Dynamic Risk Analysis Using Alarm Databases to Improve Process Safety and Product Quality: Part I—Data Compaction

Ankur Pariyani and Warren D. Seider
Dept. of Chemical and Biomolecular Engineering, University of Pennsylvania, Philadelphia, PA 19104

Ulku G. Oktem
Risk Management and Decision Processes Center, Wharton School, University of Pennsylvania, Philadelphia, PA 19104

Masoud Soroush
Dept. of Chemical and Biological Engineering, Drexel University, Philadelphia, PA 19104

DOI 10.1002/aic.12643
Published online May 16, 2011 in Wiley Online Library (wileyonlinelibrary.com).

In most industrial processes, vast amounts of data are recorded through their distributed control systems (DCSs) and emergency shutdown (ESD) systems. This two-part article presents a dynamic risk analysis methodology that uses alarm databases to improve process safety and product quality. The methodology consists of three steps: (i) tracking of abnormal events over an extended period of time, (ii) event-tree and set-theoretic formulations to compact the abnormal-event data, and (iii) Bayesian analysis to calculate the likelihood of the occurrence of incidents. Steps (i) and (ii) are presented in Part I and step (iii) in Part II. The event-trees and set-theoretic formulations allow compaction of massive numbers (millions) of abnormal events. For each abnormal event, associated with a process or quality variable, its path through the safety or quality systems designed to return its variable to the normal operation range is recorded. Event trees are prepared to record the successes and failures of each safety or quality system as it acts on each abnormal event. Over several months of operation, on the order of 10^6 paths through event trees are stored. The new set-theoretic structure condenses the paths to a single compact data record, leading to significant improvement in the efficiency of the probabilistic calculations and permitting Bayesian analysis of large alarm databases in real time. As a case study, steps (i) and (ii) are applied to an industrial, fluidized-catalytic-cracker. © 2011 American Institute of Chemical Engineers *AIChE J,* 58: 812–825, 2012

Keywords: industrial-scale processes, risk analysis, alarm databases, abnormal events, unsafe incidents, process safety, product quality, Bayesian theory, chemical/manufacturing processes, fluidized-catalytic-cracking unit

Introduction

The U.S. Chemical Safety and Hazard Investigation Board website[1] lists about 65 serious accidents that occurred over the past decade, with their consequences and key technical

Correspondence concerning this article should be addressed to W. D. Seider at seider@seas.upenn.edu.

findings. Beyond these alarming incidents, at least 123 chemical facilities in the United States keep toxic chemicals that, if released, would place one million or more nearby residents in danger, according to a study by the U.S. Environmental Protection Agency.[2] In addition, more than 700 plants could place at least 100,000 people at risk, with more than 3000 facilities having at least 10,000 people living nearby. These are incentives for improving risk assessment techniques, with the objective of approaching zero-incidents, saving lives and billions of dollars of revenues.

On the basis of the severity levels, incidents can be broadly classified as *accidents* or *near-misses*. Every accident is typically preceded by several near-misses, which are less severe events/conditions/consequences, having the potential to lead to accidents.[3,4] Given the growing global competition, tighter regulations, and the increasing number of lawsuits with higher penalties, the chemical process industries (CPIs) are placing more emphasis on improving their safety performances—by encouraging the reporting of near-misses (see Jones et al.[5] for a case study at Norsk Hydro) and several other "safety-first" policies. Because the CPIs have been adapting plants with minimal design changes to produce higher-quality products at increased production rates, the rate of reporting of near-misses has increased in recent years, with more companies seeking to improve their reporting and investigation of incidents (through initiatives by the UNEP/ILO/WHO International Programme on Chemical Safety,[6] National Response Center,[7] U.S. EPA,[8,9] European Commission,[10,11] Hazardous Substances Emergency Events Surveillance (HSEES) system by the ATSDR,[12] AIChE-CCPS,[13] and Mary Kay O'Connor Process Safety Center[14]). Several industry-standard software packages, which perform quantitative risk assessment using accident databases, are widely used. In addition, several articles and books[15–19] have proposed the analysis of accident databases using fault-trees, hazard and operability (HAZOP) studies, failure mode and effects analysis, and Bayesian theory, among other approaches, to gain predictive insights concerning accidents.

However, because most chemical processes have hundreds of variables that monitor their dynamics, in our views, much *precursor* information, belying unsafe conditions, is overlooked and unutilized as it resides in large alarm databases. This data is associated with their distributed control systems (DCSs) and emergency shutdown (ESD) systems. Although helping plant operators assess and control plant performance, especially in the face of potential safety and product-quality problems, it contains real-time information on the progression of disturbances and the performance of their regulating and protection systems (barriers to protect processes from abnormal behavior). Prior analyses[15–21] have not adequately utilized this information and have focused on the usage of accident databases only. In this two-part series, new techniques are developed to utilize the dynamic databases in assessing risk levels and predicting the probabilities of incidents.

Herein, definitions are provided in the Preliminaries for the process and quality variables introduced in our earlier work.[22] Then, their departures from, and subsequent returns to, normal operating ranges are recognized as "near-misses"—because these departures have the potential to propagate to incidents, when their regulating (process control) and protection (ESD) systems fail. These high-probability, low-consequence events are used to assess the performance and pairwise interactions of their regulating and protection systems and to predict the occurrence of incidents. With this knowledge, potential system problems can be identified and corrected before they result in sizable product and economic losses.

While near-misses directly affect process safety, they also impact product quality, with quality variations significant sources of financial losses in the CPIs. In these articles, methods are introduced to utilize the near-miss data associated with quality variables, in addition to that associated with process variables, for risk assessment to enhance both the safety and quality performances of processes. These methods improve on the integration of safety and quality management systems introduced by Dumas[23] and developed by others, as reviewed by Wilkinson and Dale.[24] More recently, Herrero et al.[25] and Williamsen[26] discussed the relationship between safety and quality management principles with analysis of data from a Spanish company and Frito-Lay. Also, Oktem[27] discussed elements of near-miss management for these integrated systems. This integration underlies several quality-improvement techniques, for example, Total Quality Management, ISO 9000, Kaizen, and Six-sigma, which aim to address root causes and improve efficiencies throughout organizations.

This article presents two steps of a three-step dynamic risk analysis methodology that uses massive alarm databases to improve process safety and product quality. The three steps are (i) tracking of abnormal events over an extended period of time, (ii) event-tree and set-theoretic formulations to compact the abnormal-event data, and (iii) Bayesian analysis to calculate the likelihood of the occurrence of incidents. Steps (i) and (ii) are presented in Part I and step (iii) in Part II. These articles extend the models that we introduced in our previous work[15,20,21] to estimate the probabilities of occurrence of accident scenarios using accident precursor data. They utilize large alarm databases, including many near-misses associated with process and quality variables, for the projection of unsafe plant conditions as well as quality problems. The new event-trees and set-theoretic formulations, developed after unsuccessful attempts using incidence matrices, allow compaction of massive numbers (millions) of abnormal events, making it possible to carry out the Bayesian analysis in real time. This article also introduces the constructs, definitions, and terminology used in both Parts I and II. As a case study, application of steps (i) and (ii) to an industrial scale, fluidized-catalytic-cracking unit (FCCU) at a major petroleum refinery, is presented. Previous studies did not utilize large dynamic alarm databases to perform risk analyses in processing plants, and thus, these two articles (Parts I and II) are the first to present a methodology to utilize these databases efficiently.

The organization of the rest of Part I is as follows. The Preliminaries discusses the DCS and ESD databases and expands on the safety, quality, and operability systems (SQOS) and upset states in our previous work.[22] Next, the dynamic risk assessment methodology is presented in the section on Dynamic Risk Assessment Method. Event-trees and set-theoretic formulations of near-miss data are introduced in the sections entitled Event-Tree Formulations for

Process and Quality Variables and Set-Theoretic Formulation. Application to an industrial scale, FCCU is presented in the Case Study 2: Abnormal Events History of the FCCU, followed by the Conclusions. An alternate formulation of the event trees is presented in the Appendix.

Preliminaries

In this section, some preliminaries and definitions are presented/revisited[22] that are needed in the subsequent sections of this article. Chemical processes frequently encounter special causes (i.e., sudden or unexpected causes of variations in process conditions due to unexpected phenomena). Their regulating and protection systems are designed to keep process and quality variables within acceptable limits. Control systems adjust manipulated variables when measurements of controlled variables are off-specification. An *abnormal event* occurs when a variable departs from its normal operating range, often resulting in off-specification products.

On the basis of the measurement types, plant variables have been divided into *process* and *quality* variables.[22]

Definition 1. A variable that is measured frequently online and describes the process dynamics (e.g., temperatures, pressures, flow rates and their rates of change, etc.) is called a process variable.

Definition 2. A variable that is related to the quality of the product (e.g., viscosity, density, average molecular weight, etc.) and is often estimated/inferred using mechanistic and/or statistical models is called a quality variable.

On the basis of the sensitivity and importance, plant variables have been classified as *primary* and *secondary* variables.[22]

Definition 3. Primary, or key, variables are closely related to process safety and are associated with the ESD system. When these variables move beyond their ESD limits, ESDs or ''trips'' are triggered, often after a small time-delay.

Definition 4. Secondary variables, on the other hand, are not associated with the ESD system. Clearly, a primary or secondary variable can be a process or quality variable.

For large-scale processes, typically 150–400 variables are monitored; however, only a small percentage (less than 10%) are chosen as primary variables. Herein, primary process variables are denoted by pPs and primary quality variables by pQs. The primary variables are selected during the design and commissioning of plants by carrying out analyses of tradeoffs between the safety and profitability of the plant. Dedimensionalization (or scaling to obtain more meaningful quantities; e.g., the Damköhler number and reactant conversion) and principal-component analyses[28] can be used to identify primary variables systematically that should be monitored along with individual process variables to improve the tracking of process dynamics.

To analyze the DCS and ESD databases, Pariyani et al.[22] focused on abnormal events. Figure 1 shows a typical control chart for a primary variable. The chart is divided into four zones, beginning with its green-belt zone (normal operation), during which the variable lies within acceptable limits. When the variable moves beyond these 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 borders between its orange- and red-belt zones are the threshold limits for the triggering of the ESD system. For secondary variables, similar control charts do not have red-belt zones.

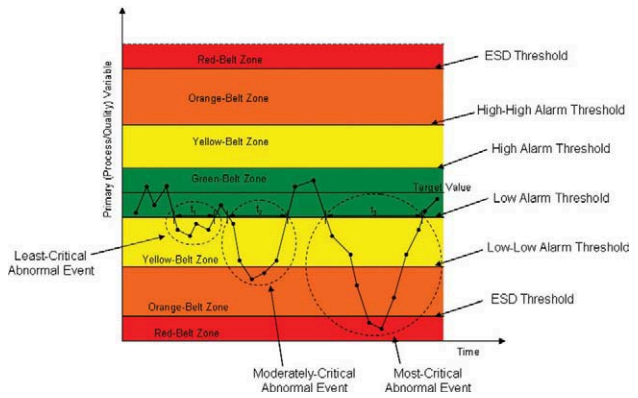

Figure 1. Various operating belt zones and alarm thresholds for a primary variable.

[Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

Abnormal events begin when process (or product-quality) variables move from their green-belt zones to their yellow-, orange-, or red-belt zones, triggering alarms. Clearly, these departures can be interpreted as precursors to undesirable consequences or accidents, when regulating and protection systems fail to maintain normal operation. Consequently, in this article, abnormal events, for variables that return to their green-belt zones, are recognized as near-misses, which could have propagated to incidents. As a result, vast amounts of near-miss data become available for dynamic risk assessment.

Depending on their criticality, abnormal events are classified into three categories: *least-critical abnormal events* that cross the high/low alarm thresholds, but do not cross the high–high/low–low alarm thresholds; *moderately-critical abnormal events* that cross the high–high/low–low alarm thresholds, but do not cross the ESD thresholds; and *most-critical abnormal events* that cross the ESD thresholds. Because secondary variables do not have red-belt zones, most-critical abnormal events are not associated with them.

Dynamic alarm databases: DCS and ESD logs

Ensuring the safety of chemical plants, their personnel, and their surrounding neighborhoods, is crucial to the success of the chemical process and nuclear industries. Among many intra- and inter-company safety-related activities, several comprehensive algorithms and software packages have been developed over the last two decades to evaluate the risk and safety levels of processes, leading to appropriate protective measures. These include SAPHIRE (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations),[29] PSAPACK 4.3 (Probabilistic Safety Analysis Package),[30] RISKMAN,[31] WinNUPRA,[32] Safety Monitor,[33] RiskSpectrum,[34] Risk & Reliability Workstation (by the Electric Power Research Institute),[35] Meridium,[36] PROACT,[37] Safeti QRA (Quantitative Risk Assessment) Package,[38] RiskVu,[39] QRA Packages by Dyadem,[40] ITEM QRAS,[41] and many more. All typically utilize accident databases, including frequencies and consequences, and associated profit losses, and perform quantitative risk analyses.

A	B	C	D	E	F	G
2008-12-23 6:01 AM	Alarm	FI50	HI	ALM	LOW	Flowrate through Pump1
2008-12-23 6:01 AM	Alarm	PDI10	LO	ALM	HIGH	Press. diff. stand pipe#1
2008-12-23 6:01 AM	Alarm	TI25	LO	ALM	MEDIUM	#1 flue gas temperature
2008-12-23 6:02 AM	Alarm	PDI10	LL	ALM	HIGH	Press. diff. stand pipe#1
2008-12-23 6:04 AM	Alarm	FI50	HI	RTN	LOW	Flowrate through Pump1
2008-12-23 6:04 AM	Alarm	TI25	LO	RTN	MEDIUM	#1 flue gas temperature

Figure 2. Screenshot from a typical DCS database showing data entries for a few minutes.

However, because they involve accidents only, excluding day-to-day alarm information (with associated near-miss data), they cannot achieve high predictive accuracies. All lack dynamic analyses that identify and target near-misses, contributing to many serious accidents over the last decade.[1,42] These losses are all the more alarming when viewed against the increasing number of shutdowns, in spite of trained operators and experienced managers. Had systematic procedures for analyzing dynamic data, identifying near-misses and the performance of their regulating and protection systems, been in place, a large fraction of these incidents would have been avoided through alerts to plant management well in advance.

In these two articles, methods are introduced for the efficient extraction of knowledge from dynamic alarm databases, namely DCS and ESD system alarm databases. Typically, DCS databases contain abnormal-event data, which include alarm identity tags for the variables, alarm types (low, high, high–high, etc.), times at which the variables cross their alarm thresholds (in both directions), and variable priorities. Their associated ESD databases, of greater consequence, contain trip event data, timer-alert data, etc. A screenshot of a typical DCS database for a brief period is shown in Figure 2. Every row represents a new entry, associated with either a process or quality variable. Column A displays the times in chronological order, with each entry displaying the ''Year-Month-Day Hour: Minute AM/PM.'' Note that the second entry is provided, although not shown in Figure 2. Column B indicates the entry type: alarm, change in controller settings, etc. Column C shows the alarm tag of the variable (defined during the commissioning of the unit). Column D shows the alarm type [LO (low), LL (low–low), HI (high), etc.]. Column E shows the drift status of the alarms, either ALM (alarm) or RTN (return); that is, whether the variable drifts beyond or returns within the alarm thresholds. Therefore, given the occurrence and return times of the variables, the durations of abnormal events (or *recovery times*) can be calculated. Column F shows the alarm priority, and column G presents a brief description of the alarm. Similar data entries exist for the ESD database.

In industrial-scale processing plants, about 5000–10,000 alarms typically occur daily, with on the order of 10^6 alarms occurring over a few months. To carry out Bayesian analysis in real time, it is required to create a compact representation of this data. Figure 3 shows a schematic of the steps to create the compact representation introduced in Part I, beginning with the raw data at the top and, after the steps described herein, resulting in likelihood data required for Bayesian analysis to estimate the failure probabilities of the safety, quality, and operability systems.

Safety, quality, and operability systems (SQOSs)

The regulating (process control) and protection (ESD) systems interact to take actions to nullify the impact of disturbances, which are precursors to safety problems and quality departures (i.e., off-specification product quality). For most processes, a safety and quality management structure responds to abnormal events with typically six SQOSs, which are components of the DCS and ESD system, and involve human operators. Unlike independent protection layers,[43] these systems are interdependent to reduce the risk levels of the process—with their pairwise interaction coefficients computed in Part II. Furthermore, they are usually activated sequentially and their actions are interdependent. Next, six of the most commonly used systems are described, with the number of systems and their functionalities dependent on the specific chemical plants. Throughout the remainder of this article, these six systems are used to illustrate the concepts presented.

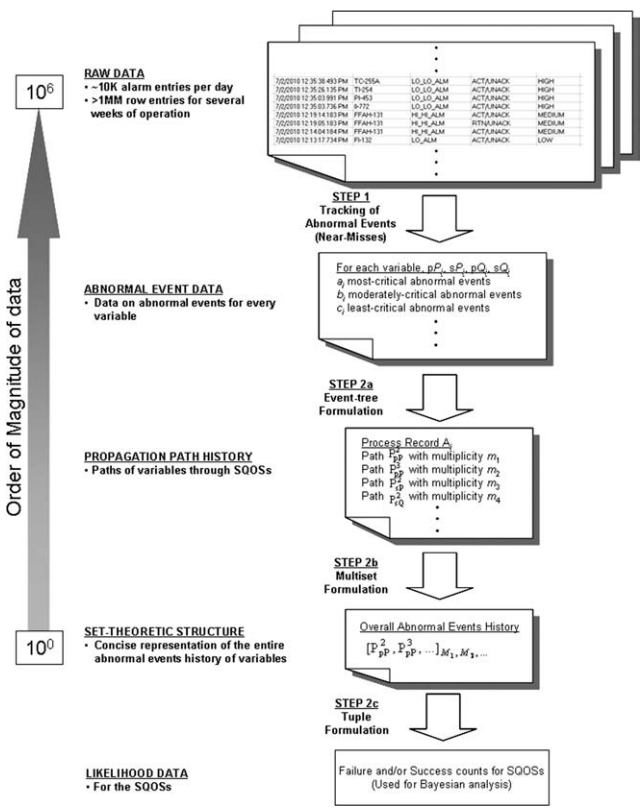

Figure 3. Steps to prepare compact likelihood data for Bayesian analysis.

Basic process control system (BPCS)—SQOS[1]—which refers to an automated basic control system within the DCS, designed to take control actions (i.e., adjust the manipulating variables) to keep the process and quality variables within their normal operating ranges. When the BPCS is unsuccessful, abnormal events occur, with alarms notifying the operators of the transition of the variables into their yellow-, orange-, or red-belt zones.

Operator (machine + human) corrective actions, level I—SQOS[2]—which refers to human operator-assisted control to keep the variables within their high/low alarm thresholds and to return them to normal operating conditions. When unsuccessful, variables enter into their orange- and red-belt zones.

Operator (machine + human) corrective actions, level II—SQOS[3]—which refers to human operator-assisted control to keep the variables within their high–high/low–low alarm thresholds and to return them to normal operating conditions. These corrective actions are more rigorous than those for level I, because when unsuccessful, the variables enter their red-belt zones, with the potential to cause an ESD of the unit.

Override controller—SQOS[4]—which refers to an automatic controller that takes radical actions when select primary variables enter their red-belt zones. When successful, no tripping occurs. Typically, it is a safety system, associated with select primary process variables. However, herein, it is taken as a SQOS.

Automatic ESD—SQOS[5]—which refers to an automatic, independent system that shuts down the unit after a small time delay.

Manual ESD—SQOS[6]—which refers to a human-operated system that shuts down the unit immediately.

To assess the reliability of these systems for a process, a framework involving event trees and multisets is formulated in Part I to provide a compact representation of vast DCS and ESD databases. It facilitates the statistical analysis using Bayesian theory in Part II. The combined framework accounts for the complex interactions that occur between the DCS, human operators, and the ESD system—yielding enhanced estimates and predictions of the failure probabilities of the SQOSs and, more importantly, the probabilities of the occurrence of shutdowns and accidents. This causative relationship between the SQOSs is modeled using copulas (multivariate functions that represent the dependencies among the systems using correlation coefficients)—to be discussed in Part II.

Upset states

A process is said to be in an upset state[22] when process or quality variables move out of their green-belt zones, indicating "out-of-control" or "perturbed" operation. Upset states lead to deterioration in operability, safety, and/or quality performances of the process. Equations to estimate the operability and safety performances have been proposed.[22]

The upset states[22] are repeated here with an improved definition of the quality upset state (QUS).

Operability-only upset state (OOUS), where at least one of the secondary process variables lies outside its green-belt zone, but all 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.

Table 1. Variable Associations with Upset States (In = Inside Green-Belt Zone, Out = Outside Green-Belt Zone)

	Process Variables		Quality Variables	
Upset States	Primary	Secondary	Primary	Secondary
OOUS	In	Out	In	In
SUS	Out	Out	In	In
QUS	In	Out	In	Out
S+QUS	Out	Out	Out	Out

Safety upset state (SUS), where at least one of the primary process variables lies outside its green-belt zone, but all the quality variables lie within their green-belt zones. In this case, both safety and operability performances are affected and a safety problem is probably to occur.

Quality upset state (QUS), where at least one of the secondary quality variables lies outside its green-belt zone, but all the primary process and primary quality 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 probably to occur. Note that when a primary quality variable lies outside its green-belt zone, both a quality defect and a safety problem are probably to occur, as discussed next.

Safety and quality upset state (S+QUS), where at least one of the primary process variables and one of the quality variables lie outside their green-belt zones. In this case, both a quality defect and a safety problem are probably to occur.

Using the definitions above, Table 1 summarizes the association of primary and secondary, process and quality variables with the different upset states.

Note that although quality variables are causally related to process variables, the occurrence of quality defects does not necessarily imply the occurrence of safety problems and vice versa. Clearly, plants can move from one upset state to another as disturbances (or special causes, which cause abnormal events) progress.

Dynamic Risk Assessment Method

The dynamic risk assessment method herein consists of three steps, shown as three regions of the pyramid in Figure 4. The steps are (1) near-miss tracking, (2) event-tree and set-theoretic formulation, and (3) Bayesian analysis.

Near-miss tracking refers to identification and tracking of near-misses over an extended period of time (weeks, months, etc.). As mentioned earlier, the abnormal events experienced by the process and quality variables are recognized as near-misses. Pariyani et al.[22] presented techniques for tracking of abnormal events and recovery-time analysis to quantify, characterize, and track near-misses experienced by individual and groups of variables over different periods of time. Using Pareto charts and alarm frequency diagrams, these

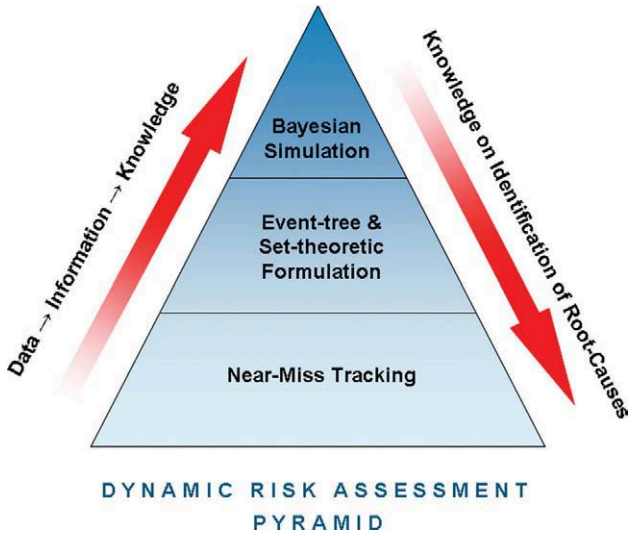

Figure 4. Dynamic risk assessment pyramid showing different stages.

[Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

techniques 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. They also suggest opportunities to explore their root causes and reduce the frequencies of unwanted alarms. The approaches improve on alarm management techniques by drawing attention to the severity of abnormal events experienced by variables and their associated recovery times (rather than alarm counts only). The results suggest the need to carry out these statistical analyses in real time—to summarize for plant operators those alarms associated with the most abnormal events and requiring the most attention; that is, allowing prioritization of the numerous flags raised by the alarms.

Event-tree and Set-theoretic formulation permits the transformation of near-miss data to information on the performances of the SQOSs. As presented in the Event-Tree Formulations for Process and Quality Variables, in this step, the near-miss data that tracks (a) special causes, (b) abnormal events, (c) the propagation of abnormal events, and (d) the attainment of end-states, is stored in set-theoretic formulations to represent the branches of event trees.

As special causes arise in processes, they are handled by the SQOSs, whose actions guide the process/quality variables through their green-/yellow-/orange-/red-belt zones, resulting in either continued normal operation (variables in their green-belt zones) or upset states (OOUS, SUS, QUS, S+QUS). The sequences of responses (i.e., successes or failures) of the SQOSs are the paths followed by the process/quality variables and are described by the branches of the event trees (as discussed in the Event-Tree Formulations for Process and Quality Variables). They track abnormal events to their end-states (i.e., normal operation, plant shut-down, accident, etc.). Using a generalized set-theoretic formulation (discussed in the section entitled Set-theoretic Formulation), these paths are represented in a condensed format—to facilitate Bayesian analysis (discussed in Part II). Stated differently, near-miss data from the DCS and ESD system databases show how variables move among their green-, yellow-, orange-, and red-belt zones to their end-states. From these, event trees are created and represented with new set-theoretic notations. This permits the systematic utilization of the historical alarm databases in real time Bayesian calculations to estimate failure probabilities, the probabilities of accidents, and the like.

Bayesian analysis refers to the utilization of the transformed data to obtain knowledge (i.e., statistical estimates) of the performances (in terms of failure probabilities) and pairwise interaction coefficients of the SQOSs. Also, the probabilities of incidents are estimated. These estimates help to identify the root causes in the process, for example, the SQOSs with high failure probabilities or variables experiencing high-abnormal-event rates. In particular, consider a case when the failure probabilities of the operator corrective actions ($SQOS^2$ and $SOQS^3$) are high—giving operators and managers incentives to identify their root causes—possibly due to insufficient operator training, stress factors, etc.

A key premise of this risk assessment framework is that performance of a SQOS (measured as failure rate or likely) is likely to influence the performances of the other SQOSs, because of (a) nonlinear relationships between the variables and (b) human behavior-based factors. For example, deterioration in the performance of the BPCS is likely to distract the operators and impede their performance. This causal relationship between the two SQOSs is accounted for using copulas, which are multivariate functions that model dependences.

Event-Tree Formulations for Process and Quality Variables

In this section, event-tree formulations are introduced, which depict the actions of the SQOSs as they respond to abnormal events—with the branches representing the paths traced by the process and quality variables. Note that each SQOS is represented by a node, with the success or failure of each system denoted by S or F, respectively, along two branches leaving each node.

Figures 5–7 show the event trees for primary process/quality variables (pPs or pQs) that enter their yellow-/orange-/red-belt zones. The trees are illustrated for the six typical SQOSs discussed earlier. The first three systems are shown across the top in Figure 5 and are denoted as $SQOS^1$, $SQOS^2$, and $SQOS^3$, respectively, as discussed in the Safety, Quality, and Operability Systems, whereas the remaining three systems are shown across the top in Figure 6 and are denoted as $SQOS^4$, $SQOS^5$, and $SQOS^6$, respectively. Figures 6 and 7 are identical except for the last end-state in path 7.

Depending on the performance (success or failure) of these SQOSs, seven paths are possible each for the SUS and QUS—with four paths leading to continued operation, CO (when all primary process variables return to their green-belt zones), two paths leading to ESD (a near-miss, which occurs when a primary variable enters its red-belt zone and ESD sequences are triggered), and one path leading to runaway reaction, RA, or quality meltdown, QM (accidents that occur when all the SQOSs fail to remove a primary process/quality variable from its red-belt zone). Uncontrolled RAs often lead

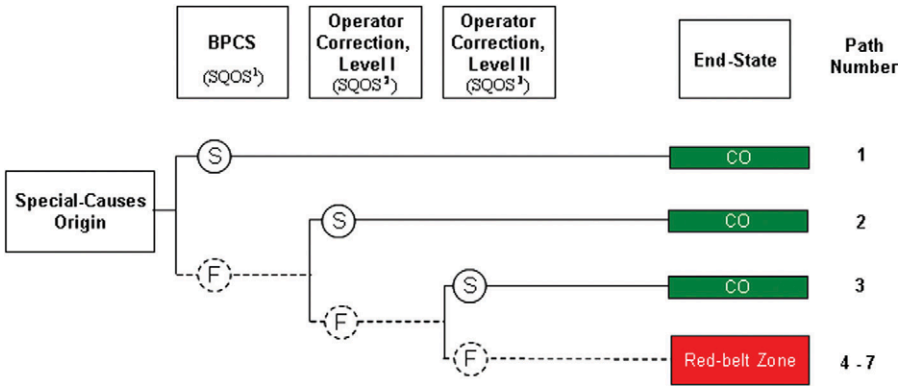

Figure 5. Event tree for primary process/quality variables in their yellow- and/or orange-belt zones.

[Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

to loss of life, serious injuries, and major equipment losses, whereas QMs often result in major economic losses due to product losses and manpower requirements to return the process to normal operation. In some cases, equipment losses are involved.

The paths are numbered according to the index of the end-state in the event tree—from top to bottom, using the notation, P^i_{pP} or P^i_{pQ}, where i is the path counter and pP or pQ indicates that the path is followed by a primary process or quality variable. The primary process/quality variables follow the uppermost path, P^1_{pP}/P^1_{pQ}, when the BPCS takes successful controlling actions and keeps them within their green-belt zones (i.e., no abnormal events occur). Symbolically, the path is represented by S^1_{pP}/S^1_{pQ} or simply S^1, where $S^k_{pP}/S^k_{pQ}/S^k$ denotes the success of SQOS k. Also, the combined path and its end-state is denoted as P^1_{pP}/P^1_{pQ}-CO.

The primary process/quality variables follow the second path, P^2_{pP}/P^2_{pQ}, when the BPCS fails to keep them within their green-belt zones, but the operators successfully return them to their green-belt zones. This path, is represented by $F^1 \rightarrow S^2$, where F^k denotes the failure of SQOS k. Together with its end-state, this least-critical abnormal event is denoted as P^2_{pP}-/P^2_{pQ}-CO. The pPs/pQs follow the third path, P^3_{pP}/P^3_{pQ}, when they enter their orange-belt zones, marking the failures of the BPCS and the first level of corrective actions by operators. However, the second level (more rigorous) corrective actions by the operators successfully return them to their green-belt zones. This path is represented by $F^1 \rightarrow F^2 \rightarrow S^3$. Together with its end-state, this moderately-critical abnormal event is denoted as P^3_{pP}/P^3_{pQ}-CO.

At times, variables oscillate between their yellow-/orange-/red-belt zones, before returning to their green-belt zones. In such cases, the above notation applies—with the criticality of the abnormal events determined by the highest belt zone entered. This concise notation, with the set-theoretic representation in the next section, will be shown to effectively represent complex alarm sequences for the Bayesian analysis in Part II. As an example, consider an abnormal event with a process variable: (a) entering its orange-belt zone, (b) returning briefly to its yellow-belt zone, (c) re-entering its orange-belt zone, and (d) returning to its green-belt zone. For this moderately-critical abnormal event, the SQOS^2 failed to keep the variable within its yellow-belt zone, and the SQOS^3 succeeded, in its second attempt, in returning the variable to its green-belt zone. Note that, in practice, when variables experience oscillations about their thresholds, deadbands (of 2–5%) are applied to disregard nuisance alarms.

The primary variables follow the remaining paths 4–7 when they enter their red-belt zones—because of the failures of BPCS and operator corrective actions (both levels), often due to insufficient response times resulting from rapid transients. The pPs/pQs follow the fourth path, P^4_{pP}/P^4_{pQ}, when the override controller successfully removes them from their red-belt zones and returns them to their green-belt zones. Similarly, paths 5–7 are traced when the override controller fails to remove the pPs/pQs from their red-belt zones and

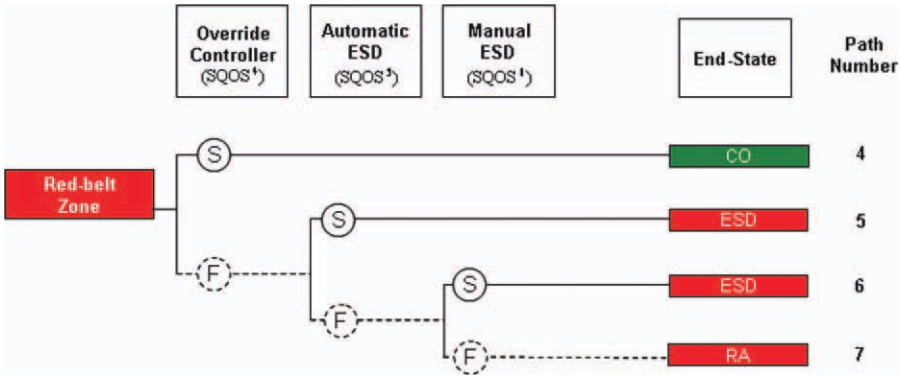

Figure 6. Event tree for primary process variables (p*P*s) in their red-belt zones.

[Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

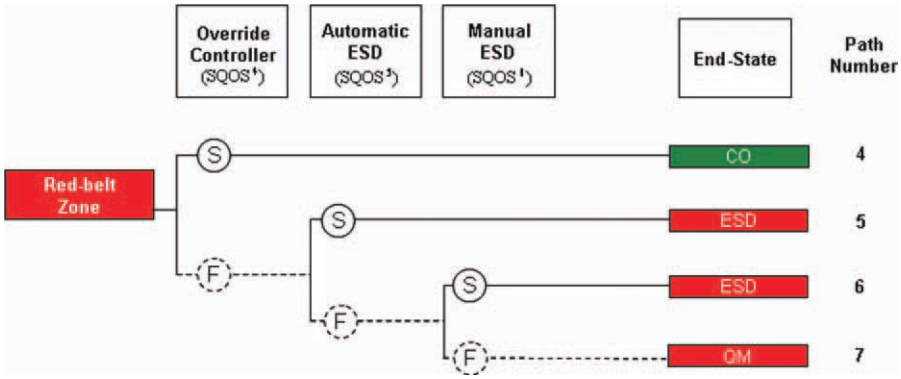

Figure 7. Event tree for primary quality variables (pQs) in their red-belt zones.

[Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

automatic/manual ESD sequences are triggered, resulting in safe shutdowns or accidents (RAs or QMs), depending on their successes or failures.

Figure 8 shows the event tree for secondary process/quality variables (sPs or sQs) that enter their yellow- or orange-belt zones. The tree represents the actions of the three SQOSs associated with the secondary variables, shown across the top. The combined paths and their end-states are denoted as P^1_{sP}/P^1_{sQ}-CO, P^2_{sP}/P^2_{sQ}-CO, and P^3_{sP}/P^3_{sQ}-CO. As these variables do not have red-belt zones, only levels I and II corrective actions by the operators are undertaken to return them to their green-belt zones. That is, no matter how long these variables are out of their green-belt zones, if the primary variables do not enter their red-belt zones, no radical actions (by the override controller or ESD system) are taken. However, if at least one primary variable enters its red-belt zone, corrective actions taken by $SQOS^4/SQOS^5/SQOS^6$ are likely to return the primary variables and, in turn, the secondary variables to their green-belt zones. In principle, the override controllers and ESD system are associated only with the primary variables. However, because of interactions between the primary and secondary variables, the effects of their corrective actions are channeled to the latter, causing them to return to their green-belt zones as well. Thus, sooner or later, all the sPs/sQs return to their green-belt zones. However, their recovery times often vary significantly. These interdependent effects due to nonlinear interactions are typically accounted for in the design of the DCSs, which often implement multivariable, nonlinear model-predictive controllers (MPCs) to handle the nonlinear interactions more efficiently than multiple single-input, single-output (SISO) controllers. Herein, the event trees for secondary variables do not explicitly account for the auxiliary effects of $SQOS^4/SQOS^5/SQOS^6$ on the secondary variables.

Note that all the SQOSs are often not associated with each process and quality variable—for example, override controllers exist only for select primary variables to reduce costly shutdowns. Also, some variables have no first- or second-level alarms to reduce alarm flooding. For those variables having fewer SQOSs, the notation is modified to show the missing systems. For example, when the override controller ($SQOS^4$) is not included in the SUS event trees (Figures 6 and 7), only six paths are possible, with their end-states, denoted as P^1_{pP}-CO, P^2_{pP}-CO, P^3_{pP}-CO, $P^5_{pP}(-\text{IV})$-ESD, $P^6_{pP}(-\text{IV})$-ESD, and $P^7_{pP}(-\text{IV})$-RA. In this notation, the path numbers are unchanged and the event trees remain applicable when SQOSs are not included.

Also, these event trees are applicable only for continuous processes, wherein process/quality variables return to their green-belt zones eventually (except when shut downs or accidents occur). Event trees for batch processes are developed similarly. They have more end-states because variables may remain out of their green-belt zones after the batches are terminated, leading to end-states having safety problems or quality defects.

Finally, returning to Figure 3, in step 1, abnormal events in the raw data are tracked to extract abnormal-event histories for each variable, pP_i, sP_i, pQ_i, sQ_i—each involves a_i most-, b_i moderately-, and c_i least-critical abnormal events.

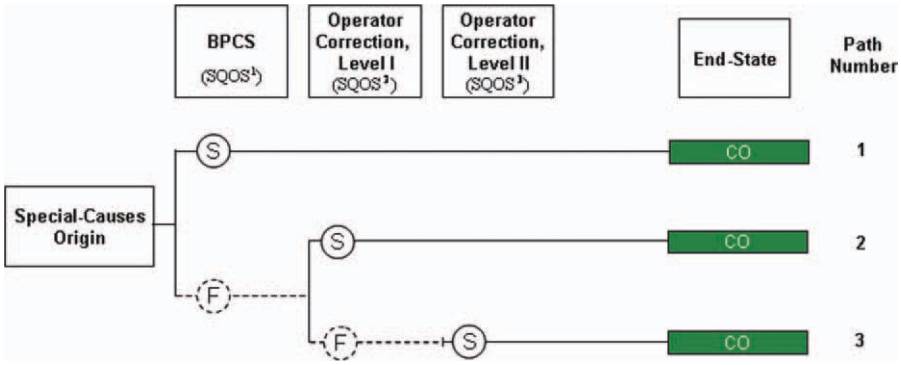

Figure 8. Event tree for secondary process/quality variables in their yellow-/orange-belt zones.

[Color figure can be viewed in the online issue, which is available at wileyonlinelibrary.com.]

Table 2. Process Report – Case Study 1

1:00 PM	Normal operation
1:01 PM	Three secondary process variables, sP_1, sP_2, sP_3, enter their yellow-belt zones (three high alarms go off)
1:02 PM	Two primary process variables, pP_1 and pP_2, enter their yellow-belt zones (two high alarms go off)
1:03 PM	One primary process variable, pP_1, enters its orange-belt zone (one high–high alarm goes off); one secondary quality variable, sQ_1, enters its yellow-belt zones (one low alarm goes off)
1:04 PM	Operators (human + machine) successfully diagnose and correct the problem, with all process and quality variables returned to their green-belt zones

Next, a set-theoretic formulation is introduced. A brief case study is presented first to show how transitions between upset states are represented.

Set-Theoretic Formulation

To introduce the set-theoretic formulation, consider Case Study 1, which is presented in Table 2 as a *process report* for a typical continuous process over a brief period (consisting of minute-by-minute status updates in which a disturbance drives a few process and quality variables out of their green-belt zones). Between 1:00 and 1:01 PM, the process enters an OOUS. In the next minute, it moves from an OOUS to a SUS as two of its primary process variables move out of their green-belt zones. Later, it moves from a SUS to S+QUS as one of its quality variables also moves out of its green-belt zone. However, within the next minute, all the variables are returned to their normal operating ranges, with CO occurring—because of levels I and II corrective actions by the operators.

In this case study, six abnormal events (five least-critical and one moderately-critical) occurred, after the BPCS failed to keep all its process and quality variables within their green-belt zones. As the SQOSs responded, the variables, sP_1, sP_2, sP_3, pP_2 and sQ_1, which entered their yellow-belt zones only, followed the path, $F^1 \rightarrow S^2$, whereas, the primary process variable, pP_1, which entered its yellow- and orange-belt zones, followed the path $F^1 \rightarrow F^2 \rightarrow S^3$. Thus, on the basis of the event trees in Figures 5–7, four distinct paths were followed: (a) P^2_{pP}—followed by pP_2, (b) P^3_{pP}—followed by pP_1, (c) P^2_{sP}—followed by sP_1, sP_2, sP_3, and (d) P^2_{sQ}—followed by sQ_1—all leading to the end-state, CO. Thus, this abnormal events history, which shows several variables experiencing abnormal events over a period of time, is represented by a collection of paths, traced by the variables, leading to the same end-state, and therefore, is referred to as a *process record*. Note that an abnormal events history may include more than one process record, corresponding to different end-states attained by the variables; for example, CO, ESD, etc.

Again, returning to Figure 3, using the abnormal-event data created in step 1, propagation paths through the SQOSs are extracted in step 2a using the event-tree formulations discussed earlier. Note that for the process report in Table 2, a process record is created comprised of paths P^2_{pP}, P^3_{pP}, P^2_{sP}, and P^2_{sQ}, followed m_1 (=1), m_2 (=1), m_3 (=3), and m_4 (=1) times by the six variables.

Next, the key premises of the set-theoretic model are presented:

(1) The paths followed by the variables are modeled as n-tuples, where n-tuples are ordered lists of finite length n. Similar to sets and multisets (discussed later), tuples contain objects.[44] However, the latter appear in a certain order (which differentiate them from *multisets*) and an object can appear more than once (which differentiates them from *sets*). Herein, for paths of event trees, modeled as n-tuples, n denotes the number of SQOSs, and the objects are Boolean variables with permissible values, 0 (FALSE) and 1 (TRUE), for the failure and success of the SQOSs, respectively. When any system is not activated, a null value, φ, is used. For the event trees discussed in the Event-Tree Formulations for Process and Quality Variables, the paths are modeled as 6-tuples (for 6 SQOSs), given by

$$P^1_{pP}, P^1_{pQ} = (1, \varphi, \varphi, \varphi, \varphi, \varphi); \quad P^2_{pP}, P^2_{pQ} = (0, 1, \varphi, \varphi, \varphi, \varphi);$$
$$P^3_{pP}, P^3_{pQ} = (0, 0, 1, \varphi, \varphi, \varphi); \quad P^4_{pP}, P^4_{pQ} = (0, 0, 0, 1, \varphi, \varphi);$$
$$P^5_{pP}, P^5_{pQ} = (0, 0, 0, 0, 1, \varphi); \quad P^6_{pP}, P^6_{pQ} = (0, 0, 0, 0, 0, 1);$$
$$P^7_{pP}, P^7_{pQ} = (0, 0, 0, 0, 0, 0);$$

And

$$P^1_{sP}, P^1_{sQ} = (1, \varphi, \varphi, \varphi, \varphi, \varphi); \quad P^2_{sP}, P^2_{sQ} = (0, 1, \varphi, \varphi, \varphi, \varphi);$$
$$P^3_{sP}, P^3_{sQ} = (0, 0, 1, \varphi, \varphi, \varphi);$$

This notation is also applicable to event trees with fewer SQOSs. For example, the 6-tuple notation for P^5_{pP} (−IV) is (0, 0, 0, φ, 1, φ).

(2) The set of distinct paths, that is, $\{P^2_{pP}, P^3_{pP}, P^2_{sP}, P^2_{sQ}\}$ for Case Study 1, denoted as a_m, followed by the process and quality variables is referred as an underlying set of paths. Note that because the elements in a set cannot be repeated,[44] the six paths (for six abnormal events) for Case Study 1 are not explicitly shown. To include the number of abnormal events associated with each path, multisets[45] are used herein. In a multiset, the elements are repeated with a multiplicity equal to the number of repetitions; and the cardinality of the multiset is the sum of the multiplicities of its elements. Note that a set is a multiset with unique elements. Hence, the abnormal events history in the process report in Table 2 is represented as a process record, A_m, represented using a multiset of cardinality 6, $[P^2_{pP}, P^3_{pP}, P^2_{sP}, P^2_{sP}, P^2_{sP}, P^2_{sQ}]$, or in the standard format for multisets, $[P^2_{pP}, P^3_{pP}, P^2_{sP}, P^2_{sQ}]_{1,\ 1,\ 3,1}$, where the multiplicities of P^2_{pP}, P^3_{pP}, P^2_{sP}, and P^2_{pQ} are 1, 1, 3, and 1, respectively, with an associated CO end-state.

It follows that, using the event-tree and set-theoretic formulation herein, any abnormal events history, comprised of abnormal events involving different process/quality variables, can be represented as process records; that is, multisets of paths (modeled as 6-tuples herein) traced by the process and quality variables as the SQOSs take actions. Also, for any process record, a unique and non-empty underlying set of paths is defined; whose elements are the various paths of the event trees, as discussed earlier.

Table 3. Abnormal Events History for Case Study 2

Variables	Least-Critical Abnormal Events	Moderately-Critical Abnormal Events	Most-Critical Abnormal Events	Trips (or ESDs)	Total Abnormal Events
pP_1	1720	21	116	2	1857
{pP_2, …, pP_4}*	176	0	3	3	179
pQ_1, …, pQ_3	504	5	0	0	509
Total abnormal events	2400	26	119	5	2545

*Variables have no high–high alarms and no override controller.

Returning to Figure 3, in step 2b, the overall abnormal events history is summarized as a multiset of paths. The second block from the bottom shows a multiset, for the entire alarm database, showing typical paths, P^2_{pP} and P^3_{pP}, and their multiplicities, M_1 and M_2. Finally, in step 2c, the likelihood data for the SQOSs is obtained from the overall abnormal events history using a tuple formulation, as illustrated for a FCCU in the next section. These contain the failure and/or success counts to be used in Bayesian analysis (Part II).

Note that an alternative formulation, using basis, consequence, and universal sets, to represent the event trees is presented in the Appendix. It presents a new way of representing and visualizing the event trees.

Next, these new formulations are used to represent the abnormal events history of an FCCU involving numerous process/quality variables over an extended period. Subsequently, it is used for Bayesian analysis in Part II.

Case Study 2: Abnormal Events History of the FCCU

In this case study, large DCS and ESD databases over an extended period of time, associated with an industrial FCCU at a major petroleum refinery that processes over 250,000 barrels of oil per day, are used. The unit has about 150–200 alarmed variables and as many as 5000–10,000 alarm occurrences per day—as a result of 500–1000 abnormal events daily. These databases (or logs) are stored on secured servers and updated dynamically with very small time delays (less than 30 s). Note that, because of data limitations, the SQOS[5] and SQOS[6] (automatic and manual ESD systems), are taken as a single SQOS. Also, four of its process and three of its quality variables are associated with ESD systems.

The abnormal events history of the primary variables for the study period is summarized in Table 3. A total of 2545 abnormal events occurred for the primary variables—2036 for the primary process and 509 for the primary quality variables. The primary process variable, pP_1, which involves all five SQOSs, experienced 1857 abnormal events (1720 least-critical, 21 moderately-critical, and 116 most-critical abnormal events, with two leading to ESDs). The remaining primary process variables, pP_2, pP_3, and pP_4 (which have no high–high/low–low alarms and override controllers), experienced only 179 abnormal events (176 least-critical and 3 most-critical leading to ESDs).

The abnormal events history for individual and groups of variables is represented by the branches (paths) of the event trees in Figures 5–8. The pPs and pQs that experienced least-critical abnormal events (i.e., entered their yellow-belt zones only), followed the path P^2_{pP} and P^2_{pQ}, respectively, leading to CO. Furthermore, the pPs and pQs that experienced moderately-critical abnormal events, followed P^3_{pP} and P^3_{pQ}, respectively, again leading to CO. When pP_1 entered its red-belt zone, but was returned to its normal operating range by the override controller, it followed the path, P^4_{pP}. Alternatively, when an ESD was triggered, it followed the path, P^5_{pP}, leading to an ESD. For the three pPs with no high–high/low–low alarms and no override controller, when they entered their red-belt zones, they triggered an automatic ESD, and followed the path P^5_{pP} (−III, −IV). Table 4 summarizes the set of paths, their multiplicities, and the associated end-states for Case Study 2.

This abnormal events history, with primary variables experiencing many abnormal events, is represented by two process records, A_1 (leading to end-state CO) and A_2 (leading to end-state ESD). Using the set-theoretic formulation, process record A_1 is represented as a multiset of paths, $[P^2_{pP}, P^3_{pP}, P^4_{pP}, P^2_{pQ}, P^3_{pQ}]_{1896,\ 21,\ 114,\ 504,\ 5}$, and process record A_2 as a multiset $[P^5_{pP}, P^5_{pP}\ (-\text{III}, -\text{IV})]_{2,\ 3}$. Clearly, the underlying sets of paths for the two process records are $\{P^2_{pP}, P^3_{pP}, P^4_{pP}, P^2_{pQ}, P^3_{pQ}\}$ and $\{P^5_{pP}, P^5_{pP}\ (-\text{III}, -\text{IV})\}$. Thus, the union of the two process records, A_1 and A_2, $[P^2_{pP}, P^3_{pP}, P^4_{pP}, P^5_{pP}, P^5_{pP}(-\text{III}, -\text{IV}), P^2_{pQ}, P^3_{pQ}]_{1896,\ 21,\ 114,\ 2,\ 3,\ 504,\ 5}$ summarizes

Table 4. Abnormal Event History of Primary Variables for Case Study 2

Type	Path	Symbolic Representation	Multiplicity	End-State
pP_1	P^2_{pP}	$F^1 \rightarrow S^2$	1720	CO
	P^3_{pP}	$F^1 \rightarrow F^2 \rightarrow S^3$	21	
	P^4_{pP}	$F^1 \rightarrow F^2 \rightarrow F^3 \rightarrow S^4$	114	
	P^5_{pP}	$F^1 \rightarrow F^2 \rightarrow F^3 \rightarrow F^4 \rightarrow S^5$	2	ESD
pP_2, …, pP_4	P^2_{pP}	$F^1 \rightarrow S^2$	176	CO
	P^5_{pP} (−III, −IV)	$F^1 \rightarrow F^2 \rightarrow S^5$	3	ESD
pQ_1, …, pQ_3	P^2_{pQ}	$F^1 \rightarrow S^2$	504	CO
	P^3_{pQ}	$F^1 \rightarrow F^2 \rightarrow S^3$	5	

Table 5. Failure and Success Counts for SQOSs in Response to All Primary Variables (for the Entire Study Period)

I	II		III		IV		V	
Failure; number of abnormal events (n_T)	Success (L_T^2)	Failure (K_T^2)	Success (L_T^3)	Failure (K_T^3)	Success (L_T^4)	Failure (K_T^4)	Success (L_T^5)	Failure (K_T^5)
2545	2400	145	26	116	114	2	5	0

Table 6. Failure and Success Counts for SQOSs in Response to pP_1 (for the Entire Study Period)

I	II		III		IV		V	
Failure; number of abnormal events (n_{pP_1})	Success ($L_{pP_1}^2$)	Failure ($K_{pP_1}^2$)	Success ($L_{pP_1}^3$)	Failure ($K_{pP_1}^3$)	Success ($L_{pP_1}^4$)	Failure ($K_{pP_1}^4$)	Success ($L_{pP_1}^5$)	Failure ($K_{pP_1}^5$)
1857	1720	137	21	116	114	2	2	0

the overall abnormal events history (of primary variables) during the study period. Using the tuple formulation for paths, it is represented as

$$[(0,1,\varphi,\varphi,\varphi,\varphi),(0,0,1,\varphi,\varphi,\varphi),(0,0,0,1,\varphi,\varphi),(0,0,0,0,1,\varphi),(0,0,\varphi,\varphi,1,\varphi),(0,1,\varphi,\varphi,\varphi,\varphi),(0,0,1,\varphi,\varphi,\varphi)]_{1896,21,114,2,3,504,5}$$

The above form permits calculation of the total failure and success counts, denoted as K_T^j and L_T^j ($j = 2, \ldots, 5$), respectively, for SQOS$^{2-5}$ in response to the abnormal events of the primary variables, by summation of the individual multiplicities of 0 and 1 for the five systems, as shown in Table 5.

In short, this new set-theoretic framework provides a compact representation in handling thousands of abnormal events depicting success/failure paths followed by the process and quality variables through the SQOSs. This framework facilitates the Bayesian analysis to compute failure probabilities of the SQOSs and incident probabilities in Part II.

In Table 5, the success and failure counts for SQOS^3 do not sum to the failure count for SQOS^2 (145), and the success count for SQOS^5 is not equal to the failure count for SQOS^4—because three of the pPs were not equipped with the high–high/low–low alarms and override controllers. Because the multisets store information for the SQOSs, specific to each variable, in a generic format, the new framework permits effective accounting of the success and failure counts for each SQOS. In the absence of these formulations, it would be very difficult to keep track of abnormal events, involving many variables, over an extended period of time.

Analogously, the abnormal events history for the variable pP_1 is represented as a combination of the two process records, B_1 and B_2, having multiset representations, $[P_{pP}^2, P_{pP}^3, P_{pP}^4]_{1720,\ 21,\ 114}$ and $[P_{pP}^5]_2$, leading to CO and ESD; that is, the union of B_1 and B_2, $[P_{pP}^2, P_{pP}^3, P_{pP}^4, P_{pP}^5]_{1720,\ 21,\ 114,2}$. Table 6 presents the failure (n_{pP_1}, $K_{pP_1}^j$) and success ($L_{pP_1}^j$) ($j = 2, \ldots, 5$) counts for the SQOSs in the response to the abnormal events of pP_1. Note that, in general, for individual variables, the failure and success counts for any SQOS is equal to failure counts for its previous SQOS, that is, for a primary variable pP_i, $n_{pP_1} = L_{pP_1}^2 + K_{pP_1}^2$ and $K_{pP_1}^{c-1} = L_{pP_1}^c + K_{pP_1}^c$, for $c = 3, 4, 5$. These results can be obtained easily by following the event trees in Figures 5–8 and distributing the counts along the succeeding branches.

Similarly, the abnormal events history for all primary process variables, pP_1, …, pP_4, is represented as $[P_{pP}^2, P_{pP}^3, P_{pP}^4, P_{pP}^5]_{1896,\ 21,\ 114,\ 5}$. The failure ($n_{pP}$, K_{pP}^j) and success (L_{pP}^j) ($j = 2, \ldots, 5$) counts for the SQOSs in the response to the abnormal events of pPs, are presented in Table 7.

Similar analysis can be done for secondary variables—to calculate the performances and pairwise interaction coefficients for SQOSs (in terms of failure probabilities) in response to abnormal events of secondary variables. Their values for individual as well as groups of variables can be monitored over a extended period of time to assess and improve the safety and operational performance of the process, for example, whenever their values increase, management and operators be alerted to take actions to address the root causes; for example, improved (1) DCS configurations and tuning, (2) operator training, (3) operating regimes, (4) process designs, and (5) alarm system configurations.

To summarize, this section presented a case study to convert the abnormal events history data for the primary variables of FCCU into information on the performances of SQOSs, described in Tables 4–7. In Part II, a multivariate Bayesian framework, based on copula theory, is presented that utilizes this information as *likelihood* to obtain knowledge on performances and pairwise interaction strengths for SQOSs and estimate the probabilities of occurrence of incidents.

Conclusions

In this Part I of a two-part article series, steps (i) and (ii) of a novel three-step dynamic risk assessment methodology

Table 7. Failure and Success Counts for SQOSs in Response to Primary Process Variables (for the Entire Study Period)

I	II		III		IV		V	
Failure; number of abnormal events (n_{pP})	Success (L_{pP}^2)	Failure (K_{pP}^2)	Success (L_{pP}^3)	Failure (K_{pP}^3)	Success (L_{pP}^4)	Failure (K_{pP}^4)	Success (L_{pP}^5)	Failure (K_{pP}^5)
2036	1896	140	21	116	114	2	5	0

for processing plants utilizing their large alarm databases are presented. This part presents a new data compaction method to convert data for massive numbers (millions) of abnormal events into compact likelihood data for real-time Bayesian analysis. Previous data structures, including event-tree incidence matrices, were unsuccessful in achieving this important objective for large amounts of abnormal event data.

Alarm data in abnormal event histories were represented efficiently by new event trees, showing the paths followed by the SQOSs in handling abnormal events. The event trees permit specific SQOSs to be assigned to various process and quality variables. The new multiset and tuple formulations provide a robust and efficient transformation into a compact representation of the success/failure paths through the SQOSs for several hundred process/quality variables. The multiset structures have on the order of 10^0 data entries; that is, a six order-of-magnitude reduction from millions of data entries—sharply increasing the efficiency in storage and handling of data. The FCCU case study showed the efficiency of the compaction method in handling large alarm datasets.

Acknowledgments

Partial support for this research from the National Science Foundation through grant CTS-0553941 is gratefully acknowledged. We thank Profs. Edward George and Shane Jensen of the Statistics Department at the Wharton School, Univ. of Pennsylvania, and Prof. Michael Carchidi of the Mechanical Engineering and Applied Mechanics Department at Penn for their helpful insights and comments.

Notation

Acronyms

ALM = alarm
BPCS = basic process control system
CO = continued operation
CPIs = chemical process industries
DCS = distributed control system
ES = end-state function
ESD = emergency shutdown
F = failure
FCCU = fluidized-catalytic-cracking unit
HI = high alarm
HH = high alarm
LL = low–low alarm
LO = low alarm
MPC = model-predictive controller
p*P*s = primary process variables
p*Q*s = primary quality variables
OOUS = operability-only upset state
QM = quality meltdown
QUS = quality upset state
RA = runaway reaction
RTN = return (of variable to its normal operating range)
s*P*s = secondary process variables
S = success
SISO = single-input, single-output
s*Q*s = secondary quality variables
SUS = safety upset state
SQOS = safety, quality, and operability system
S+QUS = safety and quality upset state

English letters

a_m = underlying set of paths for process record A_m
A_m, A_1, A_2 = process records
B_{pP}, B_{pQ} = basis set for primary, process or quality variables
B_{sP}, B_{sQ} = basis set for secondary, process or quality variables
B_P, B_Q = basis set for process or quality variables
C_{pP}, C_{pQ} = consequence set for primary, process or quality variables
C_{sP}, C_{sQ} = consequence set for secondary, process or quality variables
C_P, C_Q = consequence set for process or quality variables
C_{P+Q} = consequence set for process and quality variables
U_P, U_Q = universal set for process or quality variables
U_{P+Q} = universal set for process and quality variables
F^k = failure of SQOS^k (k = 1, …, 6)
K_T^j, L_T^j = failure and success counts for SQOS j (j = 2, …, 5) associated with all primary variables during the entire study period
$K_{pP_1}^j$, $L_{pP_1}^j$ = failure and success counts for SQOS j (j = 2, …, 5) associated with pP_1 variable during the entire study period
K_{pP}^j, K_{pP}^j = failure and success counts for SQOS j (j 2, …, 5) associated with primary process variables during the entire study period
P_{pP}^i, P_{pQ}^i = path i (in Figures 3 and 5–7) followed by a primary process or quality variable
P_{sP}^{ii}, P_{sQ}^{ii} = path ii (in Figure 8) followed by a secondary process or quality variable
n_T = number of abnormal events for all primary variables (see Table 5)
n_{pP_1} = number of abnormal events for pP_1 (see Table 6)
n_{pP} = number of abnormal events for all primary process variables (see Table 7)
S^k = success of SQOS^k (k = 1, …, 6)
SQOS^1 = basic process control system
SQOS^2 = operator (human + machine) corrective actions level I
SQOS^3 = operator (human + machine) corrective actions level II
SQOS^4 = override controller
SQOS^5 = automatic ESD system
SQOS^6 = manual ESD system

Subscript

l = counter for process records, l = 1, …, ∞

Superscripts

c = counter, c = 3, 4, 5
i = path counter for primary variables
ii = path counter for secondary variables
j = counter for failure and success counts, j = 2, …, 5
k = counter for SQOSs, k = 1, …, 6

Literature Cited

1. U.S. Chemical Safety and Hazard Investigation Board, Available at: http://www.csb.gov/. Accessed on April 16, 2011.
2. Chemical plants are feared as targets; views differ on ways to avert catastrophe. *The Washington Post*. 2001;16 December:A1.
3. Phimister JR, Oktem UG, Kleindorfer PR, Kunreuther H. Near-miss incident management in the chemical process industry. *Risk Anal*. 2003;23:445–459.
4. Rosenthal I, Kleindorfer PR, Elliott MP. Predicting and confirming the effectiveness of systems for managing low-probability chemical process risks. *Proc Saf Prog*. 2006;25:135–155.
5. Jones S, Kirchsteiger C, Bjerke W. The importance of near miss reporting to further improve safety performance. *J Loss Prev Process Ind*. 1999;12:59–67.
6. UNEP/ILO/WHO International Programme on Chemical Safety, Available at: http://www.who.int/ipcs/en/.
7. NRC, 1991. National Response Center, Available at: http://www.nrc.uscg.mil/nrchp.html.
8. U.S. Environmental Protection Agency, Available at: http://www.epa.gov/epahome/abcdata. htm.
9. RMP. 40 CFR Chapter IV, Accidental Release Prevention Requirements; Risk Management Programs Under the Clean Air Act Section 112(r)(7); Distribution of Off-Site Consequence Analysis Information. Final Rule, 65 FR 48108, 2000.

10. Rasmussen K. The experience with Major Accident Reporting System from 1984 to 1993. European Commission, Joint Research Center, EUR 16341 EN, 1996.
11. Major Accident Reporting System (MARS) Database, Available at: http://mahb.jrc.it/index.php?id=39.
12. Hazardous Substances Emergency Events Surveillance (HSEES) system by the Agency for Toxic Substances and Disease Registry (ATSDR), Available at: http://www.atsdr.cdc.gov/HS/HSEES/.
13. Process Safety Incident Database (PSID) by CCPS, Available at: http://www.aiche.org/CCPS/ActiveProjects /PSID/index.aspx.
14. Mary Kay O'Connor Process Safety Center at Texas A&M University, Available at: http://psc.tamu.edu/.
15. Meel A, Seider WD. Plant-specific dynamic failure assessment using Bayesian theory. *Chem Eng Sci*. 2006;61:7036–7056.
16. Yi W, Bier VM. An application of copulas to accident precursor analysis. *Manage Sci*. 1998;44:S257–S270.
17. Santamará Ramiro JM, Braña Aísa PA. *Risk Analysis and Reduction in the Chemical Process Industry*. New York: Blackie Academic and Professional, 1998.
18. Steinbach J. *Safety Assessment for Chemical Processes*. Weinheim: Wiley-VCH, 1999.
19. Morrison LM. Best practices in incident investigation in the chemical process industries with examples from the industry sector and specifically from Nova Chemicals. *J Hazard Mater*. 2004;111:161–166.
20. Meel A, Seider WD. Real-time risk analysis of safety systems. *Comput Chem Eng*. 2008;32:827–840.
21. Meel A, O'Neill LM, Seider WD, Oktem U, Keren N. Operational risk assessment of chemical industries by exploiting accident databases. *J Loss Prev Process Ind*. 2007;20:113–127.
22. Pariyani A, Seider, WD, Oktem UG, Soroush M. Incident investigation and dynamic analysis of large alarm databases in chemical plants: a fluidized-catalytic-cracking-unit case study. *Ind Chem Eng Res*. 2010;49:8062–8079.
23. Dumas R. Safety and quality: the human dimension. *Proc Saf*. 1987;32:11–14.
24. Wilkinson G, Dale BG. Integrated management systems: an examination of the concept and theory. *The TQM Magazine, Bedford*. 1999;11:2, 95.
25. Herrero SG, Saldana MAM, Del Campo MAM, Ritzel DO. From the traditional concept of safety management to safety integrated with quality. *J Saf Res*. 2002;33:1–20.
26. Williamsen MM. Six sigma safety—applying quality management principles to foster a zero-injury safety culture. *Proc Saf*. 2005;50:41–49.
27. Oktem UG. Near-miss: a tool for integrated safety, health, environmental and security management. *37th Annual AIChE Loss Prevention Symposium*. March 30–April 3, 2002.
28. MacGregor JF, Kourti T. Statistical process control of multivariate processes. *Control Eng Practice*. 1995;3:403–414.
29. SAPHIRE (Systems Analysis Programs for Hands-on Integrated Reliability Evaluations), Available at: https://saphire.inl.gov/.
30. PSAPACK 4.3 (Probabilistic Safety Analysis Package), Available at: http://200.0.198.11/ Programas/psa43d.htm.
31. RISKMAN Software, Available at: http://www.absconsulting.com/riskman.cfm.
32. WinNUPRA Software, Available at: http://winnupra.scientech.us/index.htm.
33. Safety Monitor Software, Available at: http://www.safetymonitor.org/.
34. RiskSpectrum Software, Available at: http://www.riskspectrum.com/.
35. Risk & Reliability Workstation, Available at: http://teams.eprisolutions.com/RR/default.aspx.
36. Meridium Software, Available at: http://www.meridium.com/software/index.asp.
37. PROACT Software, Available at: http://www.reliability.com/industry/proact/proact_suite.html.
38. Safeti QRA (Quantitative Risk Assessment) Package, Available at: http://www.dnv.com/ services/software/ products/safeti/safetiqra/.
39. RiskVu Software, Available at: http://www.isograph-software.com/rskover.htm.
40. QRA Packages by Dyadem, Available at: http://www.dyadem.com/products/.
41. ITEM Quantitative Risk Assessment System Software, Available at: http://www.itemsoft.com/iqras.html.
42. U.S. Chemical Safety and Hazard Investigation Board, "Urgent recommendation [BP Texas City Explosion and Fire, March 2004]," News release, 17 August 2005, Available at: , http://www.csb.gov/newsroom/detail.aspx?nid=215.
43. CCPS. *Layer of Protection Analysis—Simplified Process Risk Assessment*. New York: American Institute of Chemical Engineers, 2001.
44. Moschovakis YN. *Notes on Set Theory*, 2nd ed. New York: Springer, 2006.
45. Blizard WD. The development of multiset theory. *Modern Logic*. 1991;1:4, 353 (http://projecteuclid.org/DPubS?verb=Display&version=1.0&service=UI&handle=euclid.rml/1204834740&page=record).

Appendix: Alternative Representation of Event Trees

This appendix presents an alternative formulation of event trees, using basis, consequence, and universal sets. Several definitions follow that lead to the definition of the end-state function (ES).

Basis set. The sets of all the paths of event trees, traced by process/quality variables are defined as basis sets, analogous to the basis in linear algebra. The basis sets for the primary and secondary process and quality variables, based on the event trees presented in the Event-tree Formulations for Process and Quality Variables, are

$$B_{pP} = \{P^1_{pP}, P^2_{pP}, \ldots, P^7_{pP}\}, \qquad B_{pQ} = \{P^1_{pQ}, P^2_{pQ}, \ldots, P^7_{pQ}\}$$
$$B_{sP} = \{P^1_{sP}, P^2_{sP}, P^3_{sP}\}, \qquad B_{sQ} = \{P^1_{sQ}, P^2_{sQ}, P^3_{sQ}\}$$

Here, B_{pP} denotes the set of possible paths, traced by the primary process variables, as the SQOSs respond to their abnormal events. Consequently, the set of possible paths traced by all the process variables is

$$B_P = B_{pP} \cup B_{sP} = \{P^1_{sP}, P^2_{sP}, P^3_{sP}, P^1_{pP}, P^2_{pP}, \ldots P^7_{pP}\}$$

Similarly, for the quality variables, the basis set is

$$B_Q = B_{pQ} \cup B_{sQ} = \{P^1_{sQ}, P^2_{sQ}, P^3_{sQ}, P^1_{pQ}, P^2_{pQ}, \ldots, P^7_{pQ}\}$$

Therefore, the set of possible paths traced by all the process and quality variables is $B_{P+Q} = B_P \cup B_Q$. As a corollary, for any process that enters its S+QUS, the underlying sets of paths are subsets of B_{P+Q}. In addition, for any underlying set of paths, there always exists a basis set (defined above), of which it will be a subset.

Consequence set. The sets of end-states, attained by the paths of the event trees, are known as consequence sets. It follows that the consequence sets for the primary and secondary process and quality variables are

$$C_{pP} = \{\mathrm{CO}, \mathrm{ESD}, \mathrm{RA}\}; \qquad C_{pQ} = \{\mathrm{CO}, \mathrm{ESD}, \mathrm{QM}\}$$
$$C_{sP} = \{\mathrm{CO}\}; \qquad C_{sQ} = \{\mathrm{CO}\}$$

As discussed above, the sets of possible end-states attained by the process and quality variables are

$$C_P = C_{pP} \cup C_{sP} = \{\mathrm{CO}, \mathrm{ESD}, \mathrm{RA}\}$$
$$C_Q = C_{pQ} \cup C_{sQ} = \{\mathrm{CO}, \mathrm{ESD}, \mathrm{QM}\}$$

Consequently, the set of all possible end-states attained by the process and quality variables is $C_{P+Q} = C_P \cup C_Q = \{CO, ESD, RA, QM\}$.

Universal set. A universal set is an infinite set that consists of all possible process records, including the basis set. From the perspective of probability theory, universal sets are the sample space for all possible process records. Two universal sets associated with the process and quality variables are defined and denoted as U_P and U_Q. For example, U_P includes the basis set, B_P, plus all possible process records for processes in their SUS or OOUS. It follows that, U_P and U_Q are mutually exclusive sets and, $B_P \subseteq U_P$, $B_Q \subseteq U_Q$. In a similar way, the universal sets for the primary and secondary, process and quality variables are defined, denoted as U_{pP}, U_{pQ}, U_{sP}, and U_{sQ}, respectively.

The universal set for the process and quality variables, U_{P+Q}, includes all possible process records for processes in their upset states (S + QUS, QUS, SUS and OOUS). Note that

$$|U_{P+Q}| > |U_P \cup U_Q|$$

And

$$|U_P| > |U_{pP} \cup U_{sP}| \qquad |U_Q| > |U_{pQ} \cup U_{sQ}|$$

where || denotes the cardinality of a set.

Surjective, noninjective, ES function. A function f: $U \rightarrow C$ is surjective if and only if, for every c in the codomain, C, there is at least one u in the domain U with $f(u) = c$. It is non-injective if and only if there exist at least two distinct elements, u_1 and u_2, in U with $f(u_1) = f(u_2)$. Hence, the surjective, non-injective, ES: $U \rightarrow C$, maps the elements of the universal set U (domain) to its end-state, an element of its consequence set, C (codomain). For example, ES(u) denotes the end-state, when (i) u is a path followed by any process/quality variable, or (ii) u is a process record, represented as a multiset of paths followed by the process/quality variables.

Using these definitions, the event trees in Figures 5–8 for the primary and secondary process and quality variables, respectively, are represented using the following functional dependences: ES: $U_{pP} \rightarrow C_{pP}$, ES: $U_{pQ} \rightarrow C_{pQ}$, ES: $U_{sP} \rightarrow C_{sP}$, and ES: $U_{sQ} \rightarrow C_{sQ}$. Clearly, these functional dependences permit a condensed representation of the event trees.

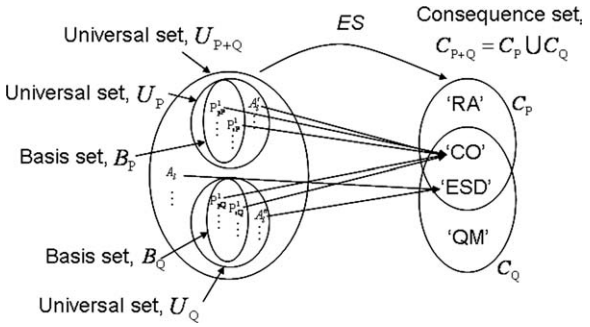

Figure A1. Schematic of the ES function for a general abnormal events history, showing several process records and individual paths traced by the process and quality variables.

Thus, the process record of Case Study 1 can be functionally represented as ES(A_m) = CO, where multiset A_m (represented as $[P^2_{pP}, P^3_{pP}, P^2_{sP}, P^2_{sQ}]_{1,\ 1,\ 3,\ 1}$) $\in U_{P+Q}$ and its underlying set of paths, $a_m \in B_{P+Q}$.

It follows that the functional representation of the overall event-tree formulation for all the primary and secondary process and quality variables is

$$ES : U_{P+Q} \rightarrow C_{P+Q}$$

Figure A1 shows a schematic of the functional representation of all the event-tree paths (P^i_{pP}, P^i_{pQ}, P^{ii}_{sP}, and P^{ii}_{sQ}, with $i = 1, \ldots, 7$, and $ii = 1, \ldots, 3$) and possible process records (A_l, A'_l, and A''_l, with $l = 1, \ldots, \infty$, having underlying sets of paths, $a_l \in B_{P+Q}$, $a'_l \in B_P$, and $a''_l \in B_Q$) for the primary and secondary, process and quality variables.

Manuscript received Aug. 12, 2010, and revision received Mar. 11, 2011.