

---

# MOTIVATIONS FOR AUTOMATING PROCESS FAULT ANALYSIS

---

Richard J. Fickelscherer, PE

*Department of Chemical and Biological Engineering, State University of New York at Buffalo,  
Buffalo, New York, USA*

## OVERVIEW

This introductory chapter to our treatment establishes and briefly discusses the current motivations for directly automating process fault analysis. It begins by listing the various traditional methods currently employed for helping human operators perform more effective process fault management. Human limitations at actually performing such management are then enumerated. Also the advantages of human analysis versus those that computer automation currently possesses are compared. This comparison is made in order to identify the most feasible approaches/best possible pathways presently existing for actually automating process fault analysis. Please note that the literature references cited in this discussion (as well of those cited throughout the remainder of this treatment's various chapters and appendices written or co-written by me) are chosen because they are the earliest

---

*Artificial Intelligence in Process Fault Diagnosis: Methods for Plant Surveillance,*  
First Edition. Edited by Richard J. Fickelscherer.

© 2024 John Wiley & Sons, Inc. Published 2024 by John Wiley & Sons, Inc.

mention of their respective particular observations that I have encountered in the open literature. These “old” citations are consequently meant to recognize and properly bestow the corresponding appropriate intellectual credit to those original pioneers in this continuing evolution of automated process fault analysis.

## CHAPTER HIGHLIGHTS

- Discussion of the changing role of human operators in modern processing plants.
- Overviews of various traditional process fault management methods that are currently being employed by the processing industries in order to address these changes.
- Descriptions of various human limitations encountered when actually performing process fault management.
- Comparisons between human-based and current computer-based analysis advantages.
- Current major motivations for further developing automated process fault analysis.

### 1.1 INTRODUCTION

Economic competition within the chemical process industries (CPI) has directly led to the construction and operation of larger, highly integrated and more fully automated production plants. As a result, the primary functions performed by the human process operators in these plants have changed. An unfortunate consequence of these changes is that those operators’ ability to perform process fault management has been diminished.<sup>1</sup> The underlying

<sup>1</sup>Dr. Joseph S. (Joe) Alford, PE, a retired control engineer, contends that this is not necessarily a universal situation based on his experience at Eli Lilly and Co. There, as computers took over the defined routine repetitive jobs that operators used to do in the manufacturing plants (e.g., manually walk the plant and collect data on clip boards), the company chose not to lay off operators, but rather to train them to use more of their natural intelligence (rather than just do rote jobs) and so trained them to be more involved in routine data analysis, process troubleshooting and fault management. So Lilly never directly laid off operators when automating their plants; instead they just used operators in more intelligent ways. This created a win-win situation for all involved. Operators liked their jobs more as that they felt their brains were being used and valued. Subsequently, process faults were better managed.

reasons behind this potentially highly dangerous situation and the various methods currently being used to counteract it are discussed here.

One continuing major trend driving the present modernization of the CPI has been the evermore increasing automation of all process control functions. The motivation for such automation is that it results in more accurately applying the best available process control strategies in a continuous, consistent, and dependable manner (Lefkowitz 1982; De Heer 1987). 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 (Lefkowitz 1982). Advancing process control computers have also provided a significant means for dealing with the diverse and complex information required to effectively operate a modern production plant (De Heer 1987). Together with continuing improvements in electronic instrumentation, these developments are directly allowing these plants to still operate effectively with considerably fewer human operators (Lefkowitz 1982).<sup>2</sup>

Another continuing trend for reducing CPI operating costs has been to maximize the availability of modern plants 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 currently used to either eliminate or minimize the severity of unexpected production disruptions. None the less, as the complexity of the processing plants has increased, making these plants available for production has become much more difficult because the number of potential operating problems has also increased (Syrbe 1981). This tends to increase the frequency of unexpected production disruptions. Consequently, maximizing these plants availability for efficient process operation has become more dependent upon effectively managing their various potential operating problems (Linhou 1981).

<sup>2</sup>Joe Alford's experience has been that while it is true that many companies choose to operate plants with fewer operators as automation increases – it is not always the case. Operator jobs can be transformed so they have greater roles in FMEAs, alarm rationalization teams, process deviation investigations, real-time fault diagnosis, certain data analysis functions, helping schedule detailed operations, etc., such that they no longer have to fear for loss of their job but can look forward to their job becoming more interesting, challenging, and intellectually diverse.

## 1.2 THE CHANGING ROLE OF THE PROCESS OPERATORS IN PLANT OPERATIONS

The process operators' main task in plant operation is to continuously assess the process state (Lefkowitz 1982) and then, based upon that assessment, react appropriately. Process operators thus have three core primary responsibilities (Rijnsdorp 1986). The first is to monitor the performance of various control loops to make sure that the process is operating properly. Their second is to make adjustments to the process operating conditions whenever product quality or production efficiency fall outside predefined tolerance limits. The operators' third, and by far most important, responsibility is to avoid emergency situations if at all possible, and if not, properly respond to them.<sup>3</sup> This means effectively and reliably performing process fault management. Such management requires that the operators correctly detect, identify, and then implement the necessary counter actions required to eliminate the process fault or faults creating the emergency situation. If it is performed incorrectly, accidents can and have occurred on many occasions.<sup>4</sup>

<sup>3</sup>Lieven DuBois observes that alarm systems are currently set up to avoid safety functions, safety systems and emergency shut-down systems being activated; i.e., all these systems are designed to avoid emergency situations. But when activated they lead inevitably to down time, off-spec quality, energy losses, waste, flaring, etc. One of the key aspects in responding to alarms, according to EEMUA 191, is that the operator should diagnose the root cause of the alarmed situation, which means performing (process and equipment) fault management.

<sup>4</sup>Joe Alford observes that this is true for those plants that are generally continuous in nature: i.e., the above list of operator roles appears to be generally accurate in those plants. However, an estimated half of all manufacturing plants are batch in nature. In most batch plants, there are a large number of manual operations and thus these plants are more "semi-automated" than completely automated. So, for many batch plants, procedures are a combination of manual operations and automated operations. For example, in sterilizing a bioreactor, the overall control is automated, but still requires operators to manually check the large number of feed, sample, and other piping connected to the bioreactor with temp sticks or other temperature measurement devices to verify that they are achieving the desired sterilization temperature. In other batch operations, operators need to manually hook up different pieces of equipment to one another to prepare for an upcoming batch run or transfer of materials. In other unit operations, operators are changing the resin in chromatography separation columns in preparation for the next batch. And, with almost all batch processes, manual cleaning of equipment is needed after each batch. And the list goes on. The number of manual operations that operators must perform in many batch plants is such that the central control room is frequently not manned as the operators are out in the field performing manual operations. (Hence there is the critical need for remote alarming systems.)

The biggest change in the functions performed by the process operators has been directly caused by the increased automation of process control. Process operators now monitor and supervise, rather than manually control, process operations. Moreover, such functions are increasingly accomplished with interface technology designed to centralize control and information presentation (Visick 1986). As a result, their duties have become less interesting and their ability to manually control the process has diminished.<sup>5</sup> Both situations have increased the job dissatisfaction experienced by the process operators (Visick 1986). This has also directly diminished the operators' ability to perform process fault management.<sup>6</sup>

A second change in the functions performed by the operators has directly resulted from having fewer operators present in modern processing plants. Each operator has become responsible for a larger portion of the overall process system's production. 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. Besides their increased risk, the potential severity of these possible accidents has also increased because larger quantities of reactive materials and energy are now being processed. This makes the operators' ability to perform effective process fault management much more critical for ensuring the safe operation of those plants.

One method used to help reduce the risk of a major accident has been the addition of emergency interlock systems to the overall process control strategy. Such systems are designed to automatically shut down the process during dangerous emergency situations, thereby reducing the likelihood of accidents occurring that could directly threaten human and environmental safety or damage the process equipment. Emergency interlock systems therefore help ensure that the process operation is safe during such emergencies by decreasing the effects of human error in such situations

<sup>5</sup>Joe Alford has not found this to be true in his experience; i.e., the operators' ability to manually do process control has not diminished as long as automated systems stick with simple single input, single output, PID feedback controllers. It is when control engineers start implementing algorithms like model predictive control that the operators' ability to do process control diminishes. But then again, he contends most process engineers can't effectively support model predictive controllers either. These controllers are sometimes just too complex and challenging to configure and properly support.

<sup>6</sup>Lieven DuBois believes that because automated and advanced control is built in or on top of basic process control systems, the role of the operator has changed. Nowadays an operator oversees more control loops, more measurements (instruments) and more equipment than ever before. It thus has become humanly impossible to learn and remember all possible faults and all potential consequences of such faults.

(Kohan 1984).<sup>7</sup> Eliminating any accidents also protects the operational integrity of the process system, which in turn allows it to be restarted more quickly after these automatic shutdowns.

However, the wide-spread 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 (Lees 1981). In emergency situations, the operators are now more concerned with taking the corrective actions required for continuing to keep the process system operating rather than those which will safely shut it down. They rely upon the interlock system to handle any 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, in order to keep the process system operating, the operators may take actions that counteract the symptoms of a fault situation without correcting that situation itself (Goff 1985). Such behavior by the operators may cause them to inadvertently circumvent the protection of the emergency interlock system, thereby creating a situation which they falsely believe to be within that protection. Another potential problem of this strategy is that the emergency interlock system may fail, which again will create a situation in which the operators falsely believe that the process system is still protected by it. These potential problems can be reduced by: (i) prudently designing those interlock systems, (ii) being certain to add sufficient redundancy to detect critically dangerous situations (Kohan 1984), (iii) establishing formal policy by which particular interlocks can be bypassed during process operation (Kletz 1985), and (iv) adequately maintaining those interlock systems (Barclay 1988).<sup>8</sup>

In summary, the automation of the required process control actions and of emergency process shutdowns has shifted the operators' main activities away from direct process control to that of passive process monitoring. Moreover, this 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 always perform the most competent process fault management has been reduced. Unfortunately, this reduction

<sup>7</sup>Lieven DuBois notes that since then these systems have evolved drastically. However, some companies allow process operators to sometimes by-pass these interlock systems to keep the plant production running. These by-passes have directly led to disasters (e.g., BP Deep Water Horizon (2010)).

<sup>8</sup>From an ISA (International Society of Automation) perspective, interlocks are part of a broader paradigm known as "Safety Instrumented Systems" (SIS) which are governed by ISA, ANSI, and IEC standards (e.g., ANSI/ISA 84 on Safety Instrumented Systems).

has occurred during an era 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 the human operators' capability to perform effective process fault management.

### **1.3 TRADITIONAL METHODS FOR PERFORMING PROCESS FAULT MANAGEMENT**

A variety of methods have been previously developed either to directly reduce the occurrence of process faults or to directly help the operators perform process fault management more effectively whenever it is required. The traditional methods currently utilized to reduce the occurrence of process faults include: (i) initially designing the process systems with greater operational safety in mind (e.g., by performing comprehensive FMEA and HAZOP studies), (ii) constructing process plants with higher quality, and therefore more reliable, process equipment, (iii) implementing comprehensive programs of preventative maintenance, and (iv) establishing and strictly following standard operating procedures and change control. The methods currently relied upon to directly help the operators perform process fault management include: (i) extensively training the operators in process fault management, (ii) increasing the effectiveness of alarm deployment strategies, (iii) designing better control consoles and man-machine interfaces, (iv) employing simple data analytics to, for example, discover cause/effect relationships, and (v) as a last resort safety measure, adding emergency interlock systems to the process control systems for the reasons previously discussed.

Despite these efforts, inadequate fault management continues to cause major accidents within the CPI. This is evident by the catastrophic accidents at Flixborough, England (1974), Bhopal, India (1984), Mexico City, Mexico (1984), and Sao Paulo, Brazil (1984) (Kletz 1985), Pasadena, Texas (1989), Texas City, Texas (2005), Jacksonville, Florida (2007), Port Wentworth, Georgia (2008), and Geismer, Louisiana (2013). It also represents a major problem for the Nuclear Power Industry, as is evident by the accidents at the power plants located in Three Mile Island, Pennsylvania (1979) and Chernobyl, Ukraine (1987). While the above disasters have been widely publicized, the vast majority of plant mishaps have not. As a result, the general lessons which could have been learned from these accidents are either never fully presented or are quickly forgotten (Kletz 1985). In fact, many accidents have been caused by the same mistakes being repeated over and

over again.<sup>9</sup> The most general lesson that can be learned from the past incidents is that almost all plant accidents are preventable if the emergency situations preceding them are properly recognized and correctly acted upon.<sup>10</sup> At a minimum this requires properly recognizing those emergency situations. Unfortunately, as discussed next, even this does not guarantee that fault management will always be performed correctly.

## 1.4 LIMITATIONS OF HUMAN OPERATORS IN PERFORMING PROCESS FAULT MANAGEMENT

The preceding discussion has indicated that the various measures currently being taken to improve process fault management do not always guarantee successful results: accidents still occur. One reason for this is that some of

<sup>9</sup>In addition to the above recognized incidents, Steve Apple points out that there are very many that have not been officially reported or noticed, i.e., there are a far greater number of un-reported near-misses. He believes the non-reporting is really a function of the litigious society in which we are living. What large manufacturer wants to notify the public that they almost blew up the neighborhood a couple of times last week? And they even go to great lengths to hide these incidents internally. As a result, tribal learning is lost, as these events are not recorded and learned from unless they are terribly harrowing. And future events that could have been avoided are left to the fate of the operator's ability to diagnose from very little information or knowledge of previous occurrences. For instance, years ago in dealing with a large company who had an incident in Bhopal, India (just for example), he discovered new company policies in place. He was trying to gather plant data for empirical modeling efforts. Their established policy as a result of that incident was that they were ordered to destroy any process data more than 90 days old. This is not currently still the case, but it lasted for several years until process engineers were able to prove the historical value of that data was greater than the risk of it remaining available.

As one final point on this topic, Steve Apple has actually been in control rooms where operators were bypassing safety systems on start-up or shut down. In fact, they were purposely bypassing systems designed to protect against unit failure for limited periods of time because "that's how they had always done it." The catastrophe at Texas City, Texas (2005) is just one example of this sort of risky practice. The operators had traditionally allowed a level limit to be bypassed on starting up the unit. When the second sensor that told them it was time to reduce the flow to that unit failed, they were captured in a "point of no return" situation that they could not recover from. The extensive re-design and instrumentation that would have been necessary to avoid this situation was painful enough that engineers simply turned their heads and allowed this practice to continue. It was not an everyday event- just on startup and they assumed it had a backup sensor to prevent failure. Boom!

<sup>10</sup>According to Duncan A. Rowan, PE, a retired DuPont forensic investigator, the majority of the catastrophic accidents he investigated during his career were caused by simple single fault situations that were misinterpreted and improperly responded to by process operating personnel.

these measures are not always properly implemented nor adequately maintained. Even if they are, these measures alone still do not provide the operators with sufficient support in all emergency situations. Moreover, it is extremely doubtful that the measures guaranteed to provide such perfect support can ever be developed. Humans just have certain inherent limitations that cause their performance as process operators to be potentially unreliable.

One of these limitations is known as **“vigilance decrement.”** Studies have shown that humans do not perform monitoring tasks very well. The number of things which go unnoticed increases the longer a human performs a given monitoring task (Eberts 1985). 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. That in turn causes boredom which could lead to inattention. Since an inattentive operator will probably not have an accurate, up-to-date cognitive model of the present process state when confronted with an emergency situation, they may mistakenly base their decisions upon an inaccurate model. Studies have also shown that the quality of a decision depends upon the amount of time the decision maker has. In an emergency situation, an inattentive operator will usually be forced to gather data and make their decisions in less time than if they had been paying full attention. Both of these situations will increase the likelihood of human error. Counteracting this limitation requires a means for relentlessly monitoring and correctly determining the actual process state. Since the agent performing that surveillance would always be aware of this true state, such an agent would maximize the time available to the decision maker when process operating problems arose.

Another limitation of human operators is a phenomenon called **“mind set”** (Kletz 1985), which is also known as **“cognitive lockup”** and **“cognitive narrowing”** (Sheridan 1981), **“tunnel vision”** (Lees 1983), and **“the point of no return”** (Rasmussen 1981). Sometimes when an operator becomes sufficiently certain as to the cause of abnormal process behavior, they become exclusively committed to that particular hypothesis and acts upon it accordingly. This commitment continues regardless of any additional evidence that they receive which refutes that hypothesis or which makes alternative hypotheses more plausible. In most of the cases, this additional evidence is actively ignored by the operator until it is too late for him to initiate the proper corrective actions (Sheridan 1981). Moreover, the longer the operator observes that the response of the system is not as they would expect, the harder they try to force it to be so (Sheridan 1981). Counteracting this limitation requires a

means for 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 observed process behavior, and this ranking would have to be updated as new evidence became available.

A third human limitation is the phenomenon known as “**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 the process operators (Sheridan 1981).<sup>11</sup> Rapid transition of the process state may also do this, especially if those operators have not experienced a similar situation and have not been told what to expect (Linhou 1981). Both situations greatly increase the levels of stress experienced by those operators (Fortin et al. 1983). Under stressful situations, humans lose information processing capability. A direct consequence of this loss is that the operator may not be able to quickly determine the true process state and formulate the appropriate corrective response (Dellner 1981). Counteracting this limitation requires a means for rapidly, rationally, and consistently correctly determining the true process state, regardless of how abnormal it is or how quickly it is changing. Such an analysis would thus help focus the operator’s attention on the most likely causes of the observed process behavior, rather than having them attempt to imagine all of the possible causes of such behavior.<sup>12</sup>

<sup>11</sup>Lieven DuBois points out that since alarm management standards have been accepted (by regulators), the number of alarms occurring during abnormal situations have been steadily decreased by using different techniques. Some of these improvements are discussed in greater detail in Chapters 3–5.

<sup>12</sup>In support of the above, a major factor then in many, if not most, emergency situations is from the resulting information overload presented to the operator. Joe Alford contends that this overload originates directly from the way automation engineers configure the overall control system (i.e., not following best practices). Information overload has been cited as a factor in most of the major accidents mentioned earlier. The point here is that poor performance in dealing with emergency situations is often not the fault of the operator – as operators are often confronted with a myriad of alarms and alerts and other information messages, often not prioritized – so they have little chance of quickly sorting through the mountain of information, blinking lights, and blaring horns that occur when abnormal situations are occurring. ISA/ANSI standards such as 18.2 (Alarm Management) and 101 (Man Machine Interfaces) are tools that should be utilized by engineers to create a more optimal environment for helping operators manage emergency situations.

Thus, one of the unintended consequences of increased automation in processing plants is the ease and low cost (essentially free) of adding alarms, alerts, and information messages for operators. Consequently, control engineers end up just configuring lots and lots of them. So, when dealing with managing abnormal situations, more focus needs to be directed to the control engineers that are making a bad situation worse by the huge amount of information they have their control system designs generate during an incident, often including many nuisance alarms.

A fourth limitation of human operators is that the situation confronting them may require knowledge that is either beyond their ability to understand (Goff 1985), that is, outside the knowledge that they have gained from their experience and training (Kletz 1985), or that they have forgotten (Kletz 1985). Although operators are generally competent individuals, they typically do not fully understand the underlying fundamental principles involved in the process system's design and operation (Kletz 1985). 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 (Visick 1986). Counteracting this limitation requires a medium in which all pertinent information about both the process system's normal and abnormal operation can be permanently stored and quickly retrieved. It also requires a method for determining which of that information is relevant to the solution of the problem currently confronting the process operator.

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 (1981) 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:

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 for storing the correct solutions to operating problems confronted in the past, correctly classifying the current plant situation as one of those problems if applicable, 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 efficiently reused in a systematic manner, 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.

## 1.5 THE ROLE OF AUTOMATED PROCESS FAULT ANALYSIS

Unfortunately, the various traditional measures currently being taken to help operators perform process fault management have not been able to provide them the support that they need to totally eliminate process accidents. Typically, these accidents have had very simple origins (Kletz 1985; Lieberman 1985). The reason that they still occur is because the number of possible process failures which need to be considered and the amount of process information which must be analyzed commonly exceed those that an operator can always effectively cope within emergency situations.

Furthermore, this situation probably cannot be counteracted by further additional investments in these traditional measures: many of them have already been exploited to nearly their full potential. Thus, in order to further improve process safety, additional process fault management methods need to be developed and successfully deployed to directly help address this problem.

As to be extensively elaborated further throughout the remainder of this treatment, the most attractive, but currently greatly underutilized, approach for helping the operators perform process fault management is to automate process fault analysis, that is, to automate the underlying reasoning required to determine the cause or causes of abnormal process behavior. Not surprisingly, various logically viable diagnostic 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, for a variety of reasons discussed in the next chapter, at the present time, the potential of existing process control computers to analyze real-time process information for such purposes is still relatively unexploited by the CPI (Venkatasubramanian 2001).

Automated process fault analysis should be used to augment, not replace, human capabilities in process fault management. Consider the current relative strengths and weaknesses of computer analysis compared with human analysis. Computers can outperform humans in doing numerous, precise and rapid calculations, and in making associative and inferential judgments (Sheridan 1981). Computers furthermore have potentially unlimited and almost completely infallible memories compared to humans, and, furthermore, can be readily networked together to powerfully enhance their capabilities. They are also just starting to begin to “learn” in complex environments. On the other hand, humans are better at those functions which cannot be standardized. Humans readily exploit commonsense reasoning very effectively in decision making, whereas computers do not, beyond that which can be expressed as the heuristics human experts rely their analyses upon (Alford et al. 1999a,b). They are also better at decision making that has not been adequately formalized (i.e., creative thought). Humans likewise perform

better pattern recognition in co-ordinations that involve the integration of a great many factors whose subtleties or non-quantifiable attributes defy computer implementation (Lefkowitz 1982). In order to ultimately achieve successful plant deployments, these various advantages in current computational capabilities always need to be kept in mind and more fully exploited when designing actual automated process fault analyzers.

Currently, the computer offers a means to rapidly analyze process information in a systematic and predetermined manner. If such analysis is already being done by the operators, automating it would free them to perform other functions. If it is not being done, it could be because the operators either do not have sufficient time or the capabilities required to perform it. In either case, properly automating such analysis should make the information reaching the operators more meaningful (De Heer 1987). Thus, the main advantage of deploying real-time, on-line process fault analysis is to dramatically reduce the cognitive load on the process operators (Laffey et al. 1988; DuBois et al. 2010). This would subsequently allow them to concentrate on those analyses which still require human judgments to perform.

As a final observation, it is possible that many of these current problems being encountered in achieving more effective process fault management could be counteracted by replacing operators with more highly trained process engineers.<sup>13,14</sup> The higher wages paid to these individuals would be

<sup>13</sup>Note: Joe Alford speculates one advantage of replacing operators with engineers is that it might finally force engineers to mend their ways and do a better job of alarm and HMI management. They would have to actually experience first-hand the results of their zealous configuration of so much information in process control computers. Another issue he observed in most of the plant automation audits he did over several years was that engineers did not inactivate alarms/alerts when they were not relevant, leading to many nuisance alarms and subsequent loss of respect of the alarm system by operators. So, again, it is great to highlight some of the inherent weaknesses of operators in dealing with process faults, but a significant part of the problem is how control engineers configure control systems.

<sup>14</sup>As Steve Apple further points out, one of the greatest problems with current HMI's is that most are designed by engineers with little consideration of human factors. The ultimate human factors today are video games. The average kid can pick one up and play with very little instruction. The average HMI actually being used on process units? – not so much. Most HMI's are designed to follow the P&ID's that were developed for the process. And most engineers understand them, and think they actually are instructional for operators who have very little understanding of thermodynamics, fluid flow, heat transfer, etc. So we as engineers design them for OUR understanding, expecting everybody to see what seems intuitively obvious to us. High performance situational awareness HMI's try to understand how humans collect and recognize data instantaneously. So, much of our goals in redesigning control systems is to actually REMOVE information that is not pertinent- both in the form of process data and alarms as well as fancy looking graphics that just take up real-estate. A perfect HMI would lead any user/operator to the same conclusion and ultimately the same resolution to the problem (so, unfortunately, there is yet no perfect HMI).

offset by their more efficient operation of the given process system. Nonetheless, since engineers are subject to the same human limitations as process operators are, doing this would not eliminate the need to directly address the fore-mentioned currently existing problems that humans exhibit in performing highly effective process fault management. Therefore, it is our overwhelming contention that automating process fault analysis currently represents the best remaining relatively unexploited means presently available for directly addressing these problems head-on. Doing so should both bolster and compliment the process operators' innate capabilities at performing effective process fault management whenever required.

## REFERENCES

- Alford, J.S., Cairney, C., Higgs, R. et al. (1999a). Real rewards from artificial intelligence. *Intech* (April ed.) 52–55.
- Alford, J.S., Cairney, C., Higgs, R. et al. (1999b). Online expert-system applications: use in fermentation plants. *Intech* (July ed.) 50–54.
- Barclay, D.A. (1988). Protecting process safety interlocks. *Chemical Engineering Progress* 84 (2): 20–24.
- De Heer, L.E. (1987). 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. G.V. Reklaitis and H.D. Spriggs), 33–66. New York: Elsevier Science Publishers Inc.
- Dellner, W.J. (1981). The user's role in automated fault detection and system recovery. In: *Human Detection and Diagnosis of System Failures* (ed. J. Rasmussen and W.B. Rouse), 487–499. New York: Plenum.
- DuBois, L., Foret, J., Mack, P., and Ryckaert, L. (2010). Advanced logic for alarm and event processing: methods to reduce cognitive load for control room operators. *IFAC Proceedings Volumes* 43 (13): 158–163.
- Eberts, R.E. (1985). Cognitive skills and process control. *Chemical Engineering Progress* 81: 30–34.
- Fortin, D.A., Rooney, T.B., and Bristol, H. (1983). Of christmas trees and sweaty palms. In: *Proceedings of the Ninth Annual Advanced Control Conference*, 49–54. West Lafayette: Indiana.
- Goff, K.W. (1985). Artificial intelligence in process control. *Mechanical Engineering* (October ed.) 53–57.
- Kletz, T.A. (1985). *What Went Wrong?, Case Histories of Process Plant Disasters*. Houston, TX: Gulf Publishing Co.
- Kohan, D. (1984). The design of interlocks and alarms. *Chemical Engineering Magazine* (May ed.) 73–80.
- Laffey, T.J., Cox, P.A., Schmidt, J.L. et al. (1988). Real-time knowledge based systems. *AI Magazine* 27.

- Lees, F.P. (1981). Computer support for diagnostic tasks in the process industries. In: *Human Detection and Diagnosis of System Failures* (ed. J. Rasmussen and W. Rouse), 369–388. New York: Plenum Press.
- Lees, F.P. (1983). Process computer alarm and disturbance analysis: review of the state of the art. *Computers and Chemical Engineering* 7 (6): 669–694.
- Lefkowitz, I. (1982). Hierarchical control in large scale industrial systems. In: *Studies in Management Science and Systems*, vol. 7, 65–98. New York: North-Holland Publishing Co.
- Lieberman, N.P. (1985). *Troubleshooting Process Operations*, Tulsa. Oklahoma: PennWell Publishing Co.
- Linhou, D.A. (1981). Aiding process plant operators in fault finding and corrective action. In: *Human Detection and Diagnosis of System Failures* (ed. J. Rasmussen and W.B. Rouse), 501–522. New York: Plenum Press.
- Rasmussen, J. (1981). Models of mental strategies in process plant diagnosis. In: *Human Detection and Diagnosis of System Failures* (ed. J. Rasmussen and W.B. Rouse), 251–258. New York: Plenum.
- Rijnsdorp, J.E. (1986). The man-machine interface. *Chemistry and Industry* (May ed.) 304–309.
- Sheridan, T.B. (1981). Understanding human error and aiding human diagnostic behaviour in nuclear power plants. In: *Human Detection and Diagnosis of System Failures* (ed. J. Rasmussen and W.B. Rouse), 19–35. New York: Plenum.
- Syrbe, M. (1981). Automatic error detection and error recording of a distributed fault-tolerant process computer system. In: *Human Detection and Diagnosis of System Failures* (ed. J. Rasmussen and W.B. Rouse), 475–486. New York: Plenum.
- Visick, D. (1986). Human operators and their role in automated plant. *Chemistry and Industry* 199–203.
- Venkatasubramanian, V., “Process fault detection and diagnosis: past, present, and future, Proceedings of CHEMFAS4, Seoul, Korea, 2001, pp. 3–15.