Incidents Investigation and Dynamic Analysis of Large Alarm Databases in Chemical Plants: A Fluidized-Catalytic-Cracking Unit Case Study†

Ankur Pariyani and Warren D. Seider*

Department of Chemical and Biomolecular Engineering, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6393

Ulku G. Oktem

Risk Management and Decision Processes Center, Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania 19104-6340

Masoud Soroush

Department of Chemical and Biological Engineering, Drexel University Philadelphia, Pennsylvania 19104

A novel framework to model the chronology of incidents is presented—depicting the relationship of initiating events with the various regulating and protection systems of the process—eventually leading to consequences, varying from zero to high severities. The key premise is that the departures and subsequent returns of process and product quality variables, from and to their normal operating ranges, are recognized as *near-misses*, which could have propagated to incidents. This leads to the availability of vast near-miss information recorded in distributed control and emergency shutdown systems databases that monitor the dynamics of the process. New performance indices, which utilize this abundant information, are introduced to conduct quantitative and qualitative (absolute and relative) assessment of the real-time safety and operability performances of an industrial fluidized-catalytic-cracking unit (FCCU) at a petroleum refinery. Also, new techniques for abnormal event tracking and recovery-time analysis are presented, which help to identify the variables that experience operational difficulties. It is shown how this information can be used to suggest improvements in the alarm-system structures for the FCCU.

1. Introduction

According to the Occupational Safety and Health Administration (OSHA), an *incident* is an unplanned, undesired event that adversely affects completion of a task. In the chemical process industries (CPIs), the extent of human and financial losses due to the incidents is staggering. On the basis of their severity levels, incidents can be broadly classified as *near-misses* or *accidents*. Though accidents have low probabilities of occurrence, they have high severities, often accompanied by on-site and/or off-site major impacts. Near-misses, on the other hand, have much higher probabilities of occurrence, but have more limited impact. Recent studies have demonstrated the importance of identifying near-misses to predict the probability of accidents[1,2] as well as reporting and investigating near-misses to reduce the potential of accidents.[3–5]

The United States Chemical Safety Board's Web site, http://www.csb.gov/, shows numerous examples of near-misses, which have low or limited severity, but occur prior to accidents and contain information that would help identify the root causes that led to the accidents. Although it is well understood that when these near-misses are addressed, the occurrence and impact of accidents are reduced, there are just a few published studies that show the potential benefit of attending to near-misses. This is mainly due to (a) the lack of interest from companies to implement near-miss management systems and (b) the skepticism of organizations in sharing collected near-miss data, due to liability concerns. One exceptional case at Norsk Hydro[6] shows that when near-miss reporting for on-shore activities over 13 years was increased from 0 to 0.5/person·year (by motivating employees to identify and report near-misses and taking corrective actions), lost-time injuries were reduced by approximately 75%.

The relative impacts of near-misses and accidents can be summarized using the safety pyramid in Figure 1.[1,3] This figure emphasizes that, for every accident, there are several near-misses, some of which are precursors to accidents (necessary, but not sufficient conditions), and indicate less severe, unsafe, conditions or consequences. Like accidents, near-misses differ in severities and probabilities of occurrence, but all near-misses should be viewed as opportunities to improve the performance of the process. Note that the distinction between near-misses and accidents can be subjective; for example, an oil-spill incident with minor property damage, but no injuries, can be viewed as an accident or a near-miss.

For the process industries, retrospective analyses show that every accident is preceded by disturbances that trigger *abnormal situations*—the propagation of which may eventually lead to the accident(s). Statistically, these disturbances are referred to as the causes of variation; that is, so-called *special* or *common causes*. The former are unanticipated, sudden phenomena, signifying unexpected in-process changes, while the latter are associated with background noise. Special causes are, therefore, precursors of abnormal situations, which are, in turn, precursors of incidents.

In this paper, the safety pyramid is expanded to a novel framework consisting of four chronological stages of incidents, beginning with their special causes. The stages expose the relationship between the special causes, near-misses, and

† Part of the special issue honoring Professor Thomas F. Edgar.

* To whom correspondence should be addressed. E-mail: seider@seas.upenn.edu.

10.1021/ie9019648
Published on Web 04/02/2010

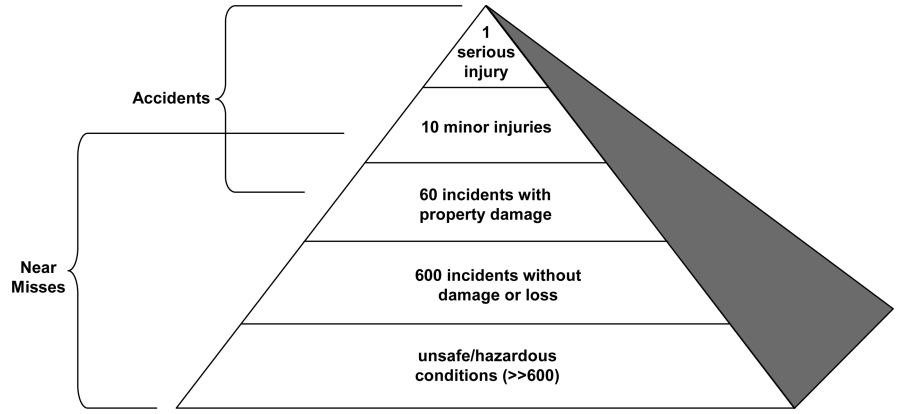

Figure 1. Safety pyramid (with typical historical values).

accidents, and the various *safety*, *quality*, and *operability systems*, which regulate process operations and/or protect against abnormal behavior at various levels.

Furthermore, over the last two decades, the CPIs have paid more attention to *preventable* incidents through various *abnormal situation management*[7–13] programs within and across companies. Abnormal situation management focuses on preventing incidents that arise due to poor alarm system management, protection systems involving human actions, training, design of automatic systems, operating procedures during emergencies, etc. To address these issues, several papers have presented successful programs and methods, often improving alarm system structures,[14–32] and performing root-cause analyses including human reliability analysis.[33–41] In this paper, new techniques to utilize near-miss information within a process are presented to assess its safety and operability performances, and to improve the reliability of its safety, quality, and operability systems using tracking and comparative analyses.

Near-misses reflect operational difficulties, experienced by the process and its regulating (process control) and protection (emergency shutdown) systems, that may or may not lead to incidents. Because few industries actively address near-misses, this paper is intended to show that tracking near-misses can serve as efficient performance indicators. Herein, for both the process and quality variables, their departures from and subsequent returns to normal operating ranges, are recognized as near-misses—because such dynamic departures have the potential to propagate to incidents—when their safety, quality, and operability systems fail. To obtain near-miss information, the dynamic distributed control system (DCS) and emergency shutdown (ESD) system databases are utilized for (1) the quantitative and qualitative (absolute and relative) assessment of safety and operability performances, (2) improvement of the alarm system and variable performance, (3) calculation of profit losses, and (4) risk analyses to predict incident probabilities. To our knowledge, these uses of DCS and ESD system databases have not been reported before. Herein, the focus is on the first two objectives, while risk analysis and profit-loss estimation will be presented elsewhere.[42,43]

Results are presented from the analysis of the DCS and ESD system databases of a fluid-catalytic-cracking unit (FCCU) at a major petroleum refinery, which processes more than 250 000 barrels of oil per day. Although the findings and patterns apply to the unit over specific time periods, the techniques and conclusions are applicable to general processes—large- or small-scale, continuous, batch, or semibatch. They show that valuable trends can be extracted from analysis of these vast, often "underutilized" databases.

Section 2 presents a framework to model the chronology of incidents—depicting the propagation of incidents through various safety, quality, and/or operability systems, eventually leading to consequences. It introduces *abnormal events*, *operating-belt zones*, and *upset states* upon which the modeling framework is based. Section 3 introduces new techniques and indices to assess the real-time safety and operability performances and their application to the FCCU. Sections 4 and 5 introduce new techniques for abnormal event tracking and recovery-time analysis, which help to identify variables experiencing operational difficulties. It is shown how this information can be used to suggest improvements in the alarm-system structures for the FCCU. Throughout this paper, emphasis is on the analysis of process-related near-miss information, often unutilized in the process industries, to provide insights and elevate process performance. A brief discussion on profit losses associated with abnormal events is presented in section 6. Finally, conclusions are presented in section 7.

2. Chronology of Incidents

Modern chemical processing units are equipped with DCSs and ESD systems to ensure safe operation and high-quality performance. The DCSs involve controller elements distributed throughout the units, with central servers that issue controlling actions. Along with human operators, they maintain the variables well within their defined operating envelopes to optimize the profitability, safety, quality, and flexibility of the units.[1] In many cases, to account for nonlinear interactions among the variables, the DCSs implement multivariable, nonlinear model-predictive controllers (MPCs) that can handle the nonlinear interactions more efficiently than multiple single-input, single-output (SISO) controllers.

All of the important operating parameters (or variables) are usually equipped with high/low and/or high-high/low-low alarms. These alarms notify the operators whenever the variables cross their threshold values. On the basis of their priorities, the alarms are displayed in the *alarm trends* window and dynamically stored in the DCS database. When a variable moves above or below defined operating limits (known as the ESD limits; usually far apart from high/low and high-high/low-low alarm thresholds), the ESD system takes over from the DCS. This is to ensure that it acts as an independent protection system, uninfluenced by a malfunctioning DCS.

Depending upon the type of their measurements, variables are divided into two groups: *process* and *quality* variables. Process variables are variables for which online measurements are available easily and frequently (after adequate filtering to

reduce the measurement noises). These track the dynamics of the process and examples include temperatures, pressures, flow rates, and their rates of change. Quality variables are related directly to the *quality* of the products; for example, viscosity, density, and average molecular weight. Their measurements are usually obtained from laboratory analyses of product samples, taken at regular intervals, and therefore, are available after time delays. Often, estimators based on mechanistic and/or statistical models, together with process variable measurements, are employed to obtain real-time frequent estimates of quality variables.

2.1. Primary and Secondary Variables. On the basis of their sensitivity and importance, variables are classified into two categories: *primary* and *secondary* variables. Primary variables are most crucial for the *safety* of the process and are associated with the ESD system. Whenever these variables move beyond their ESD limits, emergency shutdowns or "trips" are triggered, often following a short time delay. Note that typically in the CPIs, for select primary variables, *override controllers* are installed, which are activated during this delay period and take radical actions (e.g., jump change its feed variables, etc.) to bring the variables within their acceptable operating ranges. When the override controllers are successful, no tripping occurs. Secondary variables, on the other hand, are not associated with the ESD system. Note, also, that a primary or secondary variable can be a process or quality variable.

The selection of primary variables is determined by experts during the design and commissioning of the plant by carrying-out an in-depth analysis of the trade-off between the *safety* and *profitability* of the plant. Its foremost goal is to prevent accidents, having catastrophic consequences on life, property, and the environment, by execution of emergency shutdown procedures. However, shutdowns are costly lapses that result in huge profit and man-hour losses—which need to be avoided. For this reason, the primary variables are selected to be sensitive to disturbances and are critical to the desirable performance of the process. For large-scale processes, typically 150−400 variables are monitored; however, only a small percentage (<10%) are associated with the ESD system.

Because each primary and secondary variable is monitored by alarms, care in its measurement and/or estimation is required. In special situations, when nonlinear interactions among the variables are important, combined variables can be monitored by alarms—although for most processes, such as FCCUs, individual primary variables are well-recognized. In FCCUs, typical primary variables include the pressure drops in stand pipes and reactor temperature.

2.2. Priority of Alarms and Variables. Alarms are prioritized in accordance with the actions of the plant operators during upset situations. Typically, 15−25% of the alarms are designated as high-priority alarms, 20−30% as medium-priority alarms, and 50−65% as low-priority alarms. Accordingly, the variables associated with the low-, medium-, and high-priority alarms are referred to as low-, medium-, and high-priority variables. The high-priority variables usually consist of all of the primary variables and some of the secondary variables (20−25% of the total secondary variables; referred to as high-priority secondary variables). The majority of the secondary variables are designated as medium- or low-priority variables. To better clarify this categorization of variables, a typical FCC unit is considered in the Appendix.

2.3. Chronological Stages of Incidents. In this subsection, four stages are defined to model the propagation of incidents from their origins to their end-states. The stages are (a) origin of the special cause, (b) origin of the abnormal event, (c) propagation of the abnormal event, and (d) attainment of the end-state.

2.3.1. Origin of Special Causes. As discussed earlier, special causes refer to the sudden or unexpected causes of variations in process conditions, due to unanticipated phenomena (disturbances). For instance, pump or valve failures, operator errors, defective raw materials, etc. are examples of special causes. Broadly, the special causes are classified in four categories:

a. Structural Causes: actuator and other process equipment faults, aging and maintenance issues, inaccurate calibrations, defective installations, etc.
b. Process Causes: off-specification raw materials, abnormal temperature shifts in heating media, flow pockets due to unexpected density changes, etc.
c. Disturbances Due to External Effects: power breaks, deliberate personnel acts, natural forces (e.g., hot weather, wind, and rain), etc.
d. Human Errors: personnel errors resulting from the lack or inadequacy of personnel training, inattentiveness, and behavioral issues; management-related inefficiencies; etc.

Various *safety, quality, and operability systems* (SQOSs) are installed, which act as regulatory (regulating operations) and/or protection (preventing the occurrence of accidents) levels to keep the variables within their normal operating ranges (close to their target values), and to nullify the impact of special causes that can result in safety problems, off-specification products, and/or a deterioration of operability performance. The latter is discussed in detail in section 3. The first SQOS is the basic process control system (BPCS); that is, an automated control system within the DCS, which can implement nonlinear MPCs to handle nonlinear interactions among the variables effectively. When the BPCS is unsuccessful, *abnormal events* (discussed next) occur, with alarms notifying the operators of some variables having left their normal operating regions.

2.3.2. Origin of Abnormal Events. To define abnormal events, *operating-belt zones* are introduced. Figure 2 shows a control chart for a primary variable. The chart is divided into four belt zones, beginning with its green-belt zone (normal operation), during which the process variable lies within its acceptable limits. When the variable moves beyond its limits, into its yellow-belt zones, high/low alarms are triggered. When it moves beyond the limits of its yellow-belt zones, into its orange-belt zones, high-high/low-low alarms are triggered. The border between its orange- and red-belt zones is the threshold limit for the triggering of its ESD system. An *abnormal event* begins when a process or quality variable moves from its green-belt zone to its yellow-, orange-, or red-belt zones—with these colors chosen to gauge the severity of the abnormal event. Clearly, such a departure is a precursor to a near-miss or accident, when the SQOSs fail to maintain normal operation. The time to return to the green-belt zone is called the *recovery time* for the abnormal event, which depends on the time constants of the process under consideration. Figure 2 shows three recovery times, t_1, t_2, and t_3. Consequently, herein, abnormal events, for variables that return to their green-belt zones, are recognized as near-misses, which could have propagated into incidents. As a result, vast amounts of near-miss information become available for tracking and dynamic risk assessment.

Note that the threshold limits are process-specific and are carefully assigned during the commissioning of the plant using statistical process control techniques on online measurement data of variables. In particular, the limits of the green-belt zones (or

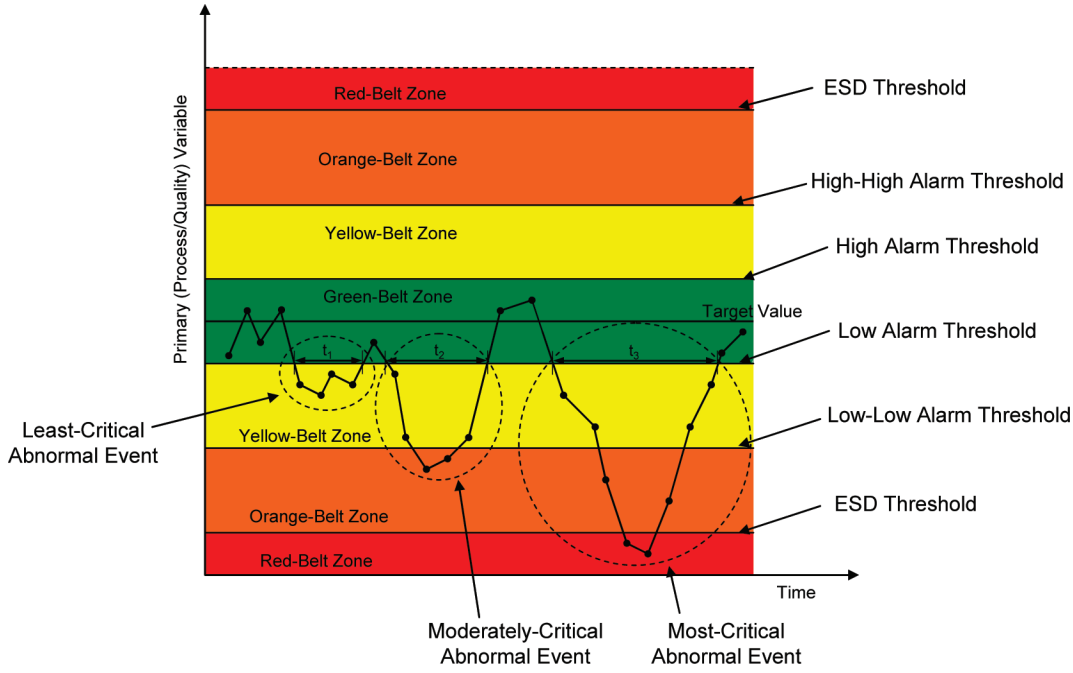

Figure 2. Control chart for a primary variable showing various operating belt zones and alarm thresholds.

normal operating ranges) are assigned such that the variations in process or quality variables due to common causes (i.e., background or measurement noise) remain within the green-belt zones—to be handled by the BPCS only. In principle, the alarms are installed to notify the operators of the onset or progression of special causes. Therefore, the key premise herein is that process or quality variables leave their green-belt zones only in response to a special cause(s).

It must, therefore, be recognized that poorly configured alarms or alarms with poorly assigned thresholds frequently result in false-positive abnormal events (often leading to *alarm flooding*; i.e., a high frequency of alarms) and false-negative abnormal events. For example, alarm thresholds too close to their target values result in false-positive abnormal events due to common causes (rather than special-causes). Whereas, alarms placed farther from their target values result in false-negative abnormal events (i.e, abnormal events resulting from special causes that remain undetected.)

Note also that common causes often evolve and progress over time, resulting in increased operational variability (i.e., increased variation in measurements about target values). Consequently, numerous abnormal events having small recovery times are a result of either (a) efficient regulation of the special causes within short recovery times or (b) a poorly configured green-belt zone, yielding many false-positive abnormal events. For these reasons, alarm thresholds, especially the high- and low-alarms about the green-belt zone, should be updated regularly to reduce the number of false-positive and -negative abnormal events.

In addition to statistical process control techniques and first-principle models, in recent years, more intelligent approaches are being developed to extract information on dynamic process variability from historical data. One technique that computes adaptive alarm limits is presented by Brooks et al.[44]

In some cases, alarm flooding occurs when alarms are installed without detailed analysis, or to warn operators, conservatively, when most of the variables move from their normal operating ranges.[14–32] When this occurs, there is often (a) a relaxation of alarm thresholds for the least important variables or (b) a deactivation of one or more alarm levels; i.e., removing their corresponding belt zones. For example, a variable having no high/low alarm threshold has no yellow-belt zone, and consequently, its green-belt zone extends to its high-high/low-low alarm thresholds. Note that the framework herein is typical—with variables having two layers of DCS alarms (high/low and high-high/low-low) and one layer of ESD alarms. Occasionally, variations occur; for example, variables having only one layer of DCS alarms, or even three layers of DCS alarms, in addition to the ESD layer. In the next section, techniques to reduce alarm flooding are discussed. These focus on the identification of variables that experience high frequencies of abnormal events and high recovery times—providing opportunities to eliminate root causes that often result in special causes.

Depending upon their criticality, abnormal events are classified into three categories, as shown in Figure 2:

(i) Least-critical abnormal events: Abnormal events that cross the high/low alarm thresholds, but do not cross the high-high/low-low alarm thresholds.

(ii) Moderately critical abnormal events: Abnormal events that cross the high-high/low-low alarm thresholds, but do not cross the ESD thresholds.

(iii) Most-critical abnormal events: Abnormal events that cross the ESD thresholds.

For secondary variables, alarm thresholds and their abnormal event classifications are shown in Figure 3. Because these variables do not have red-belt zones, *most-critical abnormal events* cannot occur. See Table 1 for a summary of the associations among primary and secondary variables and the three classes of abnormal events.

Note that in this formulation, the time for a variable to return to its green-belt zone (recovery time) does not impact its abnormal-event classification. However, in future formulations, the times for the variable(s) to return to their orange-, yellow-, and green-belt zones, leading to three levels of recovery times, will be introduced as they impact their abnormal-event classifications. Also, note that the most-critical abnormal events for

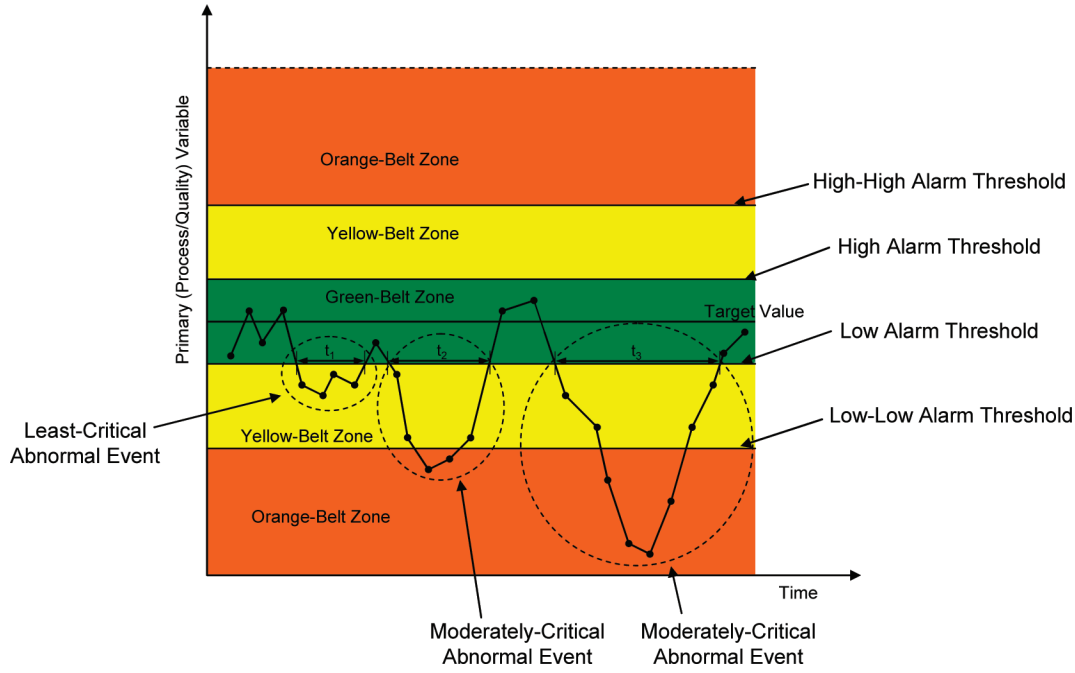

Figure 3. Control chart for a secondary variable showing various operating belt zones and alarm thresholds.

Table 1. Categories of Variables and their Abnormal Events[a]

	secondary variables			primary variables
abnormal events	low-priority variables	medium-priority variables	high-priority variables	high-priority variables
most-critical	N/A[a]	N/A	N/A	yes
moderately critical	yes	yes	yes	yes
least-critical	yes	yes	yes	yes

[a] N/A = not applicable.

those primary variables not equipped with override controllers almost always lead to an ESD.

2.3.3. Propagation of Abnormal Events. As special causes arise in processes, they are handled by the various SQOSs, whose actions guide the process/quality variables through their green-, yellow-, orange-, and red-belt zones. The DCSs and ESD systems help plant operators assess and control plant performance, especially in the face of potential safety and quality problems. Thus, the safety, quality, and operability management structure of any unit consists of the following three entities:

a. Distributed Control System (DCS). Fortunately, modern control systems—involving state-of-the-art DCSs—significantly reduce the influence of special causes. A DCS has distributed elements throughout the plant, and besides local control capabilities, it exercises centralized control. Over time, the usage of the DCS has improved the controlling capabilities and, importantly, reduced the need for human intervention.

Typically, DCSs contain two separate entities—one focusing on the *control* of the process; that is, regulation of the variables within their predefined envelopes. This is commonly referred to as the basic process control system (BPCS), which can implement multivariable MPCs that can handle interactions among the variables effectively. The other focuses on the real-time optimization of the process to reduce the operating costs (e.g., the costs of the catalyst, feed, utilities, etc.) and the maximization of profits. It is referred to as the advanced process control system (APCS). Typically, during normal operation, both the BPCS and APCS are activated. However, during emergencies (e.g., shutdowns or incidents), the APCS is switched off automatically, and the BPCS, often accompanied with emergency override controllers, normally takes radical actions to prevent the occurrence of shutdowns and accidents.

The dynamic data associated with the process and quality variables are stored in DCS servers. Typically, the DCS database contains abnormal event data; that is, alarm identity tags for the variables, alarm types (low, high, high-high, etc.), times at which the variables cross the alarm thresholds (in both directions), variable priorities, etc. Its associated ESD database, of greater consequence, contains trip-event data, timer-alert data, etc. For large-scale units, the DCS databases contain 5000−10 000 alarm entries recorded every day, associated with 500−1000 abnormal events. Thus, these databases contain much information on the dynamics of the process. In section 3, they are used to formulate performance indices to assess safety and operability performances—and in sections 4 and 5, to perform frequency-tracking and recovery-time analyses of near-misses.

b. Plant Personnel. When using the ESD system and DCSs, control rooms permit the operators to monitor and control the plant (normally comprised of several units). The control rooms contain human−machine interfaces (HMIs) through which human operators interact with the ESD system and DCS. The reliability of the human component depends on various *performance shaping factors (PSFs)*,[33] which have been classified into three categories. First, *external PSFs* define the work environment of employees; that is, the temperature, humidity, and air quality; work hours and breaks; shift rotations; actions by supervisors and management; human−machine interfaces; and team structure and method of communication (oral or written). Second, *stressor PSFs* are factors that cause stress among employees, either *psychological* or *physiological*. The former includes the task load, monotony of work, threatening actions of supervisors, and distractions, and the latter includes the duration of stress, movement constrictions, and temperature extremes. Third, *internal PSFs* denote the characteristics of employees, for example, their motivation and attitudes toward work, emotional state, and previous training experiences.

Behavior-based safety studies over the past few decades have greatly improved the understanding and implementation of the PSFs.[33–41] Clearly, improved operator performance can be

Table 2. Safety Integrity Levels and their Corresponding PFDs and RRFs[48]

SIL	PFD	RRF
1	0.1−0.01	10−100
2	0.01−0.001	100−1000
3	0.001−0.0001	1000−10000
4	0.0001−0.00001	10000−100000

achieved by careful management of the PSFs, for example, by controlling the stress levels to increase vigilance, by instituting regular training programs, and by encouraging the reporting of near-misses followed by corrective actions or at least recognitions.

Incident-related databases for over 80 companies show that human-related factors, including management, contribute largely to incidents in the process industries.[45] In another study, Grabowski et al.[46] identify positive correlations between the human factors and the occurrence of incidents in the marine transportation sector. In a recent *perceived root-cause* survey involving human operators at a petroleum refinery, 120 employees (shift supervisors, head and control operators) identified *high-stress level* as the second most important factor, after *failure of equipment*, leading to the occurrence of incidents.[47] Moreover, salary-related issues and excessive work load were identified as the prime reasons for high stress.

c. Emergency Shutdown (ESD) System. Typically, the ESD system for each unit in a chemical plant takes radical action (e.g., shuts down the unit, jump changes its feed variables, etc.) when any of its primary variables crosses its ESD limits. Also, ESD systems have safety integrity levels (SILs), a measure of their safety risk, which determines the intensity of their actions.[48,49] The SIL determines the level of risk-reduction provided by the ESD system, based on probabilistic analysis. Four SILs are defined:[48] that is, levels 1, 2, 3, and 4, with each level representing an order of magnitude of risk reduction. Table 2 shows the *risk reduction factors* (RRFs) and the probabilities of *failure under demand* (PFDs); that is, the failure probabilities. The most dependable SIL, 4, is usually reserved for nuclear plants, where very low risk levels are required, and for avionic sectors, which have the highest severity upon failure (e.g., a crash).

Typically, in modern and renovated plants, there are redundant measurements (e.g., three or four) for every primary variable. However, for older plants, these redundancies may not exist. When any primary variable crosses one of its ESD threshold limits, alarms associated with its measurements are triggered. These alarms, referred to as *timer-alerts*, are associated with the ESD system of the unit. In many systems, a time delay occurs before a tripping is initiated; that is, when the majority of the measurements of a primary variable crosses its ESD threshold, the shutdown process (tripping) begins after the time delay. For the FCCU, time delays range from 2 to 30 s. In general, small delays of 2−5 s are to prevent trips caused by measurement noise or other electronic interferences, whereas large delays of 20−30 s activate advanced override controllers, which attempt to remove the variables from their red-belt zones. These time delays are usually determined during process design and plant commissioning and are governed by the trade-offs between safety and costly shutdown lapses. The magnitude of a time delay is also selected on the basis of the dynamic characteristics of the variable. The override controllers are *low-selector switches* that take radical controlling actions when the primary variables move beyond their ESD limits. When the override controllers are successful, no tripping occurs. Normally, the ESD system operates independently of the other SQOSs. However, in many cases, it involves human assistance—and becomes dependent upon the performance of the operators in stressful environments.

Next, four *upset states* are introduced involving operability-, safety-, quality-, or safety-and-quality-related upsets. Processes are said to be in an upset state when the process or quality variables move out of their green-belt zones, indicating "out-of-control" or "perturbed" operation. These upset states are the following:

a. Operability-Only Upset State (OOUS), where at least one of the *secondary process* variables lies outside of its green-belt zone, but all of the *quality* variables and the *primary process* variables lie within their green-belt zones. In this case, only the operability performance deteriorates, whereas *safety* and *product quality* are maintained. This occurs, for example, when the flow rate of a stream, a secondary process variable, moves just above its green-belt zone, but not sufficiently far to move the product quality or primary process variables out of their green-belt zones.
b. Safety upset state (SUS), where at least one of the primary process variables lies outside of its green-belt zone, but all of the quality variables lie within their green-belt zones. In this case, both safety and operability performances are affected and a safety problem is likely to occur.
c. Quality upset state (QUS), where at least one of the quality variables lies outside of its green-belt zone, but all of the process variables lie within their green-belt zones. In this case, both quality and operability performances are affected, and an off-specification product quality (also referred to as a quality defect/departure) is likely to occur.
d. Safety and quality upset state (S+QUS), where at least one of the primary process variables and one of the quality variables lie outside of their green-belt zones. In this case, both a quality defect and a safety problem are likely to occur.

Note that although quality variables are causally related to process variables in chemical processes, the occurrence of quality defects does not necessarily imply the occurrence of safety problems and vice versa. Clearly, the process moves from one upset state to another, with the variables moving among their operating belt zones, as the special causes progress.

2.3.4. Attainment of End States. The end state (consequence) and propagation path for an abnormal event are not only governed by the actions of SQOSs, but also by the severity of the special cause(s). Figure 4 shows the chronological stages of incidents for a continuous process, beginning with normal operation. As special causes arise, they are handled by the BPCS of the DCS, whose actions result in either continued operation (green-belt zone) or an upset state (OOUS, SUS, QUS, S+QUS) with process/quality variables in their yellow-, orange-, or red-belt zones. Depending upon the states and zones, SQOSs are activated. Their actions result in end-states (consequences) summarized in the right-hand column. Note that the dashed double arrows between the upset states depict transitions among them and the solid double arrows between the upset states and SQOSs depict interactive−corrective actions. Also, S and F denote success and failure, respectively.

Note also that the colors of the consequence blocks signify the *severity* levels of the consequence; that is, *green* for a safe consequence with acceptable quality, and *red* for a consequence with highly unsafe conditions and/or unacceptable quality.

Depending on the actions of the SQOSs, the following possible end-states (consequences) occur:

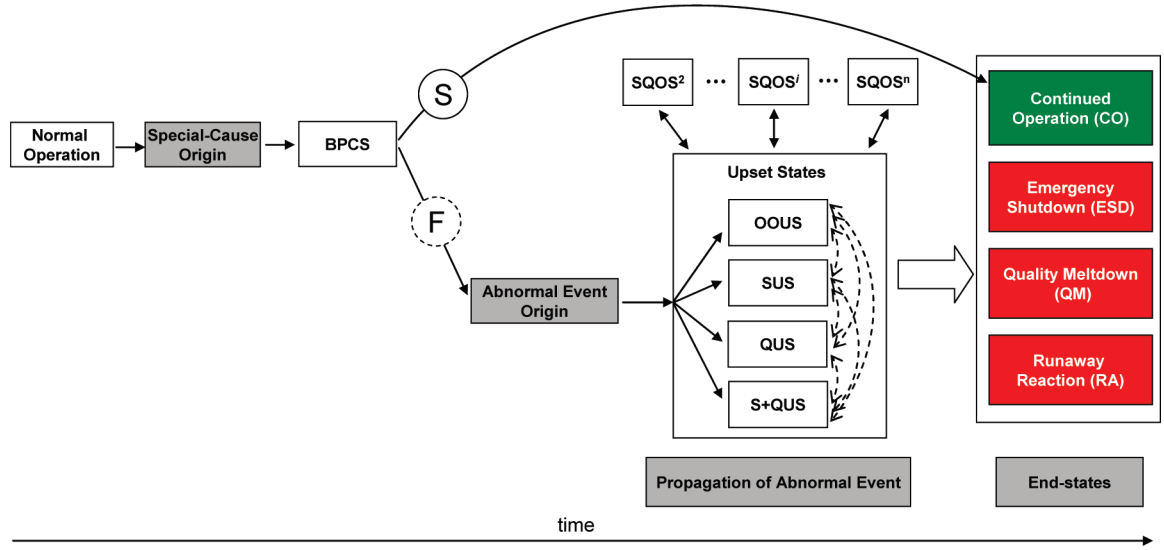

Figure 4. Model flowchart depicting the various chronological stages.

a. Continued operation (CO): this end-state (consequence) results when all of the process/*quality* variables return to their green-belt zones.
b. Emergency shutdown (ESD): this end-state (consequence), a near-miss, occurs when a primary process/quality variable enters its red-belt zone and emergency shut-down sequences (automatic/manual—when the automatic sequence fails, the operator intervenes) are triggered. Note that failure of this manual emergency shutdown results in an accident.
c. Quality meltdown (QM): this end-state (consequence) is considered to be an accident, which occurs when all of the safety, quality, and operability systems fail to remove a quality variable(s) from its red-belt zone. Major economic losses result due to product losses and manpower requirements to return the process to normal operation. In some cases, equipment losses are involved.
d. Runaway reaction (RA): this end-state (consequence) leads to a typical accident, which occurs when all of the regulating and protection systems fail to remove a primary process variable from its red-belt zone. Uncontrolled runaway reactions often lead to loss of life, serious injuries, and major equipment losses.

The above framework presents the chronology of incidents in the process industries. The final end-state is preceded by a large number of abnormal events, acted upon by the various SQOSs. It follows that with better near-miss tracking and investigation techniques, the majority of the incidents can be prevented. Next, new techniques are presented to utilize the vast amount of near-miss information to assess the dynamic safety and operability performances.

3. Real-Time Assessment of Safety and Operability Performances

The use of dynamic DCS and ESD system databases to assess the real-time performance of any chemical process has the potential to help operators identify likely problems before they evolve into incidents, to identify the root causes of abnormal events, and to reduce the frequencies of unwanted alarms. The key premise of this section is that the *safety performance* of a process is characterized by its primary variables, the *quality performance* is characterized by its quality variables, and the *operability performance* is characterized by all of its variables. These performances are determined by the dynamics of the associated variables. Next, performance indices are introduced to quantitatively and qualitatively assess the safety and operability performances, which are illustrated for the operation of an FCCU at a major petroleum refinery. Due to the unavailability of data for the FCCU quality variables, because their alarm thresholds were deactivated and product analyses were not available, an index to assess the quality performance is not presented.

3.1. Operability and Safety Performance Indices. The operability performance describes the overall efficiency of process operations and governs the operating costs of the plant.[50] In other words, it signifies how *well* the process operations are carried out by the safety, quality, and operability systems (SQOSs)—as determined by the collective performance of the *process* and *quality* variables. It is maximized when all of the variables are within their normal operating ranges (i.e., green-belt zones—with no abnormal events), and minimized when *all* of the variables move out of their normal operating ranges. Because most abnormal events directly or indirectly deteriorate the off-specification quality and quantity of the products, suboptimal operability performance results in profit losses.

Similarly, the safety performance describes how *safely* the process operations are carried out by the SQOSs—as determined by the performance of the primary variables. It is maximized (i.e., perfectly safe) when all of the primary variables are within their normal operating ranges (i.e., green-belt zones—with no abnormal events), and minimized (i.e., extremely unsafe) when *all* of the primary variables are in their red-belt zones. Because abnormal events associated with the primary variables pose *risks* to the process, they deteriorate both the safety and operability performances. Note that the secondary variables (in large numbers) are not used to evaluate the safety performance since their influence is channeled through the abnormal events of the few primary variables.

Next, two indices are defined to assess the safety and operability performances of processes in real-time and to quantitatively evaluate their dependence on the abnormal events of the variables. By monitoring the suboptimal behavior of these indices, the operators can detect more easily special causes in the early or intermediate stages, permitting them to take precautionary actions before incidents occur.

Table 3. Threshold Levels for the Membership Zones in Operability Performance

operability performance (membership zones)	threshold levels
excellent	OPI ≥ 99th percentile
high	90th percentile ≤ OPI < 99th percentile
good	75th percentile ≤ OPI < 90th percentile
average	50th percentile ≤ OPI < 75th percentile
low	25th percentile ≤ OPI < 50th percentile
significantly low	10th percentile ≤ OPI < 25th percentile
extremely low	OPI < 10th percentile

First, to quantify the operability performance at time, t, an *operability performance index (OPI)*, is defined:

$$\mathrm{OPI}(t) = \sum_{i=\mathrm{HP,MP,LP}} w_i(1 - f_i(t)) \tag{1}$$

where i denotes the category of the variables [high-priority (HP), medium-priority (MP), low-priority (LP)], w_i is the normalized weighting factor for category i with $w_{\mathrm{HP}} + w_{\mathrm{MP}} + w_{\mathrm{LP}} = 1$, and $f_i(t)$ is the ratio of the number of variables of category i out of their normal operating ranges to the total number of variables of category i. Each weighting factor is assigned based upon the relative impact of the category of variables on the operability performance; a category with a higher priority has more impact, and consequently, $w_{\mathrm{HP}} = 1/2$, $w_{\mathrm{MP}} = 1/3$, and $w_{\mathrm{LP}} = 1/6$ are suggested herein. These are representative values that can be altered during risk analysis. Clearly, the OPI is maximized at 1, with all variables in their normal operating ranges, and minimized at 0, with all variables outside of their normal operating ranges.

The OPI varies dynamically, depending on the actions of the SQOSs. For qualitative analysis, seven levels of performance are defined using the following membership zones: excellent, high, good, average, low, significantly low, and extremely low. Their threshold values are determined using key statistical values (e.g., median, quartiles, and other percentile values) for the OPI over extended periods (e.g., months or years). For example, with the threshold value for excellent at the 99% percentile, based on past OPI values, when current OPI values lie within the top 1% of the past OPI values over a sufficiently long time, the operability performance is designated as excellent. Furthermore, these threshold values should be updated regularly, perhaps every week or month using the latest data. The membership zones and their threshold values are presented in Table 3.

It follows that the rate of change of the OPI with respect to the change in the number of abnormal events in category i is

$$\frac{\partial \mathrm{OPI}}{\partial \mathrm{AE}_i} = -\frac{w_i}{N_i} \tag{2}$$

where AE_i and N_i are the number of abnormal events (i.e., variables out of their normal operating ranges) and the total number of variables for category i. Thus, for the FCCU, for unit increases in the number of abnormal events, the OPI decreases by 0.014, 7.6×10^{-3}, and 7.9×10^{-4} for the HP, MP, and LP variables. Hence, the impact of an abnormal event associated with a HP variable on the operability performance is nearly 2 and 18 times of those associated with medium- and low-priority variables. This result is useful in estimating the profit losses associated with abnormal events.

Table 4. Criteria for the Membership Zones in Safety Performance

safety performance (membership zones)	criterion
perfectly safe	all the primary variables are within their green-belt zones
safe	at least one of the primary variables experiences a least-critical abnormal event(s)
moderately safe	at least one of the primary variables experiences a moderately critical abnormal event(s)
unsafe	at least one of the primary variables experiences a most-critical abnormal event(s)
extremely unsafe	all of the primary variables experience most-critical abnormal events

Similarly, to quantify the safety performance at time, t, a *safety performance index (SPI)*, is defined:

$$\mathrm{SPI}(t) = \sum_{k=1}^{n} w_{\mathrm{HP},P_k}(1 - A_{\mathrm{HP},P_k}(t)) \tag{3}$$

where n is the number of primary variables, k is the index of the primary variable, P_k is primary variable k, w_{HP,P_k} are the normalized weighting factors for the high-priority primary variables, and $A_{\mathrm{HP},P_k}(t)$ is the *impact parameter* for the operating belt zone in which the primary variable P_k lies at time, t. Because the safety performance worsens as a primary variable moves from its green-, to yellow-, to orange-, and to red-belt zones, herein: for the green-belt zone, $A_{\mathrm{HP},P_k} = 0$; for the yellow-belt zone, $A_{\mathrm{HP},P_k} = 0.01$; for the orange-belt zone, $A_{\mathrm{HP},P_k} = 0.1$, and for the red-belt zone $A_{\mathrm{HP},P_k} = 1$. This is equivalent to assuming that as a primary variable moves from its green-belt zone to its red-belt zone, the associated safety risk levels increase by factors of 10. Again, these are representative values to be adjusted by risk analysts. Also, for the FCCU analysis in section 3.2, the weighting factors are equal; i.e., $w_{\mathrm{HP},P_k} = 1/n$. Clearly, the SPI is maximized at 1, with all of the primary variables in their normal operating ranges, and minimized at 0, with all of the primary variables in their red-belt zones. As for operability performance, levels of safety performance are defined using the following membership zones: perfectly safe, safe, moderately safe, unsafe, and extremely unsafe. The membership zones and the criteria used to set their threshold values are presented in Table 4.

For the FCCU, the threshold levels are obtained using simple permutation calculations, as discussed in section 3.2. Comparison of these OPI and SPI with daily and hourly moving-average values should help the operators conveniently monitor the real-time operations and identify major special causes or disturbances sufficiently early to prevent incidents.

Next, the safety and operability performances of the FCCU are analyzed using the OPI and SPI.

3.2. Application to FCCU. Before conducting the operability- and safety-performance analyses, the dynamic frequencies of the high-, medium-, and low-priority variables outside of their normal operating values are presented in Figure 5 for two consecutive days (days 1 and 2). According to the DCS and ESD logs, during days 1 and 2, five most-critical abnormal events occurred (three associated with primary variable 1, P_1, one with primary variable 2, P_2, and one with primary variable 3, P_3), two of which resulted in trips on day 2 at 5:56 p.m. (P_2) and 6:00 p.m. (P_3). The three most-critical abnormal events associated with P_1, which did not result in trips, occurred on day 2 at 4:38 a.m., 5:55 p.m., and 6:23 p.m. (shown as black vertical lines). Here, the dynamic frequency of the number of variables out of their green-belt zones at any instant is the number of abnormal events at that instant. Note that just before

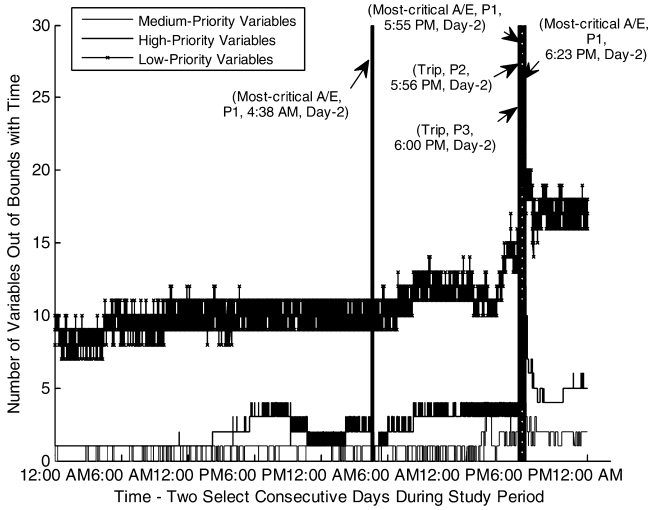

Figure 5. Profiles of variables out of their normal operating ranges for two select consecutive days during the study period.

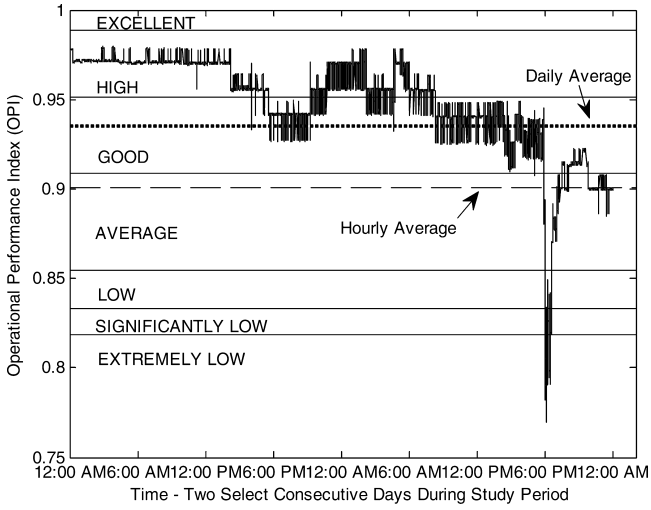

Figure 6. Profile of operability performance index (OPI) for the FCCU over two consecutive days during the study period, along with the membership zones and their threshold levels, and the daily and hourly moving averages.

the trip (P_2, 5:56 p.m., day 2), 18 variables were out of bounds, but just a few minutes later, 44 variables were out of bounds, creating a flood of alarms for the operators.

Based on the real-time frequencies of the high-, medium-, and low-priority variables, OPI are calculated over the two days using eq 1. The thresholds for the different operability performance levels are determined using the OPI over the entire study period. These are the following:

1. 99% percentile = 0.9885.
2. 90% percentile = 0.9515.
3. 75% percentile = 0.9087.
4. 50% percentile = 0.8543.
5. 25% percentile = 0.8332.
6. 10% percentile = 0.8189.

Next, the profile of OPI is presented in Figure 6—with the hourly and daily averages equal to 0.9007 and 0.9349. Over the two-day period, two trips and three most-critical abnormal events occurred, and consequently, the operability and safety performances are much worse than the average performance for the study period. Note that the hourly average is a 1 h moving average (calculated over the preceding 1 h). Similarly, the daily average is a one-day moving average (calculated over the past 24 h).

Notice the gradual decreases or dips in the OPI curve, for example, the transition from the high to good zone, beginning at about 12:00 p.m. on the first day. Such unusual trends indicate the onset of new special causes and can help operators (and engineers) identify likely problems before they evolve into incidents and alert them to identify the root causes of abnormal events.

Next, the safety performance of the FCCU is examined, it being noted that the safety performance diminishes as more primary variables experience most-critical abnormal events. For this reason, three safety levels are added: unsafe, significantly unsafe, and critically unsafe—corresponding to the cases when one, two, and three of the four variables experience most-critical abnormal events. The new safety levels with their thresholds are shown in Figure 7. Because the impact factors, A_{HP,P_k}, are discontinuous, SPI in the shaded boxes are unattainable. Note that the threshold values are evaluated by permutation of the different A_{HP,P_k}, thereby, yielding all possible values attained by the SPI.

The profile of SPI for the FCCU is presented in Figures 8 and 9, with Figure 8 showing the SPI from 0.9 to 1 and Figure 9 showing the SPI from 0.7 to 0.9. Most values are on the order of 0.99; however, the minimum SPI is 0.75, which is the upper threshold for the *unsafe* level. The two figures show these ranges clearly, with unsafe behavior over just small time intervals during day 2 primarily because of the two trips.

The daily average for day 2 was 0.9973, and this indicates that, on average, the FCCU was safe. The hourly moving average (not shown) was 0.9975, slightly higher than the daily moving average. Thus, the profiles of performance indices presented herein provide both quantitative and qualitative measures of the real-time safety and operability performances using the DCS and ESD system databases. Note that these performance indices were computed several months after the data became available. In practice, comparisons of the OPI and SPI data with the daily and hourly moving averages are recommended for operators to understand their relative performances.

Also, these performance indices can be incorporated in HMIs to better inform operators of the operational and safety performances, enabling them to act well in advance of potential trips. The gradual/sudden adjustments in the OPI and SPI, particularly in transitions between membership zones, reflect the progressions of special causes, enabling operators to act, and/or alert operations management to prevent potential trips.

Next, new techniques for the efficient tracking of vast amounts of near-miss information are introduced.

4. Tracking and Analysis of Abnormal Events

Near-misses are natural leading indicators of incidents related to the safety, health, environmental efficiency, and security of chemical processes.[3,51] Because they possess the potential to evolve into accidents, risk analysts can proactively track their frequencies and learn from the patterns displayed over time. As mentioned earlier, a case study at Norsk Hydro[6] shows that when near-miss reporting over 13 years was increased from 0 to 0.5/person·year, lost-time injuries decreased by approximately 75%.

Herein, the abnormal events (departures of the process and quality variables from their normal operating ranges) are "near-misses". The premise is that the number of abnormal events experienced by the variable(s) and their associated recovery times (to return to their normal operating ranges) are effective measures of safety and operational difficulties experienced by

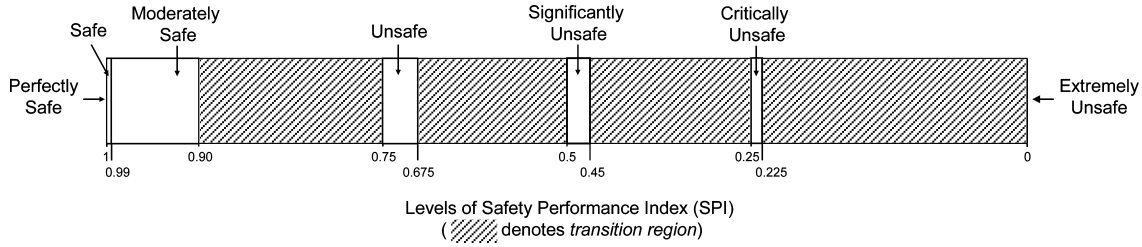

Figure 7. Levels of the safety performance index, SPI, and their associated ranges.

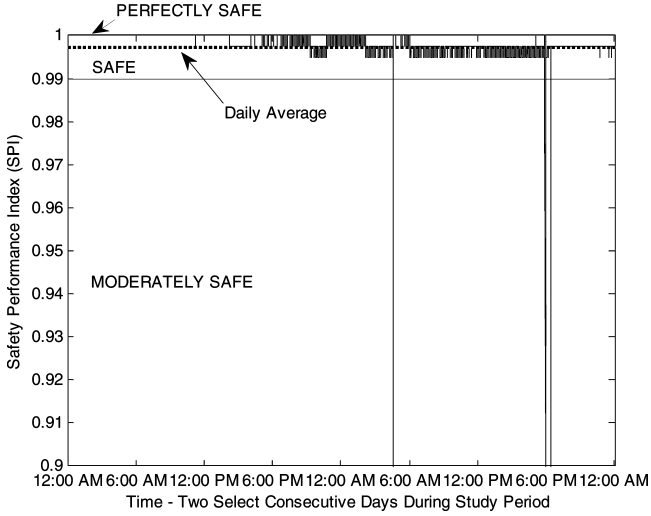

Figure 8. Profile of safety performance index, SPI, from 0.9 to 1 for the FCCU over two consecutive days. Also shown are the membership zones, their threshold levels, and the daily average.

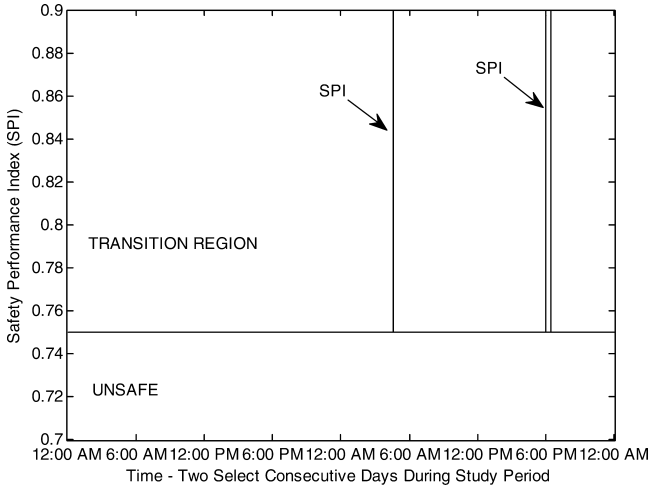

Figure 9. Profile of the safety performance indicator, SPI, from 0.7 to 0.9 for the FCCU over two consecutive days, along with the membership zones and the transition region.

individual and groups of variables. By tracking the frequency of abnormal events and their recovery times, comparisons with past performances and related variables are possible. Then, steps can be taken to reduce the frequency of abnormal events and their associated recovery times, thereby improving the safety, quality, and operability performances; for example, by improving the process designs and control strategies; by improving the operator training, by regularly updating the alarm thresholds to reduce the occurrence of false-positive abnormal events, and consequently, reduce alarm flooding, etc.—factors likely to mitigate the occurrence of incidents as well.

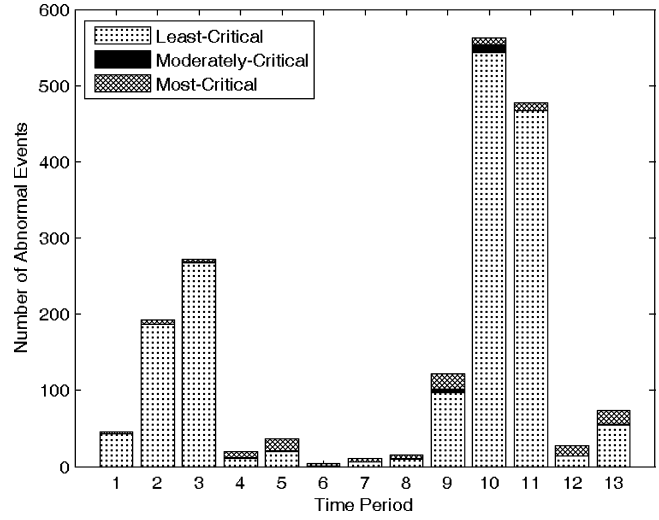

Figure 10. Frequency of least-, moderately-, and most-critical abnormal events for P_1.

Next, the tracking of abnormal events is discussed, followed by alarm system analysis, with results presented for the FCCU case study. Both the DCS and ESD databases are used for the overall time period divided into 13 equal periods, labeled as 1−13. The results are presented in the form of *key performance indicators* for the unit. Note that during time periods 10 and 11, the FCCU was in "special operations" mode due to the shutdowns for repairs of a related column and reboiler—with its feed rate reduced below the design minimum. Consequently, the catalyst circulation rate, a key parameter for stable operation, was low, causing the unit to be quite unstable.

4.1. Tracking of Abnormal Events. Abnormal events tracking can be performed for individual as well as groups of variables. The next few graphs present information for the individual primary variables, P_k, beginning with P_1 in Figure 10. Note that the operability performance for a process is inversely proportional to its operational difficulties, measured by the number of abnormal events, as discussed in section 3. Figure 10 compares the operational difficulties experienced by P_1 for 13 consecutive time periods—permitting management to focus on periods with inferior performances. Note that the significant increases in the abnormal events in time periods 10 and 11 were anticipated due to the planned special operations, mentioned above.

Over this study period, P_1 accounted for nearly 91% of the abnormal events associated with the primary variables, most of which were least-critical, as anticipated in the safety pyramid (Figure 1). Note, however, that the frequency of the most-critical abnormal events exceeds that of the moderately critical abnormal events, an unanticipated result. Consequently, when P_1 crosses its second alarm layer (low-low or high-high), it is more likely to cross its ESD limit (and be termed a most-critical abnormal event) than to return to its yellow-belt zone (and be termed a

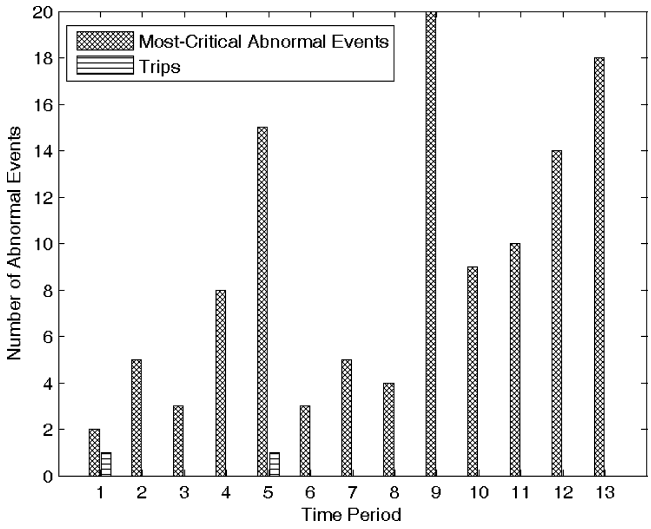

Figure 11. Number of most-critical abnormal events and trips for P_1.

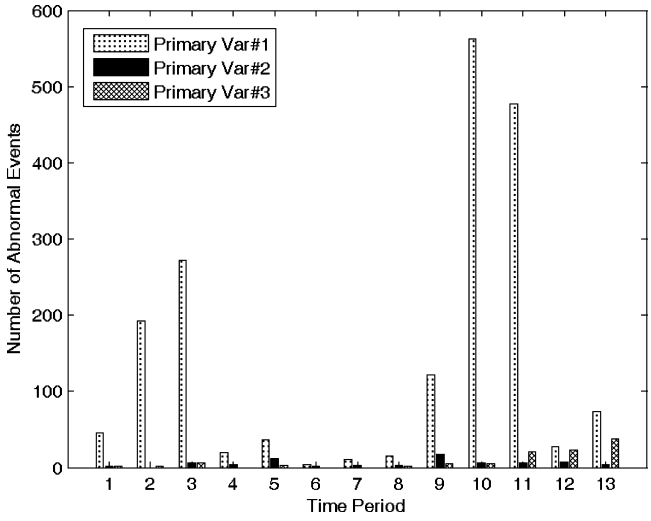

Figure 12. Comparison of frequencies of abnormal events (all criticalities) for the primary variables.

moderately critical abnormal event). Also, there is no significant correlation between the frequencies of the least- and most-critical abnormal events; that is, a high number of least-critical abnormal events for P_1 in a time period may or may not be accompanied by a high number of most-critical abnormal events.

Note that P_1 has an advanced override controller, which is activated when the variable moves beyond its ESD limits, with radical controlling actions taken to move the variable from its red-belt zone, preventing the occurrence of an emergency shutdown. After 30 s, when the override controller is unsuccessful in moving the variable from its red-belt zone, emergency shutdown occurs. For the other primary variables, the time delay is 2 s (to filter the noise) and no override controllers are used. For P_1, Figure 11 shows that the most-critical abnormal events rarely result in trips, primarily due to the robust actions of the override controller. Only 2 trips occurred: one in the first time period and the other in the fifth time period.

Similar results are available for the other primary variables. A comparison of the frequencies of the abnormal events (including all criticalities) for the top three primary variables is presented in Figure 12. The number of abnormal events for P_2 and P_3 are less than an order of magnitude below those for P_1. Clearly, the former are relatively stable variables that experience few abnormal events—thanks to robust controllers and the inherently safe FCCU design. Note that 97.5% of the most-critical abnormal events were associated with P_1, which justifies its override controller due to such a high rate of abnormal events.

Similar results are available for groups of variables (e.g., the primary variables, high-priority secondary variables, medium-priority variables, etc.) and can be obtained for other groups having similar characteristics.

4.2. Alarm System Analysis. The alarm threshold levels for the variables and the prioritization of alarms are carefully determined during the commissioning of plants. With numerous variables monitoring the process dynamics and alarms, notifying the plant operators of the many shifts among the operating-belt zones, poorly configured alarms frequently result in false-positive and -negative abnormal events. These can overwhelm the operators, leading to distractions and stress. Note that due to the nonlinear, causal relationships among variables, the special causes can lead to ignition effects, often resulting in alarm flooding due to correlated alarms. These interdependent effects due to interactions are typically accounted for in the design of DCSs that can implement multivariable controllers, such as multivariable model-predictive controllers (MPCs), that can handle the interactions more effectively than multiple single-input, single-output (SISO) controllers.

Before a new approach to alarm-system analysis is presented, the most common types of alarms, employed in the industries are presented below, with their threshold limits shown schematically in Figures 2 and 3:

a. Low alarm (LO): this alarm is associated with the DCS. It is triggered when any process or quality variable crosses its predefined low limit; i.e., moves from its green- to yellow-belt zone.
b. High alarm (HI): this alarm is associated with the DCS. It is triggered when any process or quality variable crosses its predefined high limit (i.e., moves from its green- to yellow-belt zone). In particular, when any manipulated process or quality variable crosses its predefined high limit, a *manipulated high alarm* is triggered. An example is a high alarm associated with a valve-opening variable, used to manipulate the valve when controlling the bulk temperature of the reactor.
c. Low-low alarm (LL): this alarm is associated with the DCS. It is triggered when any process or quality variable crosses its predefined low-low limit; i.e., moves from its yellow- to orange-belt zone.
d. High-high alarm (HH): this alarm is associated with the DCS. It is triggered when any process or quality variable crosses its predefined high-high limit (i.e., moves from its yellow- to orange-belt zone).
e. Timer alerts: when any variable moves above or below its ESD thresholds, the ESD system takes over from the DCS. This ensures that the ESD system acts as an independent protection system, uninfluenced by a malfunctioning DCS. For every primary variable, the number of redundant measurements depends on the safety integrity level (SIL). When any primary variable crosses its ESD thresholds (i.e., moves into its red-belt zone), alarms associated with these measurements, referred to as *timer alerts*, are triggered.

Depending upon the safety, profitability, quality and controllability objectives, often defined during the commissioning of plants, additional layers of DCS alarms, for example, high-high-high (HHH) and low-low-low (LLL) alarms, are occasionally defined.

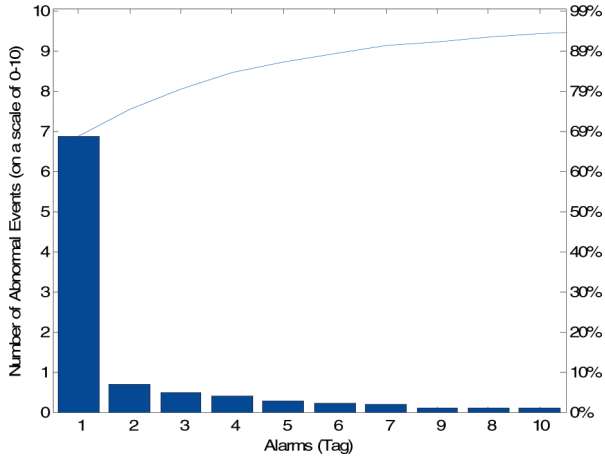

Figure 13. Pareto chart showing top 10 high-priority variables (with associated alarm tags on the abscissa) having the most prevalent alarms for the study period.

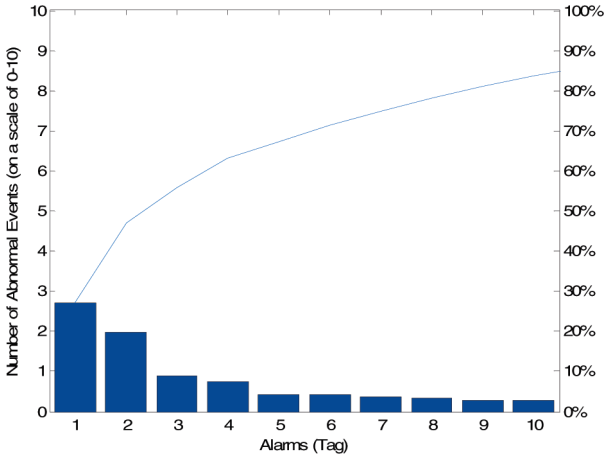

Figure 14. Pareto chart showing top 10 high-priority secondary variables (with associated alarm tags on the abscissa) having the most prevalent alarms during the study period.

Next, the new alarm-system analysis is presented, for use eventually in reducing the frequencies of unwanted alarms, optimizing the number of alarm types, and facilitating alarm system management, etc.[14–32]

Figures 13 and 14 present Pareto charts showing the top 10 (1) high-priority and (2) high-priority secondary variables having the most prevalent alarms, with the ordinate showing the scaled number of abnormal events for the overall study period. As observed in Figure 13, P_1 accounts for nearly 70% of the total abnormal events associated with the high-priority variables, whereas in Figure 14, the three variables having the most alarms account for nearly 60% of the abnormal events associated with the high-priority secondary variables. Note that the curves give the cumulative total of the alarms from left-to-right. Similarly, individual alarms can be tracked for each variable, over extended periods, with the highest frequencies identified for investigation purposes. Of special note, Figure 15 shows the frequency of the alarm types (i.e., LO, HI, MHI, LL, etc.) associated with the top 10 high-priority secondary variables (having the most prevalent alarms during the study period). Note that the IOP and IOP-alarms indicate invalid scale ranges when a measurement is in the close proximity of its limiting values. In these cases, a recalibration can be performed. Also, note that for the variables associated with alarm tag nos. 1−3, 5, 6, and 9, the majority of the abnormal events, are least-critical in nature. By (1) using a tighter control strategy, (2) making changes in the process designs and/or operating regimes, (3) updating the alarm thresholds to reduce the occurrence of false-positive abnormal events, or (4) relaxing high-low alarm thresholds for the less important variables, the frequency of the least-critical abnormal events associated with these variables can be reduced significantly—reducing the overall frequency of alarms associated with the high-priority secondary variables by almost 65%—and helping the operators focus on the more important alarms and messages. Again, because this analysis was carried out several months after the data became available, none of these improvements could be actually implemented and tested in our work. However, it is clear that a real-time implementation will likely result in improvements.

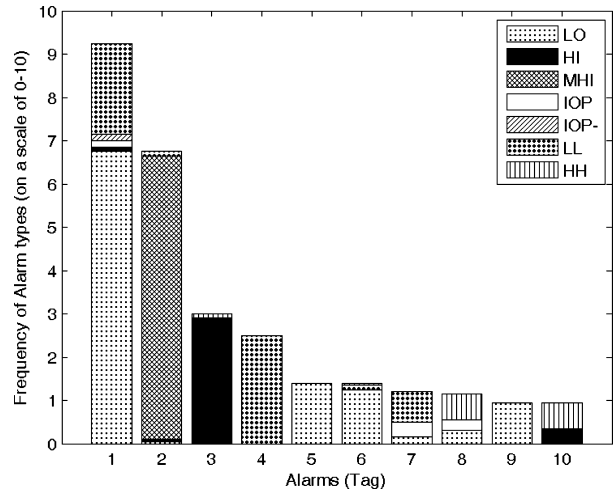

Figure 15. Frequency of alarm types for top 10 high-priority secondary variables (with associated alarm tags on the abscissa) having the most prevalent alarms for the study period.

Again, similar analyses are possible for the medium- and low-priority variables. Hence, these analyses of the abnormal events are useful for comparative assessment and improvement of the performance of a process on a timely basis. They permit identification of variables that experience excessive numbers of abnormal events, drawing the attention of plant management to potential improvements in control strategies, alarm thresholds, and process designs. This approach improves upon alarm management techniques by drawing attention to the severity of abnormal events experienced by variables and their associated recovery times. It better quantifies the near-misses experienced by the individual variables and the effectiveness of the individual alarm limits. This method supplemented with the event-balance trend graph[52] can be used to reduce alarm-flooding considerably.

5. Recovery-Time Analysis using Dynamic Databases

In this section, a detailed recovery-time analysis of the abnormal events using the DCS and ESD system databases during the study period is presented. This analysis helps to identify variables with high recovery times, indicating the presence of special causes that potentially cause off-specification product-quality and safety problems.

As discussed earlier, when any variable moves from its green-belt zone (normal operating zone) to its yellow-, orange-, or red-belt zones, the start of an abnormal event is recorded. Furthermore, the time to return to its green-belt zone is the recovery time for its abnormal event. In general, the recovery time depends upon (1) the speed of corrective actions by the operators (human + machine), (2) the severity of the fault or special cause, and (3) the dynamics of the process, among other

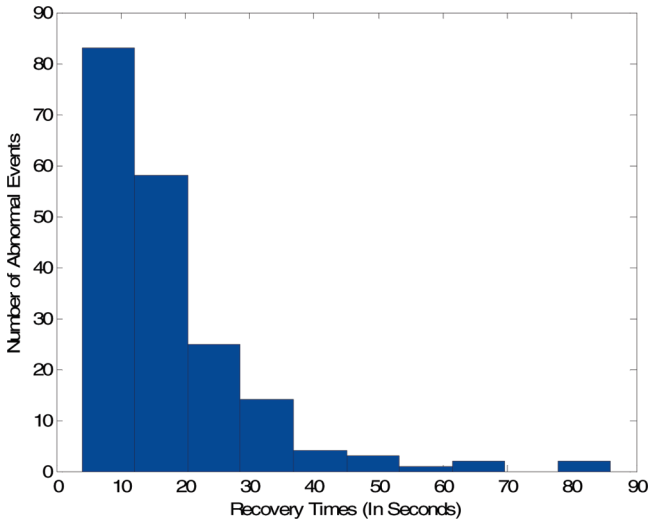

Figure 16. Histogram of recovery times for abnormal events associated with the P_1 for time period 2.

factors. For a given variable, over a time period, a distribution of recovery times for its associated abnormal events is obtained. One such distribution (histogram) is presented in Figure 16 for P_1, during the second time period, in which 192 abnormal events occurred (of all criticalities). Although, most of the abnormal events recovered within 20 s, a sizable number required more time, some as much as 90 s. For most variables, similar histograms have this positively skewed distribution; that is, concentrated toward the left with long tails to the right.

To characterize these histograms, the mean, standard deviation, median, and interquartile range are typically calculated. The mean is defined as the sum of the recovery times for all of the abnormal events divided by the total number of abnormal events. The *standard deviation* describes the spread of the distribution. The median separates the upper half from the lower half of the distribution. It is quoted with the *interquartile range*—the difference between the 75th percentile and 25th percentile values—another measure of the spread of the distribution. Note that the presence of outliers tends to create more positively skewed time distributions; that is, time distributions having longer right tails. However, the extent of skewness depends on the number of abnormal events per period—when large, the outliers have little impact on the mean and standard deviation, and when small, these values are increased. Also note that, unlike the mean and standard deviation, the median and interquartile range are not significantly affected by outliers (which are observations numerically distant from most of the data points).

In Figure 16, the average recovery time is 17.5 s and the standard deviation is 12.7 s; that is, for the majority of its abnormal events during the second time period, P_1 returned to its green-belt zone within 4.8 and 30.2 s. The median recovery time was 14 s, and the interquartile range was 11 s. In the next subsection, recovery-time analysis for P_1 is presented, followed by box-and-whisker plots. Similar analyses can be performed for individual and groups of variables.

5.1. Recovery-Time Analysis for Primary Variable 1 (P_1). Figure 17 presents the average recovery times, period-by-period, for abnormal events associated with P_1 during the total study period. The recovery time means are close, between 17 and 27 s, except for the fifth time period, having the highest mean of 47 s. Note that time periods with more abnormal events tend to have lower average recovery times and vice versa.

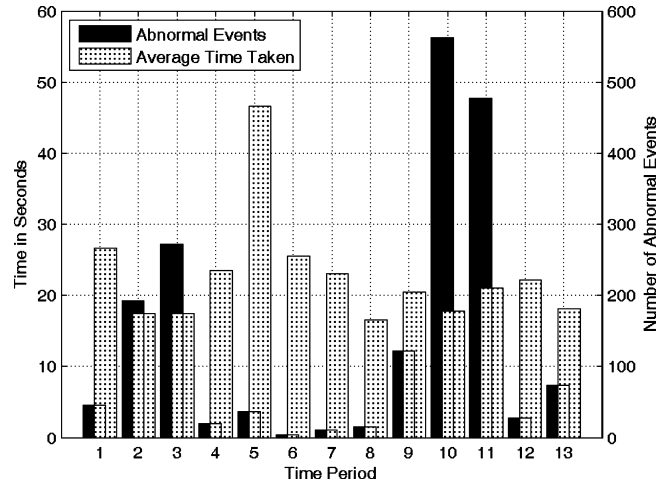

Figure 17. Average recovery times for abnormal events associated with P_1 during the study period.

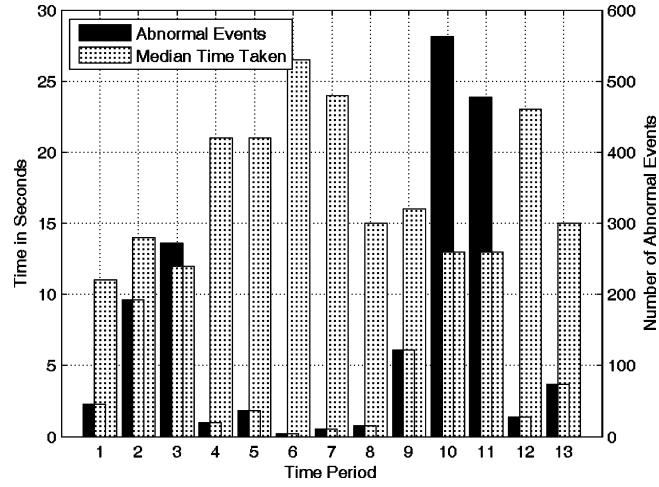

Figure 18. Median recovery times for abnormal events associated with P_1 during the study period.

To verify that the values presented in this figure are resistant to the outliers (i.e., not significantly affected), consider the fifth time period, which experienced only 36 abnormal events, but had the highest average recovery time of 47 s. The median of the recovery times for the abnormal events in this time period was 21 s. Consequently, for 18 of the 36 abnormal events, the recovery times were less than 21 s, while the remaining 18 had much higher recovery times—which increased the average value to 47 s. This observation may be helpful when interpreting the statistical results.

Figure 18 presents the median values of the recovery times for abnormal events associated with P_1 during the total study period. In this case, the sixth time period experienced the highest median value of 26 s.

Next, Figure 19 compares the average recovery times for least-, moderately-, and most-critical abnormal events along with the overall average value (horizontal line) for P_1 during the entire study period. As observed, the average recovery times associated with the moderately- and most-critical abnormal events are more than double those associated with the least-critical abnormal events. Also, because most of the abnormal events associated with P_1 are least-critical, their small recovery times significantly reduce the overall average.

Similarly, Figure 20 compares the median of recovery times associated with abnormal events of different criticalities for P_1 during the study period. In both the cases, the overall values

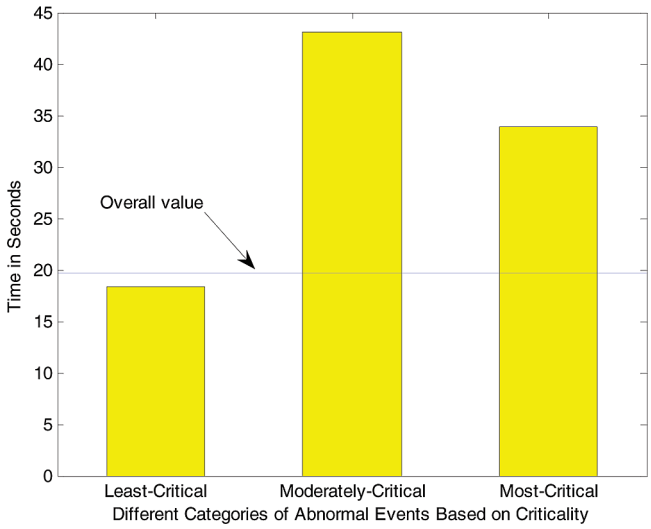

Figure 19. Comparison of average recovery times for abnormal events of different criticalities associated with P_1 over the study period.

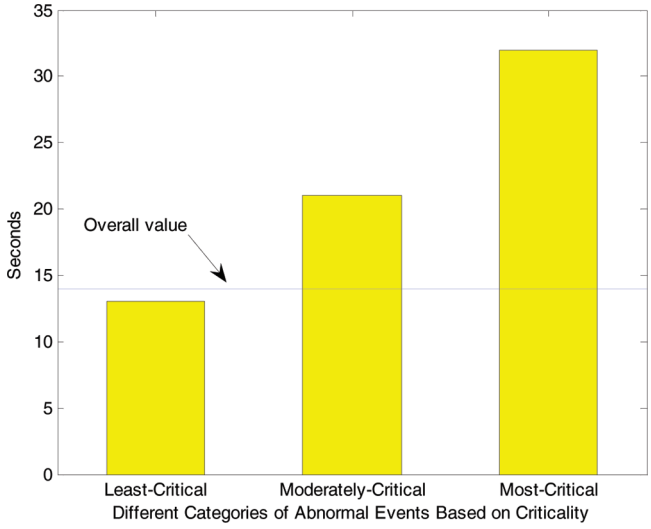

Figure 20. Comparison of median recovery times for abnormal events of different criticalities associated with P_1 during the study period.

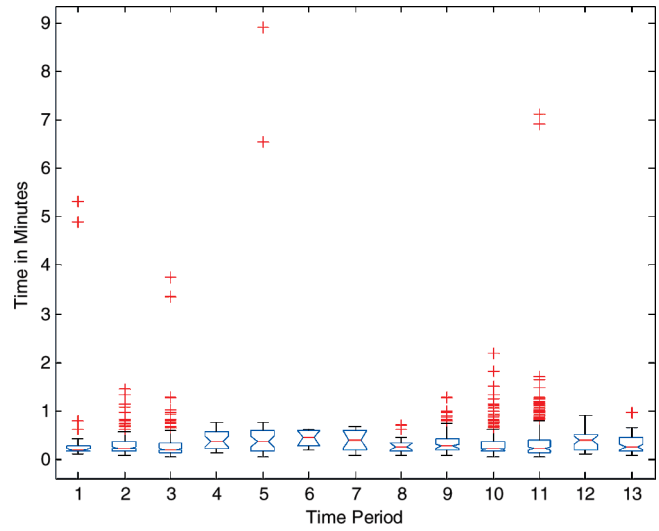

Figure 21. Box plots of recovery times for abnormal events associated with P_1 during the study period.

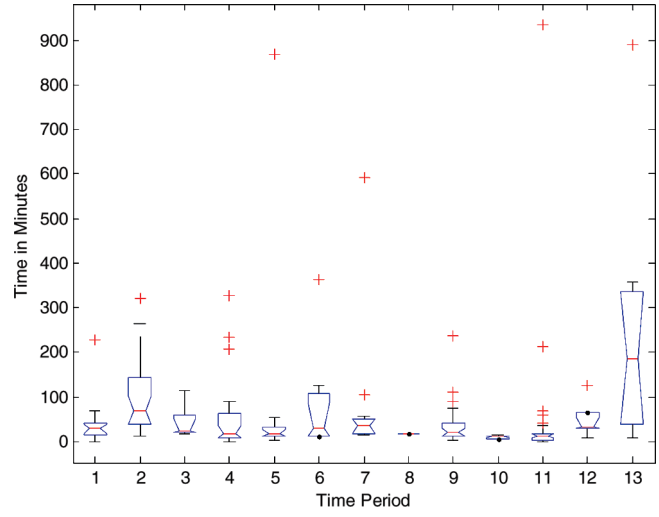

Figure 22. Box plots of recovery times for abnormal events associated with S_1 during the study period.

are close to the corresponding values associated with the least-critical abnormal events. Notice that the overall mean is higher than the overall median, primarily because of the high recovery times of the outliers.

5.2. Box and Whisker Plots. In this subsection, an alternative visualization of recovery times, using *box and whisker plots*,[53] is presented—a useful way to analyze the spread of data period-by-period. To define the symbols, first view Figures 21 and 22, which display recovery time data for abnormal events associated with P_1 and the secondary variable 1 (S_1; flow rate of regenerated flue gas). In these figures, the ordinate is the time in minutes. For each period, six measures associated with its recovery-time distribution are displayed, beginning with the first (1), the outliers, shown as + signs, which are observations numerically distant from most of the data. Statistically, an outlier is any data observation that lies more than 1.5IR lower than the first quartile or higher than the third quartile, where IR is the interquartile range. After the outliers are removed, the two measures (2, 3), the smallest and largest nonoutliers observations, are displayed using horizontal lines in blue or "whiskers". The next two measures (4, 5) are the 25th and 75th percentile values, shown at the ends of the enclosed box in blue. Note that the difference between 75th and 25th percentile values is the interquartile range. And, finally, the last measure (6) is the median, shown as a red horizontal line.

Figures 21 and 22 highlight the outliers and display the relative differences between the medians from period-to-period. The outliers, especially, deserve special attention—possibly at the management level. Note that, in Figure 22, the best performance for the first secondary variable, S_1, was observed in time periods 8 and 10, with the smallest recovery times, no outliers, and small median values. Similar analyses can be displayed for other variables and for groups of variables.

5.3. Identification of Variables with the Highest Recovery Times. Figure 23 displays the average recovery times and the number of abnormal events for the high-priority secondary variables, with alarm tags on the abscissa, having the 10 highest average recovery times. The variable having the highest average recovery time was a differential pressure variable, which experienced 50 abnormal events during the study period. Clearly, its unusually high average recovery time indicates operational difficulties—suggesting that plant management undertake a study of its possible root-causes. Factors like outdated process designs and alarm thresholds, and poor control strategies might be responsible. In either case, regular performance assessments (using concepts discussed in sections 2, 3, and 4) are recom-

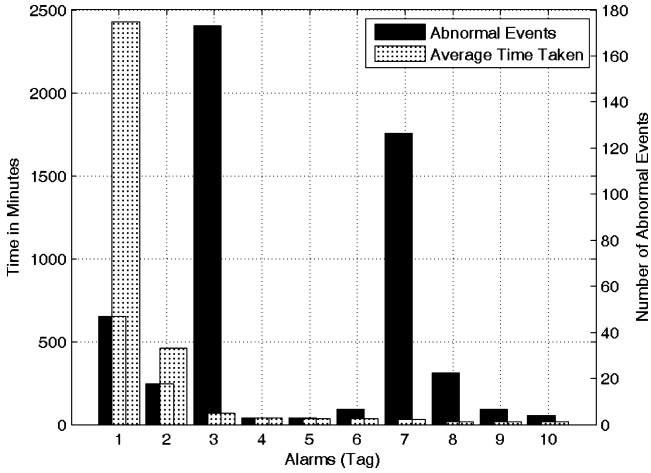

Figure 23. High-priority secondary variables having the 10 highest average recovery times for their abnormal events over the study period.

mended to reduce the associated profit losses and to improve the overall plant operability performance.

The variable having the third highest average recovery time, 68 min, also experienced the highest number of abnormal events among the high-priority secondary variables during the study period. Note that, the average values for high-priority secondary variables are calculated to be almost an order of magnitude higher than their median values—primarily because some of the abnormal events associated with the high-priority secondary variables had very high recovery times leading to high average values—possibly due to reduced operator (both human and machine) attention—due to the secondary nature of these alarms.

If desired, similar analyses can be carried out for the medium- and low-priority variables.

To conclude this section, the recovery-time analysis of abnormal events is a useful technique to improve the operability performance of the process. Variables experiencing abnormal events with high recovery times deserve special attention by the operators and management. Clearly, the performances of the variables depend on the DCS, controller tuning, the alarm system configuration, and the process design. Yet, a higher number of abnormal events, with low OPI and SPI, and high recovery times lead to an increased recognition of near-misses—alerting operators and management to consider corrective actions; e.g., to improve the (1) DCS configuration and its tuning, (2) operating regimes, (3) process design, and (4) alarm system configuration.

6. Profit Losses Associated with Abnormal Events

Near-misses have associated costs, which are not usually accounted for because they are difficult to estimate quantitatively. For example, when high-high alarms are triggered, they may or may not lead to profit losses, depending upon the override control system, operator actions, and the like. Also, near-misses have different impacts. While they usually adversely affect the product quality, they can also reduce the production rate, require more operators to avoid serious consequences, and when plant shutdowns cause product-delivery delays, negatively affect a company's reputation.

As discussed in sections 2−5, abnormal events deteriorate the operability performance, with the potential to reduce the safety and quality performances, increasing profit losses. Consequently, every abnormal event of any variable is associated with a profit loss (PL), with PLs as functions of the times the process and quality variables remain outside of their normal operating ranges (green-belt zones). Using the performance assessment techniques introduced above, new techniques to estimate profit losses due to abnormal events will be presented in our future work. Our initial calculations show negative impacts of near-misses on profitability, and consequently, the benefits of identifying and acting upon them. It is expected that profit and sales losses data will be incorporated to estimate the costs of near-misses.

7. Summary and Conclusions

Novel techniques to identify and utilize near-miss information from DCS and ESD databases for processing units—to assess and improve their safety and operability performances—were presented. A four-stage modeling framework depicting the chronology of incidents was described, which expands upon the relationship of near-misses and accidents in the safety pyramid (Figure 1) and includes the origin of the special causes and actions of the SQOSs. This framework emphasizes that near-misses are precursors to incidents and there are benefits in tracking and acting upon them.

Performance indices were introduced to assess quantitatively and qualitatively the safety and operability performances of any process unit in real-time and were successfully applied to the FCCU. Also, techniques to track the abnormal events for different time periods were presented, suggesting potential opportunities to explore their root causes. These tracking tools also suggest alarm-system analyses, leading to a reduction in the frequencies of unwanted alarms—through optimizing the number of alarm types, regularly updating/reconfiguring the alarm thresholds and ESD limits, changing the control strategies and/or process designs, etc. Pareto charts and alarm-type frequency diagrams were presented to display effectively the results of alarm system analysis for the large set of FCCU variables.

Furthermore, a recovery-time analysis of the abnormal events was presented. For most of the variables, recovery times have similar positively skewed distributions; that is, concentrated toward the left with long tails to the right. Statistical measures like mean and median were calculated for primary and secondary variables and analyzed for the study period to obtain various inherent trends and characteristics of the FCCU. An alternative way to visualize recovery times, known as box and whisker plots, was also discussed. The plots were shown to be useful in analyzing the spread of data period-by-period and identifying outliers for any time period. From the analysis, it was concluded that variables experiencing abnormal events with high recovery times deserve special attention by the plant personnel and management; for example, by updating/reconfiguring the alarm thresholds and changing the controller settings.

Finally, the results presented herein provided insights into the capabilities and characteristics of these techniques, which are applicable to any process—large- or small-scale, batch, semibatch, or continuous.

Acknowledgment

Partial support for this research from the National Science Foundation through grant CTS-0553941 is gratefully acknowledged.

Appendix

Consider a typical FCC unit shown in Figure 24 that catalytically cracks unconverted oil from a hydrocracking unit and heavy-vacuum gas-oil feed, into lighter, more valuable

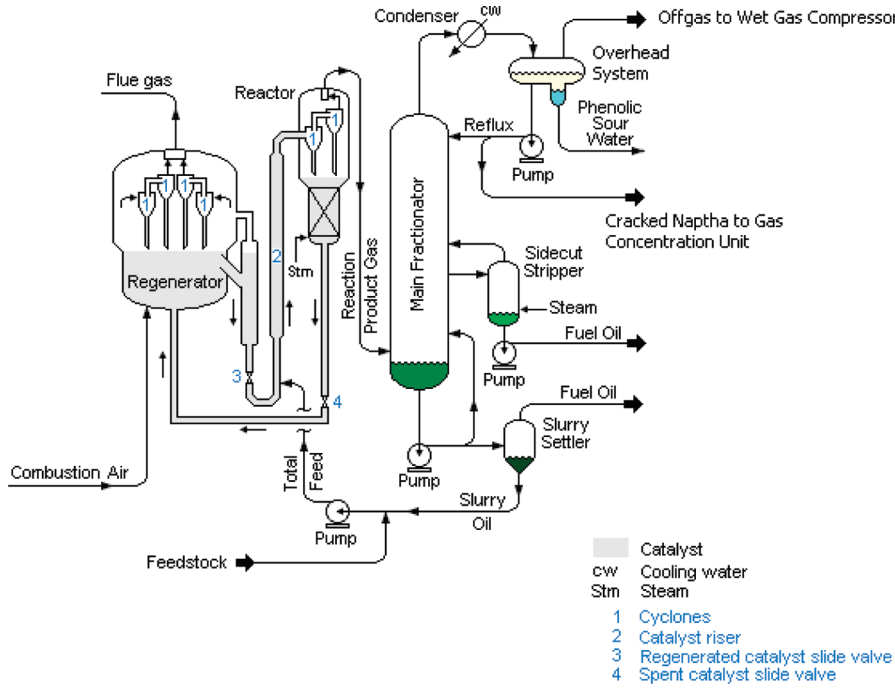

Figure 24. Typical fluid catalytic cracking unit (FCCU).[54]

products (that is, high-octane gasoline, naphtha, and fuel oils), using a specialized catalyst (solid) maintained in a suspension or fluidized state by reaction products, air, or steam in the reactor, regenerator, and catalyst transfer lines. The cracking process takes place in the *catalyst riser*, where the feed is vaporized and cracked into small molecules using hot regenerated catalyst from the *regenerator*. At the end of the riser, spent catalyst and product are separated by the *reactor* cyclones. Catalyst is directed to the stripping section, where hydrocarbons are stripped off from the spent catalyst. The reaction product gas proceeds to the main fractionator for condensation and product separation, whereas the spent catalyst proceeds to the regenerator, where the deposited coke is burned off. The regenerator cyclones then separate the catalyst from the flue gas and the hot regenerated catalyst returns to the riser. Note that the regenerator provides heat for the cracking reaction via hot regenerated catalyst, and in turn, the reactor provides the fuel for the regenerator in the form of deposited coke. And, therefore, changes in the operation (pressures, temperatures, etc.) of one unit impact the catalyst circulation and affect the operation of the other unit.

Twenty-four process and seven quality variables are monitored in this unit, and four of its process variables and three of its quality variables are associated with the emergency shutdown (ESD) system. These seven variables are therefore referred to as primary variables, with primary process variables denoted as pP_1, pP_2, pP_3, and pP_4 and primary quality variables as pQ_1, pQ_2, and pQ_3. Typically, the primary process variables are the pressure drops in the stand pipes, the reactor temperature, and the like, as they are the most important variables that govern the safety of the cracking process and the quality of the products—and the choice of the primary quality variables tends to vary from plant-to-plant. The remaining variables that are not associated with the ESD system are referred to as secondary process and quality variables and denoted as sP_1, sP_2, ..., sP_{20}, and sQ_1, sQ_2, sQ_3, and sQ_4. These variables are summarized in Table 5.

To assist the operators (human + machine) during upset states, alarms (and consequently, variables) are prioritized as high-, medium-, and low-priority alarms. The high-priority variables usually consist of all of the primary variables and some of the secondary variables (20−25%). Thus, for the above example, the high-priority variables include pP_1, pP_2, pP_3, pP_4, pQ_1, pQ_2, pQ_3, and approximately 5−7 secondary variables, which are referred as high-priority secondary variables. The remaining secondary variables are designated as either medium- or low-priority variables.

Table 5. Categories of Variables for a Typical FCCU

variables	primary (associated with ESD system)	secondary (not associated with ESD system)
process	pP_1, pP_2, pP_3, pP_4	sP_1, sP_2, ..., sP_{20}
quality	pQ_1, pQ_2, pQ_3	sQ_1, sQ_2, sQ_3, sQ_4

Nomenclature

Acronyms

APCS = advanced process control system
BPCS = basic process control system
CO = continued operation
CPI = chemical process industries
DCS = distributed control system
ESD = emergency shutdown
FCCU = fluid catalytic cracking unit
HI = high alarm
HH = high-high alarm
HMI = human−machine interface
HP = high-priority
IOP, IOP- = input open errors
LC = least-critical
LO = low alarm
LL = low-low alarm
LP = low-priority
MC = most-critical
MDC = moderately critical
MHI = manipulated high alarm
MP = medium-priority
OOUS = operability-only upset state

OPI = operability performance index
PFD = probability of failure under demand
PL = profit losses
PSF = performance shaping factor
QM = quality meltdown
QUS = quality upset state
RA = runaway reaction
RRF = risk reduction factor
SIL = safety integrity level
SPI = safety performance index
SQOS = safety, quality, and operability systems
SUS = safety upset state
S+QUS = safety and quality upset state

English letters

A_{HP,P_k} = impact parameter for a high-priority primary variable, P_k
AE_i = number of abnormal events associated with variables of category i
f_i = ratio of number of variables of category i out of their normal operating ranges to the total number of variables of category i
G = green-belt zone
N_i = total number of variables of category i
O = orange belt-zone
P_k = primary variable k
R = red-belt zone
S_k = secondary variable k
t_k = recovery times in Figure 2
w_i = normalized weighting factor for variables of category i
w_{HP,P_k} = normalized weighting factor for high-priority, primary variable P_k
Y = yellow-belt zone

Subscripts

i = counter for category of variables [high-priority (HP), medium-priority (MP), low-priority (LP)]
j = counter for operating belt-zone [green (G), yellow (Y), orange (O), red (R)]
k = primary variable index counter

Superscripts

j = counter for operating belt zone [green (G), yellow (Y), orange (O), red (R)]
l = counter for criticality of abnormal events (most-, moderately-, or least-critical)

Literature Cited

(1) Meel, A.; Seider, W. D. Plant-Specific Dynamic Failure Assessment using Bayesian Theory. *Chem. Eng. Sci.* **2006**, *61*, 7036.

(2) Yi, W.; Bier, V. M. An application of copulas to accident precursor analysis. *Manage. Sci.* **1998**, *44* (12), S257.

(3) Phimister, J. R.; Oktem, U. G.; Kleindorfer, P. R.; Kunreuther, H. Near-miss incident management in the chemical process industry. *Risk Anal.* **2003**, *23*, 445.

(4) Rosenthal, I.; Kleindorfer, P. R.; Elliott, M. P. Predicting and confirming the effectiveness of systems for managing low-probability: Chemical process risks. *Proc. Safety Prog.* **2006**, *25* (2), 135.

(5) Cooke, D. L.; Rohleder, T. R. Learning from incidents: from normal accidents to high reliability. *System Dynam. Rev.* **2006**, *22* (3), 213.

(6) Jones, S.; Kirchsteiger, C.; Bjerke, W. The importance of near miss reporting to further improve safety performance. *J. Loss Prevention Process Ind.* **1999**, *12* (1), 59.

(7) Bullemer, P.; Nimmo, I. Tackle abnormal situation management with better training. *Chem. Eng. Progress* **1998**, *94* (1), 43.

(8) Bullemer, P. T.; Nimmo, I. Understanding and supporting abnormal situation management in industrial process control environments: a new approach to training. Proceedings of the 1994 *IEEE International Conference on Systems, Man, and Cybernetics. Part 1 (of 3)*; San Antonio, TX, October 2−5, 1994; Vol. 1; p 391.

(9) Brown, D. C.; O'Donnell, M. Too much of a good thing? Alarm management experience in BP oil. Part 1: Generic problems with DCS alarm systems. *IEE Colloquium (Digest)* **1997**, *136*, 5/1.

(10) Nimmo, I. Abnormal situation management in the petrochemical industry. *Instr. Chem. Pet. Ind., Proc.* **1996**, *26*, 77.

(11) Nimmo, I. Industry initiative addresses 'abnormal events'. *Hydrocarbon Process.* **1998**, *77* (10), 71.

(12) Nimmo, I. Adequately Address Abnormal Situation Operations. *Chem. Eng. Progress* **1995**, *91* (9), 36.

(13) Andow, P. Abnormal situation management: A major US programme to improve management of abnormal situations. *IEE Colloquium (Digest)* **1997**, *136*, 3/1.

(14) EEMUA. *Alarm systems - a guide to design, management and procurement*; EEMUA (Engineering Equipment and Materials Users' Association) publication: London, 2007.

(15) Smith, H.; Howard, C.; Foord, T. Alarms management - Priority, floods, tears or gain? Introduction to the "problem. *Measure. Control.* **2003**, *36* (4), 109.

(16) Goble, G.; Stauffer, T. R. Don't be Alarmed: Avoid unplanned downtime from alarm overload, use top techniques to improve alarm management. *InTech Magazine* **2007**, January;http://www.isa.org/InTechTemplate.cfm?Section=article_index1&template=/ContentManagement/ContentDisplay.cfm&ContentID=58395.

(17) ARC White Paper, Emerson Strategies for Abnormal Situation Avoidance & Alarm Management. http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/Whitepapers/WP_ARC_Alarm_Mgt.pdf.

(18) Katzel, J. Managing alarms. *Control Eng.* **2007**, *54* (2), 50.

(19) Errington, J.; DeMaere, T.; Reising, D. V. After the alarm rationalization - Managing the DCS alarm system. *AIChE Spring National Meeting, Conf. Proc.* **2004**, 1234.

(20) Brown, N. Effective alarm management. *Hydrocarbon Process.* **2004**, *83* (1), 65.

(21) Brown, N. Alarm management - The EEMUA guidelines in practice. *Measure. Control* **2003**, *36* (4), 114.

(22) Nimmo, I. Alarm overload. *Chem. Process.* **2005**, *68* (1), 28.

(23) Wilkinson, J.; Lucas, D. Better alarm handling - a practical application of human factors. *Measure. Control* **2002**, *35* (2), 52.

(24) Wilson, M. Alarm management and its importance in ensuring safety. *IEE Colloquium (Digest)* **1998**, *279*, 6/1.

(25) Bransby, M. L.; Jenkinson, J. Alarm management in the chemical and power industries-a survey for the HSE. *IEE Colloquium Stemming Alarm Flood (Digest)* **1997**, *136*, 1/1.

(26) Marvan, M. Alarming blunders: What not to do in alarm management. *ISA EXPO 2005 Technical Conference*, Chicago, IL, October 25−27, 2005; Vol. 459, p 884.

(27) Srinivasan, R.; Liu, J.; Lim, K. W.; Tan, K. C.; Ho, W. K. Intelligent alarm management in a petroleum refinery. *Hydrocarbon Process.* **2004**, *83* (11), 47.

(28) Gaertner, D. Bringing nuisance alarms under control. *Control Eng.* **2007**, *54* (3), IP10.

(29) Kettschau, H.-J.; Brück, S.; Schefczik, P. LUCAS - An expert system for intelligent fault management and alarm correlation. *IEEE Symposium Record on Network Operations and Management Symposium*, Florence, Italy, April 15−19, 2002; p 903.

(30) Bransby, M.; Jenkinson, J. *The management of alarm systems (Contract Research Report)*; HSE (Health and Safety Executive) Books: Sudbury, U.K., 1998.

(31) Easter, J. R.; Haentjens, J. Advanced alarm management system. Advanced Control and Instrumentation Systems in Nuclear Power Plants. Design, Verification and Validation. *IAEA/IWG/ATWR & NPPCI Technical Committee Meeting (VTT-SYMP-147)*, Espoo, Finland, June 20−23, 1994; p 199.

(32) Mattiasson, C. T. Alarm system from the operator's perspective. Proceedings of the 1999 *International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres*, Bath, U.K., June 21−23, 1999; Vol. 463, p 217.

(33) Swain, A. D.; Guttmann, H. E. *Handbook of human reliability analysis with emphasis on nuclear power plant applications*; US Nuclear Regulatory Commission: Washington, DC, 1983; NUREG/CR-1278.

(34) Bustamante, E. A.; Bliss, J. P.; Anderson, B. L. Effects of varying the threshold of alarm systems and workload on human performance. *Ergonomics* **2007**, *50* (7), 1127.

(35) Cullen, L.; Anderson, M. Human factors integration for a new top tier COMAH site - Optimizing safety and meeting legislative requirements. *Process Safe. Environ. Protec.* **2005**, *83* (B2), 101.

(36) HSE. *Reducing error and influencing behaviour (Health and Safety Guidance 48)*; HSE (Health and Safety Executive) Books: Sudbury, U.K., 1999.

(37) Noyes, J., Bransby, M., Ed. Proceedings of *People in Control - Human factors in control room design*; Bath, U.K., June 21−23, 1999; IEE Control Engineering Series: London, U.K., 2002; Vol. 60.

(38) Brabazon, P.; Conlin, H. *Assessing the safety of staffing arrangements for process operations in the chemical and allied industries (Contract Research Report)*; HSE (Health and Safety Executive) Books: Sudbury, U.K., 2001.

(39) Nimmo, I. It's time to consider human factors in alarm management. *Chem. Eng. Prog.* **2002**, *98* (11), 30.

(40) Bullemer, P.; Nimmo, I. Tackle abnormal situation management with better training. *Chem. Eng. Prog.* **1998**, *94* (1), 43.

(41) Mayer, A. K.; Sanchez, J.; Fisk, A. D.; Rogers, W. A. Don't let me down: The role of operator expectations in human-automation interaction. *Proc. Human Factors Ergonomics Soc.* **2006**, 2345.

(42) Pariyani, A.; Seider, W. D.; Oktem, U. G.; Soroush, M. Dynamic Risk Analysis for Synergistic Enhancement of Process Safety and Product Quality using Large Databases: Part I - Theory and Modeling. to be submitted to *AIChE J.* **2010**.

(43) Pariyani, A.; Seider, W. D.; Oktem, U. G.; Soroush, M.; George, E. I.; Jensen, S. Dynamic Risk Analysis for Synergistic Enhancement of Process Safety and Product Quality using Large Databases: Part II - Bayesian Analysis and Results. to be submitted to *AIChE J.*, **2010**.

(44) Brooks, R.; Thorpe, R.; Wilson, J. A new method for defining and managing process alarms and for correcting process operation when an alarm occurs. *J. Hazard. Mater.* **2004**, *115* (1), 169.

(45) Sepeda, A. L. Lessons learned from process incident databases and the process safety incident database (PSID) approach sponsored by the Center for Chemical Process Safety. *J. of Hazard. Mater.* **2006**, *130*, 9.

(46) Grabowski, M.; Ayyalasomayajula, P.; Merrick, J.; Harrald, J. R.; Roberts, K. Leading indicators of safety in virtual organizations. *Safe. Sci.* **2007**, *45*, 1013.

(47) Pariyani, A.; Oktem, U. G.; Seider, W. D. Perceived Root-Cause Survey of Operators at a Major Petroleum Refinery, in preparation.

(48) *Application of Safety Instrumented Systems (SIS) for the Process Industry, Instrumentation, Systems, and Automation Society*, ANSI/ISA S84.01-1996; Instrumentation, Systems, and Automation Society: Research Triangle Park, NC, 1996.

(49) Green, D. L.; Dowell, A. M. How to design, verify and validate emergency shutdown systems. *ISA Trans.* **1995**, *34* (3), 261.

(50) CCPS. *Guidelines for Hazard Evaluation Procedures*, 3rd ed.; Center for Chemical Process Safety/AIChE: New York, 2008.

(51) Oktem, U. Near-Miss: A Tool for Integrated Safety, Health, Environmental and Security Management. *37th Annual AIChE Loss prevention Symposium*, New Orleans, Louisiana, March 31−April 2, 2003.

(52) Yuki, Y. Alarm system optimization for increasing operations productivity. *ISA Trans.* **2002**, *41* (3), 383.

(53) Ryan, T. P. *Modern Engineering Statistics*; John Wiley & Sons: New Jersey, 2007.

(54) http://en.wikipedia.org/wiki/Fluid_catalytic_cracking (Accessed December 1, 2009).

Received for review December 10, 2009
Revised manuscript received February 27, 2010
Accepted March 2, 2010

IE9019648