
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.

Optimal Automated Process Fault Analysis, First Edition.

Richard J. Fickelscherer and Daniel L. Chester.

© 2013 John Wiley & Sons, Inc. Published 2013 by John Wiley & Sons, Inc.

2 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

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

4 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

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]. Venkatasubramaniam [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].

6 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

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 inputs; and the third is to reduce operators' stress when abnormal process operating conditions occur. As a result of such fault management training, operators develop competence as well as confidence in their ability to perform successfully during abnormal process operating conditions [41].

Nonetheless, problems can arise when attempting to train operators properly in process fault management. Perhaps the greatest problem is that typically it is not possible for operators to practice with, and be tested on, the actual process system during their training. This causes various problems in trying to simulate the actual process conditions [42]. Operators are still expected to be versatile enough to diagnose faults they have not experienced previously, might not fully understand, and perhaps might not foresee [42]. As noted by both Ducan [42] and Rasmussen [43], the operators who are most proficient at fault management are those who are trained by experienced operators or by the experience of controlling the process system manually. Consequently, the

8 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

current trend toward fewer process operators and automated process control will cause the operators' training to be less than optimal.

Adding alarm systems to a process control system is another method currently used to help operators perform process fault management. Alarm systems are designed to alert operators to abnormal operating conditions before emergency situations develop. Such warnings usually give operators sufficient information to identify, respond to, and completely rectify the cause of abnormal conditions long before an emergency shutdown occurs. Furthermore, even if such a shutdown does occur, the cause can usually be readily determined from the pattern of alarm messages that are generated before the interlock system is activated.

Unfortunately, the proliferation of alarms in chemical and nuclear plants has led to a situation known as *alarm inflation*. This situation has arisen because of the increased number of alarms used in these plants, the fact that many of these alarms do not directly indicate the cause of the abnormal process conditions, and the fact that an inconsistent philosophy is sometimes used to design alarm systems [7]. Nonoptimal alarm design [44, 45] (1) frustrates operators, (2) triggers needless process deviation investigations, and (3) causes others to perceive that the process is not in control. This leads to a fundamental definition of an ideal alarm: that an ideal alarm represents an abnormal condition that requires a response.

Currently, alarm inflation greatly complicates an analysis required by an operator to understand the underlying causes of the alarms. This, in turn, creates two potential problems in process fault management. The first is that operators may ignore significant alarms. In a study of process alarm systems, Kortlandt [5,46] discovered that only 10% of the alarms in one plant caused operators to take corrective action. Of the other alarms, 50% were followed by no operator action whatsoever, while 40% resulted directly as a consequence of a previous operator action. Obviously, in such situations the effectiveness of the alarm systems to alert the operators to process problems is very low. Worse yet, this can lead to a situation in which the operators ignore activated alarms because they believe those alarms to be either unreliable or unimportant. Many plant accidents have resulted from just such operator behavior [10].

Alarm inflation (also referred to as *alarm floods*) [47] adds greatly to the problem known as *cognitive overload*. During major process upsets, hundreds or even thousands of alarms can become activated very quickly. This situation makes it very difficult for an operator to identify the most significant alarms and then diagnose the cause or causes of those alarms [46]. Consequently, alarm inflation defeats the original purpose of an alarm system, which is to help an operator assimilate more effectively the large amount of information coming into the control room [46] into an accurate model of the process state. This has led to efforts to create *smart alarms* [44, 45] or *intelligent alerts*.

These can (1) access all pertinent process information within a process control computer, (2) provide insight to operators as to the root cause, (3) display the expected operator response, and (4) link to paging systems.

Another method currently used to help operators perform process fault management is the addition of emergency interlock systems to a process control system. Since the role played by interlock systems in process safety was discussed earlier, only a few comments about their inherent limitations are given here. Interlock systems can be poorly designed, can be overridden by process operators, can fail, and can even be inconsequential in averting major catastrophes. Therefore, the mere existence of emergency interlock systems does not guarantee that process personnel and equipment will be protected completely.

The final method for helping operators perform process fault management is the creation of better control consoles and human-machine interfaces. Such consoles and interfaces are intended to help operators extract the most crucial information from a background of irrelevant information [6]. Better designs, along with more intelligent interpretation of the process data, appear to be the best means for dealing with problems of information overload. However, the problem with developing general interfaces is that the information operators need depends on the particular situation being confronted at that moment. For example, the information required by operators during process startup is different from the information they use to solve a problem during normal process operation. This makes it very difficult to design interfaces that are optimal for all possible situations.

Despite these efforts, inadequate fault management continues to cause major accidents within the chemical process industries. This is evident by the catastrophic accidents at Bhopal, India (1984), Mexico City, Mexico (1984), and São Paulo, Brazil (1984) [10]. It also represents a major problem for the nuclear power industry, as is evident by the accidents at power plants located at Three Mile Island, Pennsylvania (1979), and at Chernobyl in Ukraine (1987). Although these accidents have been widely publicized, the vast majority of plant mishaps have not. As a result, general lessons that could have been learned from these accidents are either never fully presented or are quickly forgotten [10]. In fact, many accidents have been caused by the same mistakes being repeated over and over. The most general lesson that can be learned from past incidents is that almost all plant accidents are preventable if the emergency situations preceding them are properly recognized and acted upon correctly.¹ At a minimum this requires proper recognition of those emergency

¹According to Duncan A. Rowan, a retired DuPont forensic investigator, the majority of the catastrophic accidents he investigated were caused by simple single-fault situations that were misinterpreted and responded to improperly by process operating personnel.

10 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

situations. Unfortunately, even this does not guarantee that fault management will be performed correctly.

1.5 LIMITATIONS OF HUMAN OPERATORS IN PERFORMING PROCESS FAULT MANAGEMENT

The preceding discussion has indicated that the various measures taken to improve process fault management do not always guarantee successful results; accidents still occur. One reason for this is that some of these measures are not always properly implemented or adequately maintained. Even if they are, these measures alone do not provide operators with sufficient support in all emergency situations. Moreover, it is extremely doubtful that measures guaranteed to provide such support can ever be developed. Human beings have certain inherent limitations that always cause their performance as process operators to be potentially unreliable.

One of these limitations is *vigilance decrement*. Studies have shown that human beings do not perform monitoring tasks very well. The number of things that go unnoticed increases the longer a person performs a given monitoring task [48]. With process operators, this phenomenon results directly from fatigue and boredom associated with control room duties in modern production plants. Automation has left process operators with fewer control functions to perform. This leads to both greater job de-skilling and dissatisfaction. This, in turn, causes boredom that leads to inattention. Since an inattentive operator will probably not have an accurate, up-to-date cognitive model of the process state when confronted with an emergency situation, he or she may mistakenly base decisions on an inaccurate model. Studies have also shown that the quality of a decision depends on the amount of time the decision maker has available. In an emergency situation, an inattentive operator will usually be forced to gather data and make decisions in less time than if he or she had been paying attention. Both of these situations will increase the likelihood of human error. Counteracting this limitation requires a means of relentlessly monitoring and analyzing a process state correctly. Since an agent performing such monitoring and analysis would always be aware of the actual process state, the agent would maximize the time available to the decision maker when process operating problems arise.

Another limitation of human operators is the phenomenon of *mind-set* [10], also known as *cognitive lockup*, *cognitive narrowing* [49], *tunnel vision* [46], and *point of no return* [43]. Sometimes when an operator becomes sufficiently certain of the cause of abnormal process behavior, she or he becomes committed exclusively to that hypothesis and acts upon it accordingly. This

commitment continues regardless of any additional evidence the operator receives which refutes that hypothesis or makes alternative hypotheses more plausible. In most cases, this additional evidence is ignored by the operator until it is too late to initiate proper corrective action [49]. Moreover, the longer an operator observes that the response of the system is not as would be expected, the harder that she or he tries to force it to be so [49]. Counteracting this limitation requires a means of examining all the available evidence in a rational, unbiased manner so that all plausible fault hypotheses consistent with that evidence can be derived. These hypotheses would have to be ranked according to how well they explained the process behavior observed, and this ranking would have to be updated as new evidence became available.

A third human limitation is the phenomenon of *cognitive overload*. Even when the detection of system failures is automatic, the sheer number of alarms in the first few minutes of a major process failure can bewilder operators [49]. Rapid transition of the process state may also do this, especially if operators have not experienced a similar situation and have not been told what to expect [4]. Both situations greatly increase the levels of stress experienced by those operators [50]. Under stressful situations, human beings lose information-processing capability. A direct consequence of this loss is that the operator may not be able to analyze the process state quickly and formulate the appropriate corrective response [41]. Counteracting this limitation requires a means for rapid, rational, and consistent analysis of the process state, regardless of how abnormal it is or how quickly it is changing. Such an analysis would focus the operator's attention on the most likely causes of the process behavior observed, rather than having to attempt to imagine all the possible causes of such behavior.

A fourth limitation of human operators is that the situation confronting them may require knowledge that is beyond their ability to understand [9] or outside the knowledge they have gained from their experience and training [10], or knowledge that they have forgotten [10]. Although operators are generally competent, they typically do not fully understand the underlying fundamental principles involved in the process system's design and operation [10]. Such knowledge is required so that the operators are more capable of flexible and analytical thought during emergency situations. This creates the somewhat paradoxical situation of the need for highly trained personnel to operate "automated" plants [6]. Counteracting this limitation requires a medium in which all pertinent information about the process system can be stored permanently and retrieved quickly. It also requires a method of determining which information is relevant to the solution of the problem currently confronting the process operator.

12 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

The final human limitation is that, even in the best of situations, humans make errors. Despite efforts intended to reduce such errors, human errors can never be totally eliminated. Sheridan [49] eloquently states the reason why:

Human errors are woven into the fabric of human behavior, in that, while not intending to make any errors, people make implicit and explicit decisions, based upon what they have been taught and what they have experienced, which then determines error tendencies.

He adds [49]:

The results of the human error may be subsequent machine errors, or it may embarrass, fluster, frighten, or confuse the person so that he is more likely to make additional errors himself.

Counteracting this limitation requires a means of storing the correct solutions to operating problems confronted in the past, correctly classifying the current plant situation as one of those problems, and then instantiating the appropriate stored solution with the current process state information. This would enable all the proper analyses performed in the past to be reused efficiently and systematically, thereby eliminating the need to recreate them each time they are required. It should also decrease the chances that the wrong analysis would be used or that the correct analysis would be used improperly.

1.6 THE ROLE OF AUTOMATED PROCESS FAULT ANALYSIS

Measures taken in the past to help operators perform process fault management have not been able to provide them with the support that they need for total elimination of process accidents. Typically, such accidents have had very simple origins [10,51]. These accidents have occurred because the number of possible process failures that need to be considered and the amount of process information that has to be analyzed commonly exceed those that an operator can cope with effectively in emergency situations.

Furthermore, this situation probably cannot be counteracted by additional investments in the various measures discussed previously. Many of these methods have already been developed to nearly their full potential. Thus, to further improve process safety, additional process fault management methods need to be developed to help address this problem directly.

An attractive approach to helping operators perform process fault management is to automate the analysis required to determine the cause or causes of abnormal process behavior: that is, to automate process fault analysis.

Not surprisingly, strategies for automating fault diagnosis in chemical and nuclear process plants have been proposed for nearly as long as computers have been used in process control. However, at the present time, the potential of the process control computers to analyze process information for such purposes is still relatively unexploited [14]. The reasons for this are discussed in Appendix A.

Automated process fault analysis should be used to augment, not replace, human capabilities in process fault management. Consider the relative strengths and weaknesses of automated analysis compared with human analysis. Computers can outperform humans in doing numerous, precise, and rapid calculations and in making associative and inferential judgments [49]. On the other hand, people are better at functions that cannot be standardized. They are also better at decision making that has not been adequately formalized (i.e., creative thought) and in coordinations that involve the integration of a great many factors whose subtleties or nonquantifiable attributes defy computer implementation [1]. These differences need to be kept in mind when designing automated fault analyzers.

Currently, the computer offers a means to analyze process information rapidly in a systematic and predetermined manner. If such analysis is already being done by the operators, automating the analysis would free them to perform other functions. If it is not being done, it could be because the operators do not have either sufficient time or the capabilities required. In either case, proper automation of such analysis should make the information reaching the operators more meaningful [2]. Thus, the main advantage of real-time online fault analysis is to reduce the cognitive load on operators [52], to allow them to concentrate on those analyses that require human judgment.

1.7 ANTICIPATED FUTURE CPI TRENDS

The preceding discussion has indicated how automated process fault analysis can be used to help operators better perform process fault management. The main reasons that such automation will continue to increase have to do with the trends predicted for the CPI [53].

Two of these trends are toward an increased emphasis on quality control and process optimization. Both trends will require that a given process system be operated under tighter control limits. It will thus become more important to detect and correct incipient failures long before they cause major operating problems. The sensitivity analysis required to do this will probably have to be much greater than that which can be performed continuously by even the best human operators.

14 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

Another trend predicted within the chemical industry is toward more flexible plants operated over a wider range of operating conditions and producing a wider variety of products. This will make it more difficult for operators to perform fault management because they will have had much less operating experience than in the past with any particular process system or set of operating conditions. With less experience on which to base their decisions, it will be more difficult for operators to determine if observed process behavior is normal and to determine the underlying cause or causes when it is not.

Two other trends predicted are toward specialty product manufacturing and shorter product life cycles. Again, both trends will probably make it more difficult for the operators to perform effective fault management because they will have had much less operational experience with these processes.

It is possible that some of the current problems in process fault management could be counteracted by replacing operators with more highly trained process engineers. The higher wages paid to the engineers would be offset by their more effective operation of the process system. Nonetheless, since engineers are subject to the same human limitations as process operators, doing this would only postpone the need to directly address the problems discussed above. Consequently, it is our contention that automating process fault analysis represents the best currently unexploited means available to address these problems directly. A generalized model-based methodology for optimal automation of process fault analysis is the *method of minimal evidence* (MOME), described in detail later. First, we define some of the concepts associated with process fault analysis that are used throughout our discussion.

1.8 PROCESS FAULT ANALYSIS CONCEPT TERMINOLOGY

The terms *fault* and *fault situation* refer to the actual event that is creating either a potential or an actual process operating problem. In contrast, the term *symptom* refers to observable manifestations of fault situations and to observable manifestations of nonfault events. For example, a stuck valve is considered a fault situation whether or not it affects process operation in any observable way. Furthermore, if the valve causes a high-temperature alarm, for example, the alarm is considered a symptom of that fault situation. It might also be a symptom of many other fault situations and nonfault events.

Diagnostic evidence refers to any symptom that supports the plausibility of one or more fault hypotheses. This evidence may also support the plausibility of any number of nonfault hypotheses. Diagnostic evidence is based on information obtained from the current operating behavior of the target process system. This current process information is refined into diagnostic evidence through the application of knowledge regarding a process system's

normal operating behavior. It will be assumed that only the values of the process variables measured directly by process sensors at a constant sampling frequency are used to create diagnostic evidence. This assumption is made for convenience and will not affect the generality of the following discussion whatsoever.

A *target process system* is that portion of the entire system being actively analyzed for process fault situations by the fault analyzer.

A *process operating event* is any occurrence that affects a process system's normal operating behavior sufficiently to generate symptoms. Such occurrences can be actual process fault situations such as pump failures or stuck valves, or nonfault events such as normal process startups and shutdowns or production rate changes. Any combination of process fault situations and nonfault events is also considered a process operating event.

A fault analyzer's *intended scope* is that subset of potential process operating events that the fault analyzer is designed explicitly to correctly identify and classify. By definition, a fault analyzer's intended scope includes its *target fault situations*, those potential process fault situations that the fault analyzer is specifically designed to detect and diagnose. The intended scope is constrained by the fault analyzer's *intended operational domain*, which specifies the process operating states that the fault analyzer can analyze for its target fault situations: for example, all possible process production levels and steady- and unsteady-state operation.

Classifying a process operating event correctly means that the fault analyzer can properly discriminate that event from all other possible events (i.e., the fault analyzer will not misdiagnose that event as another). According to this definition, to operate properly the fault analyzer does not necessarily have to identify a process operating event explicitly; it just has not to misidentify that event. Thus, to classify an event correctly, the fault analyzer has to either diagnose that event as the fault that is occurring or to misdiagnose it by not making any diagnosis whatsoever (i.e., by remaining silent). Performing in this conservative manner is advantageous because it will not distract or confuse operators during emergency situations.

A fault analyzer's competence refers to how correctly it classifies the various possible process operating events contained within its intended scope. A fault analyzer that can classify all of these events correctly is considered *completely competent*.

A fault analyzer's competence can be quite different from its *robustness*, which refers to how correctly a fault analyzer can classify the various process operating events that actually occur during a target process system's operation. Consequently, a fault analyzer's competence is related to how well its performance lives up to its design specifications, whereas its robustness is an indication of how useful those design specifications actually are for the target

16 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

process system. A fault analyzer's competence will approach its robustness, as its intended scope includes more of the operating events that can actually occur during the process system's operation.

A fault analyzer's *diagnostic resolution* is the level of discrimination between a particular fault situation and all other possible process operating events. *Perfect resolution* refers to those fault situations that can be uniquely discriminated from all other possible process operating events contained within the fault analyzer's intended scope.

A fault analyzer's *diagnostic sensitivity* for a particular fault situation refers to the minimum values of that fault situation's magnitude or rate of occurrence that can be detected and diagnosed correctly. These values depend directly on the current process operating conditions and the degree of diagnostic resolution sought. Fault situations that have magnitudes and/or rates of occurrence at or above a fault analyzer's minimum diagnostic sensitivity are considered *significant* with respect to the fault analyzer.

A fault analyzer's *diagnostic response time* is the interval between the onset of a significant process operating event and its diagnosis by the fault analyzer. It is thus the interval required to expose the complete pattern of symptoms used by the fault analyzer to diagnose its associated faults.

Finally, a fault analyzer's *utility* is a measure of the usefulness derived from its diagnoses by process operators. Utility is thus a composite metric of the fault analyzer's competence and robustness and also its possible diagnostic resolution, sensitivity, and response time for identifying each of its covered process operating events.

REFERENCES

1. Lefkowitz, I., "Hierarchical Control in Large Scale Industrial Systems," in *Studies in Management Science and Systems*, Vol. 7, North-Holland, New York, 1982, pp. 65–98.
2. De Heer, L. E., "Plant Scale Process Monitoring and Control Systems: Eighteen Years and Counting," in *Proceedings of the First International Conference on Foundations of Computer Aided Process Operations*, ed. by G. V. Reklaitis and H. D. Spriggs, Elsevier Science, New York, 1987, pp. 33–66.
3. Syrbe, M., "Automatic Error Detection and Error Recording of a Distributed Fault-Tolerant Process Computer System," in *Human Detection and Diagnosis of System Failures*, ed. by J. Rasmussen and W. B. Rouse, Plenum Press, New York, 1981, pp. 475–486.
4. Linhou, D. A., "Aiding Process Plant Operators in Fault Finding and Corrective Action," in *Human Detection and Diagnosis of System Failures*, ed. by J. Rasmussen and W. B. Rouse, Plenum Press, New York, 1981, pp. 501–522.

REFERENCES 17

5. Rijnsdorp, J. E., "The Man-Machine Interface," *Chemistry and Industry*, May 1986, pp. 304-309.
6. Visick, D., "Human Operators and Their Role in an Automated Plant," *Chemistry and Industry*, May 1986, pp. 199-203.
7. Kohan, D., "The Design of Interlocks and Alarms," *Chemical Engineering*, February, 1984, pp. 73-80.
8. Lees, F. P., "Computer Support for Diagnostic Tasks in the Process Industries," in *Human Detection and Diagnosis of System Failures*, ed. by J. Rasmussen and W. Rouse, Plenum Press, New York, 1981, pp. 369-388.
9. Goff, K. W., "Artificial Intelligence in Process Control," *Mechanical Engineering*, October 1985, pp. 53-57.
10. Kletz, T. A., *What Went Wrong?: Case Histories of Process Plant Disasters*, Gulf Publishing, Houston, TX, 1985.
11. Barclay, D. A., "Protecting Process Safety Interlocks," *Chemical Engineering Progress*, Vol. 84, No. 2, February 1988, pp. 20-24.
12. "Chemical Industry to Act on Safety," *Processing*, December 1985, p. 19.
13. O'Shima, E., "Computer Aided Plant Operation," *Computers and Chemical Engineering*, Vol. 7, No. 4, 1983, pp. 311-329.
14. Venkatasubramanian, V., "Process Fault Detection and Diagnosis: Past, Present, and Future," *Proceedings of CHEMFAS4*, Seoul, Korea, 2001, pp. 3-15.
15. Nimmo, I., "Adequately Address Abnormal Operations," *Chemical Engineering Progress*, September 1995, pp. 36-45.
16. Lees, F. P., *Loss Prevention in the Process Industry*, Butterworth, London, 1980.
17. Duxbury, H. A., and M. L. Preston, "The Process Systems Contribution to Process Safety," in *Proceedings of the First International Conference on Foundations of Computer Aided Process Operations*, ed. by G. V. Reklaitis and H. D. Spriggs, Elsevier Science, New York, 1987, pp. 177-198.
18. Arendt, J. S., and M. L. Casada, "Prisim: An Expert System for Process Risk Management," Paper 82e, presented at the *AIChE Spring National Meeting*, Houston, TX, April 1987.
19. Arueti, S., W. C. Gekler, M. Kazarians, and S. Kaplan, "Integrated Risk Assessment Program for Risk Management," Paper 83e, presented at the *AIChE Spring National Meeting*, Houston, TX, April 1987.
20. Venkatasubramanian, V., and R. Vaidhyanathan, "A Knowledge-Based Framework for Automating HAZOP Analysis," *AIChE Journal*, Vol. 40, No. 3, 1994, pp. 496-505.
21. Vaidhyanathan, R., and V. Venkatasubramanian, "Experience with an Expert System for Automated HAZOP Analysis," *Computers and Chemical Engineering*, Vol. 20, Suppl. B, 1996, pp. S1589-S1594.
22. Suh, J. C., S. Lee, and E. S. Yoon, "New Strategy for Automated Hazard Analysis of Chemical Plants: Part 2. Reasoning Algorithm and Case Study," *Journal of Loss Prevention in the Process Industries*, Vol. 10, No. 2, 1997, pp. 127-134.

18 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

23. Venkatsubramanian, V., J. S. Zhao, and S. Viswanathan, "Intelligent Systems for HAZOP Analysis of Complex Process Plants," *Computers and Chemical Engineering*, Vol. 24, No. 9–10, 2000, pp. 2291–2302.
24. Kang, B., E. S. Yoon, and J. C. Suh, "Application of Automated Hazard Analysis by New Multiple Process-Representation Models to Chemical Plants," *Industrial and Engineering Chemistry Research*, Vol. 40, No. 8, 2001, pp. 1891–1902.
25. Zhao, C., M. Brushan, and V. Venkatsubramanian, "Phausuite: An Automated HAZOP Analysis Tool for Chemical Processes: Part I. Knowledge Engineering Framework," *Process Safety and Environmental Protection*, Vol. 83, No. B6, 2005, pp. 509–532.
26. Zhao, C., M. Brushan, and V. Venkatsubramanian, "Phausuite: An Automated HAZOP Analysis Tool for Chemical Processes: Part II. Implementation and Case Study," *Process Safety and Environmental Protection*, Vol. 83, No. B6, 2005, pp. 533–548.
27. Cui, L., J. Zhao, T. Qui, et al., "Layered Diagraph Model for HAZOP Analysis of Chemical Processes," *Process Safety Progress*, Vol. 27, No. 4, 2008, pp. 293–305.
28. Wang, H., B. Chen, X. He, et al., "A Sign Digraphs Based Method for Detecting Inherently Unsafe Factors of Chemical Processes at Conceptual Design Stage," *Chinese Journal of Chemical Engineering*, Vol. 16, No. 1, 2008, pp. 52–56.
29. Zhao, J., L. Cui, L. Zhao, et al., "Learning HAZOP Expert System by Case-Based Reasoning and Ontology," *Computers and Chemical Engineering*, Vol. 33, No. 1, 2009, pp. 371–378.
30. Rahman, S., F. Khan, and B. Veitch, "ExpHAZOP(+): Knowledge-Based Expert System to Conduct Automated HAZOP," *Journal of Loss Prevention in the Process Industries*, Vol. 22, No. 4, 2009, pp. 373–380.
31. Wang, H., B. Chen, X. He, et al., "SDG-Based HAZOP Analysis of Operating Mistakes for PVC Process," *Process Safety and Environmental Protection*, Vol. 87, No. 1, 2009, pp. 40–46.
32. Groen, F. J., C. Smidts, and A. Mosleh, "QRAS: Quantative Risk Assessment System," *Reliability Engineering and System Safety*, Vol. 91, No. 3, 2006, pp. 292–304.
33. Meel, A., and W. D. Seider, "Plant Specific Dynamic Failure Assessment Using Baysian Theory," *Chemical Engineering Science*, Vol. 61, No. 21, 2006, pp. 7036–7056.
34. Meel, A., and W. D. Seider, "Real Time Risk Analysis of Safety Systems," *Computers and Chemical Engineering*, Vol. 32, No. 4–5, 2008, pp. 827–840.
35. Wilson, R. L., Jr., "Back to Basics: Redefining the Mission Planning in an Automated World," in *Proceedings of the First International Conference on Foundations of Computer Aided Process Operations*, ed. by G. V. Reklaitis and H. D. Spriggs, Elsevier Science, New York, 1987, pp. 253–276.
36. Grievink, J., K. Smit, R. Dekker, and C. F. H. van Rijn, "Managing Reliability and Maintenance in the Process Industry," in *Proceedings of the Second International Conference on Foundations of Computer Aided Process Operations*, ed. by

- D. W. T. Rippin, J. C. Hale, and J. F. Davis, CACHE, Inc., Austin, TX, 1994, pp. 133–157.
37. Yang, S. K., “A Condition-Based Failure Prediction and Processing Scheme for Preventive Maintenance,” *IEEE Transactions on Reliability*, Vol. 52, No. 3, 2003, pp. 373–383.
38. Peng, Y., M. Dong, and M. J. Zuo, “Current Status of Machine Prognostics in Condition-Based Maintenance: A Review,” *International Journal of Advanced Manufacturing Technology*, Vol. 50, No. 1–4, 2010, pp. 297–313.
39. Mundo, K. J., “Reliability of Chemical Plants,” *Large Scale Systems*, ed. by Y. Haines, North-Holland, New York, 1982, pp. 55–67.
40. Williams, G. P., W. W. Hoehing, and R. G. Byington, “Causes of Ammonia Plant Shutdowns: Survey V,” *Plant/Operations Progress*, April 1988, pp. 99–110.
41. Dellner, W. J., “The User’s Role in Automated Fault Detection and System Recovery,” in *Human Detection and Diagnosis of System Failures*, ed. by J. Rasmussen and W. B. Rouse, Plenum Press, New York, 1981, pp. 487–499.
42. Ducan, K. D., “Training for Fault Diagnosis in Industrial Process Plants,” in *Human Detection and Diagnosis of System Failures*, ed. by J. Rasmussen and W. B. Rouse, Plenum Press, New York, 1981, pp. 553–573.
43. Rasmussen, J., “Models of Mental Strategies in Process Plant Diagnosis,” in *Human Detection and Diagnosis of System Failures*, ed. by J. Rasmussen and W. B. Rouse, Plenum Press, New York, 1981, pp. 251–258.
44. Alford, J. S., J. Kindervater, and R. Stankovich, “Alarm Management for Regulated Industries,” *Chemical Engineering Progress*, No. 4, April 2005, pp. 25–30.
45. Alford, J. S., “Bioprocess Control: Advances and Challenges,” *Computers and Chemical Engineering*, Vol. 30, 2006, pp. 1464–1475.
46. Lees, F. P., “Process Computer Alarm and Disturbance Analysis: Review of the State of the Art,” *Computers and Chemical Engineering*, Vol. 7, No. 6, 1983, pp. 669–694.
47. Crowe, R., “Abnormal Situation Management,” *Chemical Engineering Progress*, April 2002, p. 77.
48. Eberts, R. E., “Cognitive Skills and Process Control,” *Chemical Engineering Progress*, December 1985, pp. 30–34.
49. Sheridan, T. B., “Understanding Human Error and Aiding Human Diagnostic Behaviour in Nuclear Power Plants,” in *Human Detection and Diagnosis of System Failures*, ed. by J. Rasmussen and W. B. Rouse, Plenum Press, New York, 1981, pp. 19–35.
50. Fortin, D. A., T. B. Rooney, and H. Bristol, “Of Christmas Trees and Sweaty Palms,” in *Proceedings of the Ninth Annual Advanced Control Conference*, West Lafayette, IN, 1983, pp. 49–54.
51. Lieberman, N. P., *Troubleshooting Process Operations*, PennWell Publishing, Tulsa, OK, 1985.

20 MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

52. Laffey, T. J., P. A. Cox, J. L. Schmidt, S. M. Kao, and J. Y. Read, "Real-Time Knowledge Based Systems," *AI Magazine*, Spring 1988, p. 27.
53. Schlenker, R. P., Keynote Address: "Process Industry Automation: The Challenge of Change," in *Proceedings of the First International Conference on Foundations of Computer Aided Process Operations*, ed. by G. V. Reklaitis and H. D. Spriggs, Elsevier Science, New York, 1987, pp. 1–26.