Fast Process Security Assessment Theory

Korkut Uygun and Yinlun Huang
Dept. of Chemical Engineering and Materials Science, Wayne State University, Detroit, MI 48202

Helen H. Lou
Dept. of Chemical Engineering, Lamar University, Beaumont, TX 77706

DOI 10.1002/aic.10179
Published online in Wiley InterScience (www.interscience.wiley.com).

This communication introduces a comprehensive theory for process security assessment. The theory can quickly provide mathematically proven upper and lower bounds on minimum time to disaster (the time disaster conditions will be reached in worst-case scenarios). Computational efficiency and reliability are achieved by performing process security assessment based on a time-derivative–based approach, rather than conducting massive process dynamic simulations. Further, the methodology enables prioritizing the process variables critical to plant security. This facilitates pinpointing the possible reasons of a security-threatening situation, quantifying the importance of each disturbance factor on the system's vulnerability, and creating a prioritized list of improvements/counteractions for ensuring process security. Two runaway reactor examples are studied to demonstrate the methodology for security-threat analysis. © 2004 American Institute of Chemical Engineers *AIChE J,* 50: 2187–2202, 2004

Keywords: process security, γ-analysis, priority list, runaway reaction

Introduction

Shortly after the national tragedy of September 11, 2001, the Center for Chemical Process Safety (CCPS) under AIChE developed a security vulnerability assessment (SVA) methodology (CCPS, 2002). Soon after, the National Institute of Justice, in collaboration with Sandia National Laboratories, introduced an extended SVA methodology to quantify the security degree of chemical facilities (NIJ, 2002). The two methodologies use "the best judgment of security, safety, and other appropriate professionals," and permit the comparison of security levels of facilities and the prioritization of security enhancement efforts. The methodologies are systematic, although essentially experience based. They have been widely adopted by chemical plants. Nevertheless, a very recent report by U.S. GAO (2003) indicates that "the extent of security preparedness in chemical facilities" is currently "unknown."

Chemical plant security consists of three main components: physical security, cyber security, and process security. Although the first two can be ensured through improving plant infrastructure and management, and thus are technically relatively simple, the last one must quantify the relationships between process operation and process security and therefore is *fundamentally* and *technically* very complicated. Note that no fundamental method can hope to prevent the consequences of a bomb being dropped on the facility. However, the inherent vulnerability of a process in cases of sabotages and accidents can be reduced by developing better-designed processes. As such, process security is mainly concerned with these technological attacks by adversaries who have sufficient technical background on production. Such attacks are completely unexpected, complex, multiscaled, and can be very destructive. Thus, the most challenging tasks for process security are: (1) how to *rapidly* and *precisely* assess process security, and (2) if not secure, how to *quickly* identify *effective* actions to eliminate or otherwise mitigate the security threat(s). It was recently suggested by Lou et al. (2003) that process security should be a separate subject of interest, under a broader umbrella of safety methodologies. The goal of process security studies is the design of secure processes through use of rigorous and

Correspondence concerning this article should be addressed to Y. Huang at yhuang@wayne.edu.

deterministic simulation-oriented methods, as it is also accepted in this work.

Process safety is a mature area, and numerous safety tools are already available. Because safety and security are very closely related, some of the existing safety tools can be applied to the security problem. Although the exact relationship between safety and security is a subject of debate, it is quite often true that improving safety implies improving security, and vice versa. However, a *safe* plant is not necessarily *secure*, given that the safety problem regards only accidental occurrences, whereas the element of harmful intent also has to be considered in evaluating security.

Further, existing safety tools are either qualitative or probabilistic. Hazard and Operability (HAZOP) (CCPS, 1992) is an excellent method for qualitative analysis based on experience. There are also many index-based methods, such as the Prototype Index for inherent safety (Edwards and Lawrence, 1993) and Inherent Safety index (Heikkila et al., 1996). Although producing quantitative results, these indices are not based on rigorous modeling studies, but are typically based on heuristics. Risk-assessment methods, such as event tree/fault tree approaches, form the most mathematical branch of safety assessment techniques; they are also probabilistic. In the matter of process security, a low probability of occurrence is not a sufficient condition for security because the consequences can be easily catastrophic.

Also, the similarity of purpose between inherently safer design and process security should not be overlooked. The ultimate goal in both studies is to design systems that are not subject to risks, whether these are safety risks, environmental risks, or security risks (Hendershot, 2003). The solution methods, however, are significantly different. Inherently safer design strategies are based on checklists or structured brainstorming tools (Palaniappan et al., 2002) that promote creativity but are qualitative, and risk-assessment methods that are probabilistic. The methods of process security, however, are proposed to be rigorous optimization and simulation methods that are both quantitative and deterministic (Lou et al., 2003).

There is a major void of security analysis tools, based on process system science, that can produce reliable evaluations of process security of a given plant. Clearly, the development of an exact security science should be considered as a challenge to the chemical engineering community. Such a methodology is an absolute necessity in the face of the recent exposures of the vulnerabilities of conventional risk-assessment methods. Needless to say, development of process security tools is an urgent, but also long-term project.

Recently, Lou et al. (2003) defined process security from the perspective of process operation, and outlined the difference between process safety and process security. Furthermore, they introduced a process operational zone classification method and a process security index. In their method, however, determination of a process security level requires extensive, time-consuming dynamic simulations. This is impractical for large-scale problems. Also note that the available process simulators are incapable of modeling the types of malfunctions/disturbances that lead to disaster scenarios; thus simulation studies can rarely achieve reliable estimations of worst-case scenarios.

Very recently, Uygun et al. (2003) introduced a novel process security analysis method: the γ-analysis. By this method, the time derivatives of a plant dynamic model are investigated directly. This allows quick estimations for the minimum time that the process will go to disaster under a security threat. In this regard, a mathematical definition of *process security* was introduced and the *process critical time* measure was developed. It is proven that *process critical time* is an underestimate of the actual time the process will take to go to disaster in a worst-case scenario. *Process critical time*, therefore, forms a sufficient, but not necessary condition for the *process security* of a given plant. Note, however, that the *process critical time* measure is an underestimation based on the worst-case scenario. Therefore, the estimations on process security tend to exaggerate the severity of the situation.

In this work, a comprehensive theory of process security assessment will be introduced. First, it will be proven that the *process critical time* can be used as sole decision criterion for single-state systems. For multidimensional systems, the *security limit time* will be introduced as an upper bound for the actual minimum time to disaster. Calculation of an upper bound, along with the above-mentioned lower bound, enables the evaluation of a confidence interval for the minimum time a process will go to disaster in the worst-case scenario. This allows a thorough assessment of process security vulnerability, and facilitates conclusive decision making about the process. In development of *security limit time*, a definition of synergistic variables will be introduced. It will be mathematically confirmed that for synergistic variables, the *security limit time* is a valid upper bound. Furthermore, a systematic threat-analysis methodology will be developed, which uses the γ-analysis technique for identification and analysis of possible security threats and their sources. A number of new security-related criteria will also be introduced. These facilitate the analysis, quantification, and prioritization of the sources of security threats, and the identification of possible security enhancement methods. Two examples will be studied to demonstrate the method introduced, as well as to describe the details of security modeling.

Process Security Modeling

In this work, it is assumed that a process security model is available and is in the following form

$$d\boldsymbol{y}/dt = \boldsymbol{f}(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d}) \tag{1}$$

where $\boldsymbol{y}$ is the vector of system variables; $\boldsymbol{u}$ is the vector of manipulated variables; and $\boldsymbol{d}$ is the vector of disturbances. Vectors $\boldsymbol{u}$ and $\boldsymbol{d}$ are together designated as the *inputs*. Note that, in a security-threatening situation, both manipulated variables and disturbances may be the causes of security threat.

Also note that the nominal operation point of the system is described by vector $\boldsymbol{y}_0$. For a continuous system, determination of the nominal point is obviously given by the steady-state operation. For a batch or semibatch process, the operation undergoes several modes and thus it has no usual nominal point concept as in a continuous system. The measures and methods developed in this work can use any point in an operation range as a reference point, provided it is used consistently.

In process security studies, a system model should possess two essential properties:

(1) *Property 1: Postnominal validity*. The system model should be valid not only for the normal operation range, but for

the entire operation range up to the point of disaster. This point is critical because certain assumptions valid in nominal operation (such as constant heat capacities and no phase-change) will not be valid during the transition to the disaster point. The model should be able to describe the system beyond the normal operation as discussed by Lou et al. (2003), which could be achieved by either a single but more complex model or a multitude of simple models each valid within a certain range.

(2) *Property 2: Correct identification of vulnerable variables.* Regular process models consider only a few variables as possible disturbance sources. In process security, many system components can be malfunctioning or under adverse control, and thus they have to be accounted for in the model. To achieve this, a basic requirement is creating a list of *vulnerable* and *invulnerable* variables.

In a process model, the system dynamics is described by a number of governing equations, as exemplified in Eq. 1. When a conventional model is being adopted for use in process security studies, the differences in the fundamental assumptions for process security should be noted. Some of the system variables that were assumed to be following their governing equations may be subject to accidents/attacks that cause them to change abruptly. For instance the contents of a tank may be quickly removed as a result of a puncture/hole in the equipment. Such variables are exposed to direct attacks and thus are *vulnerable*. For process security modeling, vulnerable variables should be considered directly as disturbances. On the other hand, some variables, typically intrinsic variables such as temperature and pressure, cannot be directly manipulated. These variables will be referred to as *invulnerable* variables because they are not subject to direct attacks. It should be noted that the invulnerability refers to direct exposure only; thus an invulnerable variable can still be manipulated indirectly through disturbances and manipulated variables.

Also, it is important to clarify how the disaster is defined in process security studies. The definition of critical variables is intrinsically related to the definition of disaster.

Definition 1: Critical Variables. In many chemical systems, a plant model consists of more than one system variable, yet only a few of these need to be used directly to define disaster boundaries, such as pressure. These variables are designated as *critical variables*. To distinguish the critical variables from the rest of the system variables, the critical variable will be denoted as y_c, and the noncritical variables will be indicated by the subscript n as y_n. The analysis methodology developed in this work is based on a single critical variable only. For a system with more than one critical variable, the analysis method described here should be repeated for each such variable. Also note that by definition the critical variable has to be an invulnerable variable.

γ-Analysis

A mathematical process security assessment theory requires a mathematical definition of process security itself, and therefore these definitions are reviewed first.

Definition 2 (Uygun et al., 2003). *Process security* is the ability of a system to retain secure operation when suffering subtle attacks. The term "subtle attacks," in this context, limits the attention to more technologically crafty attacks, rather than those direct and brute force attacks, such as bombing. Such attacks are mathematically represented as disturbances ($\boldsymbol{d}$) and crippled control and safety systems ($\boldsymbol{u}$) in the process security model.

Remark 1. Note that, although disturbances and manipulated variables are treated in the same way in the examples in this work, it is possible to use the methodology developed to analyze existing safety systems as outlined by Uygun et al. (2003). Therefore, the two will be differentiated throughout the text. This point will be discussed again in the Security-threat analysis section in the definition of *threat vectors*.

Definition 3 (Uygun et al., 2003). A process is secure if

$$\tau \geq \tau^r \tag{2}$$

where τ, designated the minimum time to disaster (MTD), is the minimum time required by the process to move from the nominal operation point to the security disaster zone; τ^r, designated the *resolution time*, is the minimum time needed for detecting the threat, making decisions, and taking necessary countermeasures to eliminate the threat.

Definition 4. The reference points for defining the minimum time to disaster τ are the nominal operation point $y_{c,0}$ and the disaster point $y_{c,d}$ for the critical variable. In this work, a disaster condition is defined mathematically as

$$y_c \geq y_{c,d} \tag{3}$$

The disaster condition is based on the critical variable only. Thus, y_c and $y_{c,d}$ are scalars.

In chemical processes, a disaster zone is characterized by high values of critical variable(s), such as a high pressure and/or a high temperature. The definition above, as well as certain equations in the γ-analysis method, is formulated accordingly. In applications to the problems with different disaster zone topologies, these should be modified as necessary.

A more mathematical definition of MTD is given by the following dynamic optimization problem

$$\tau = \min_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} \int_{y_{c,0}}^{y_{c,d}} \frac{dy_c}{f_c(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d})} \tag{4}$$

s.t.

$$\frac{d\boldsymbol{y}_n}{dt} = \boldsymbol{f}_n(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d}) \tag{5}$$

$$\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{6}$$

The problem above is essentially a minimum-time type dynamic optimization problem with a nonlinear system model. Although it is possible to solve the dynamic optimization problem directly, there are two important obstacles. First, the solution identification process is generally quite time consuming. Second, and more important, the convergence properties of existing dynamic optimization algorithms are generally poor if the models are nonlinear, which limits the reliability of the results. This problem is caused by the complexity introduced by the time dependency, where the nonlinearity of the problem may cause a variety of convergence problems.

The principal idea in the γ-analysis is to investigate directly the time derivatives of system dynamic equations, rather than to go through a time-consuming integration process. This simplifies the optimization problems, thus substantially improving both convergence and computational efficiency.

Definition 5 (Uygun et al., 2003). The *process critical time* ω is a worst-case estimate of τ, defined as

$$\omega = \frac{|y_{c,d} - y_{c,0}|}{\gamma} \tag{7}$$

where

$$\gamma = \max_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} f_c(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d}) \tag{8}$$

s.t.

$$\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{9}$$

Note that $f_c = dy_c/dt$ is the speed of the system moving from one state to the other. Because the derivative cannot exceed γ, the system cannot move from the nominal point (y_0) to disaster in a time interval shorter than ω. Therefore, ω is an underestimate of the actual minimum time to disaster (τ) (that is, $\tau \geq \omega$), provided the maximization problem is solved to globality. A detailed proof was provided by Uygun et al. (2003).

Remark 2. γ is defined as the maximum of the time-derivative function, given that security-threatening events frequently occur at high temperatures and pressures. For different cases, alternative formulations described by Uygun et al. (2003) can be used.

Remark 3. The physical limitations given by Eq. 9 in Definition 5 are critical to the solution of the optimization problem because the solution will be very likely bounded by these variable limits. That is, at least some constraints will be active at the optimum and thus have a significant effect on ω. Therefore, they should be determined carefully and precisely.

Remark 4. In certain cases, it is possible that some additional constraints exist, such as property estimation correlations. It is also possible that the physical limits on variables, as defined by Eq. 9, cannot be stated as simple bounds in the optimization problem, but have to be imposed as more complex constraints. Such constraints should be added to the γ-analysis problem as additional constraints. The second case study exemplifies this situation and clarifies some important aspects of process security modeling.

Enhancing accuracy

In calculation of *process critical time*, the time derivative is approximated by its maximum value in producing a lower bound on MTD. This approach is similar to applying single-step Euler integration, and therefore is not very accurate. Naturally, the accuracy can be improved by using multiple steps. The principal idea is to partition the output zone of the critical system variable into subregions, and to evaluate separate values of critical time for each subregion. The *process critical time* will then be simply the sum of subregional critical times. A mathematical representation of this accuracy enhancement method is given below

$$\omega = \sum_{i=1}^{n} \omega^i \tag{10}$$

where

$$\omega^i = \frac{\Delta y_c}{\gamma^i} \tag{11}$$

$$\Delta y_c = \frac{|y_{c,d} - y_{c,0}|}{n} \tag{12}$$

and

$$\gamma^i = \max_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} f_c(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d}) \tag{13}$$

s.t.

$$\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{14}$$

$$y_c \in [y_{c,0} + (i-1)\Delta y_c, y_{c,0} + i\Delta y_c] \tag{15}$$

where n is the number of subregions that is indexed by superscript i. As the number of regions increases, the accuracy will also increase.

Lemma 1. *If the γ value is zero or negative for a subregion, then the process is secure.*

Remark 5. If the γ value cannot be positive, then it is impossible for the system to have an increase in the critical variable beyond the current level. In other words, the disaster zone is not reachable. According to Definition 3, a disaster condition can *never* be reached and thus the process is *secure*. In this case, the *process critical time* is considered to be infinite.

Theorem 1. *Process critical time will be equal to the actual minimum time to disaster (τ), if a sufficiently large number of subregions are used for a single-state system that is defined by a single differential equation.*

Proof of Theorem 1. Equation 4 with a single system variable can be written as

$$\tau = \min_{y_c,\boldsymbol{u},\boldsymbol{d}} \int_{y_{c,0}}^{y_{c,d}} \frac{dy_c}{f_c(y_c, \boldsymbol{u}, \boldsymbol{d})} \qquad y_c, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{16}$$

Note that the constraints in Eq. 5 do not apply because there is only one system variable.

For a system with n subregions, Eq. 16 can be rewritten as

$$\tau = \min_{y_c, \boldsymbol{u}, \boldsymbol{d}} \int_{y_c^{i,\min}}^{y_c^{i,\max}} \frac{dy_c}{f_c(y_c, \boldsymbol{u}, \boldsymbol{d})} \tag{17}$$

where the integral bounds are given by

$$y_c^{i,\min} = y_{c,0} + (i-1)\Delta y_c \tag{18}$$

$$y_c^{i,\max} = y_{c,0} + i\Delta y_c \tag{19}$$

$$\Delta y_c = \frac{|y_{c,d} - y_{c,0}|}{n} \tag{20}$$

At the limit, when $n \to \infty$, $y_c^{i,\min} \approx y_c^{i,\max} = y_c^i$. The important point is that, because there is only one single system variable and y_c^i is practically fixed by the subregion partitioning, the only degree of freedom in f_c is the input variable vectors, $\boldsymbol{u}$ and $\boldsymbol{d}$. Therefore, for a single-variable system, it can be stated as

$$f_c(y_c^i, \boldsymbol{u}, \boldsymbol{d}) = f_c(\boldsymbol{u}, \boldsymbol{d})|_{y_c = y_c^i} \tag{21}$$

Accordingly, the integral may be simplified as

$$\int_{y_c^{i,\min}}^{y_c^{i,\max}} \frac{dy_c}{f_c(y_c, \boldsymbol{u}, \boldsymbol{d})} = \frac{\Delta y_c}{f_c(\boldsymbol{u}, \boldsymbol{d})|_{y_c = y_c^i}} \tag{22}$$

Also, the system variable y_c is no longer a decision variable. Therefore, substituting Eq. 22 into Eq. 17 yields

$$\tau = \min_{\boldsymbol{u}, \boldsymbol{d}} \left[\lim_{n\to\infty} \sum_{i=1}^{n} \frac{\Delta y_c}{f_c(\boldsymbol{u}, \boldsymbol{d})|_{y_c = y_c^i}} \right] \tag{23}$$

In Eq. 23, the solutions of the terms in the summation are independent of each other, that is, the value of derivative obtained at i does not affect that obtained at $i + 1$, and so on. This is true because there are no additional system variables that can create any correlation. Hence, in Eq. 23, the minimum of the sum equals the sum of minimums

$$\tau = \lim_{n\to\infty} \sum_{i=1}^{n} \min_{\boldsymbol{u}, \boldsymbol{d}} \left[\frac{\Delta y_c}{f_c(\boldsymbol{u}, \boldsymbol{d})|_{y_c = y_c^i}} \right] \tag{24}$$

or, alternatively,

$$\tau = \lim_{n\to\infty} \sum_{i=1}^{n} \frac{\Delta y_c}{\max\limits_{\boldsymbol{u}, \boldsymbol{d}} f_c(\boldsymbol{u}, \boldsymbol{d})|_{y_c = y_c^i}} \tag{25}$$

The maximum term in the denominator is the γ term in Eq. 13. Substitution of Eq. 13 into Eq. 25 yields

$$\tau = \lim_{n\to\infty} \sum_{i=1}^{n} \frac{\Delta y_c}{\gamma^i} \tag{26}$$

According to Eqs. 10 to 15, this is equal to the *process critical time*. Therefore, for a single-variable system, if a sufficiently large number of subregions is used, then

$$\tau = \omega \tag{27}$$

■

Remark 6. Theorem 1 works because an infinite number of subregions equate to discretizing the system equations and solving them as algebraic equations. However, the discretization is made on the system output (dependent) variable rather than the time (independent) variable. Multiple system variables require a discretization along all the system variables. This will exponentially increase the number of subregions, and in turn, the number of optimizations to be solved, which is thus impractical. An alternative method for tackling multivariable systems will be outlined in the following section.

Security Limit Time

A primary objective in this work is to develop a valid upper bound to τ to complement the lower bound outlined above. An obvious upper bound is nominal operation, which means the process never goes to the disaster zone; thus the upper-bound time is infinity. Naturally this estimate does not provide any information. The necessity here is to create an upper bound such that we can claim "*in the worst-case scenario, the process will reach the disaster zone in less time than the upper bound*."

In evaluation of *process critical time*, all system variables (except the critical variable) are treated as vulnerable variables as a consequence of the worst-case scenario assumption underlying the analysis technique. Obviously, this is not valid for invulnerable variables that follow their governing equations. For multisystem-variable problems, this approach results in exaggeration of the calculated γ value. Thus, ω is valid as a strict underestimate of the minimum time to disaster. However, it is possible to use the same method to create an upper bound so that a confidence interval can be created for the actual minimum time to disaster for the process. The definition of synergy is necessary to accomplish this task.

Definition 6. Synergistic variables are variables for which the following relationship is true

$$\int_D f_c dy_c \geq \int_{D'} f_c|_{\boldsymbol{y}^n = \boldsymbol{y}_{n,0}} dy_c \qquad \forall\ \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{28}$$

where $\boldsymbol{y}^n$ designates the vector of noncritical variables; D and D' stand for the quickest paths (with respect to time) to the disaster. Note that the paths may be different because there is an additional constraint in the latter case.

Remark 7. Equation 28 can be effectively stated as "*the average value of the derivative function, in transition to disaster, does not increase when the noncritical variable is fixed to its nominal value*." Basically, synergistic variables form inherent positive-feedback loops with the critical variable that may lead to instability. It should be underlined that this synergy is not desirable from the viewpoint of safety, security, and control because it is a possible source of instability. Therefore, "synergy" does not have the usual positive meaning in the context of this work.

A simple example of synergistic variables is the temperature in a reactor (y_c) and the temperature in the cooling jacket (y_n). In many cases, the synergistic variables in a system are obvious and can be determined without any mathematical analysis.

Definition 7. The *security limit time* is calculated by

$$\omega^s = \lim_{n \to \infty} \sum_{i=1}^{n} \frac{\Delta y_c}{\gamma^{s,i}} \tag{29}$$

where

$$\gamma^{s,i} = \max_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} f_c(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d}) \tag{30}$$

s.t.

$$\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{31}$$

$$\boldsymbol{y} = \boldsymbol{y}^0 \tag{32}$$

$$y_c \in [y_{c,0} + (i-1)\Delta y_c, \; y_{c,0} + i\Delta y_c] \tag{33}$$

$$\Delta y_c = \frac{|y_{c,d} - y_{c,0}|}{n} \tag{34}$$

A more compact and equivalent statement is

$$\omega^s = \int_{y_{c,0}}^{y_{c,d}} \frac{dy_c}{\max\limits_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} f_c|_{y_n = y_{n,0}}} \qquad \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{35}$$

Theorem 2. *The security limit time ω^s is a valid upper bound on the actual minimum time to disaster, provided the noncritical variables are synergistic variables.*

Proof of Theorem 2. Note that Eq. 4 describes the quickest paths in Eq. 28. Accordingly, Eq. 28 can be equivalently stated as

$$\min_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} \int_{y_{c,0}}^{y_{c,d}} \frac{dy_c}{f_c} \le \min_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} \int_{y_{c,0}}^{y_{c,d}} \frac{dy_c}{f_c|_{y_n = y_{n,0}}} \tag{36}$$

Also noting the general inequality

$$\min_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} \int_{y_{c,0}}^{y_{c,d}} \frac{dy_c}{f_c|_{y_n = y_{n,0}}} \le \int_{y_{c,0}}^{y_{c,d}} \left(\min_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} \frac{1}{f_c|_{y_n = y_{n,0}}} \right) dy_c \tag{37}$$

Thus, combining Eqs. 36 and 37 yields

$$\min_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} \int_{y_{c,0}}^{y_{c,d}} \frac{dy_c}{f_c} \le \int_{y_{c,0}}^{y_{c,d}} \left(\min_{\boldsymbol{y},\boldsymbol{u},\boldsymbol{d}} \frac{1}{f_c|_{y_n = y_{n,0}}} \right) dy_c \tag{38}$$

Finally, using the definitions in Eqs. 4 and 35, it can be stated that

$$\tau \le \omega \tag{39}$$

■

Remark 8. According to Eq. 39 and Definition 5, we have

$$\omega \le \tau \le \omega^s \tag{40}$$

Thus, the *process critical time* and the *security limit time* bound the minimum time to disaster.

In certain cases, Eq. 28 can be verified without rigorous mathematics, as the relationship between variables makes obvious. When this is not possible, Eq. 28 is not easy to prove mathematically. In such cases, an alternative condition will be defined that is easier to determine based on direct analysis of the derivative functions.

Definition 8. Strictly synergistic variables are variables for which the following relationship is true

$$\left(\frac{\partial f_c}{\partial y_n} \right) \left(\frac{\partial y_n}{\partial y_c} \right) \ge 0 \qquad \forall \;\; \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{41}$$

where the y_n designates noncritical variable(s).

Remark 9. Equation 41 can be summarized as "*the synergistic variable increases (decreases) with an increase in the critical variable, and this increase (decrease) further increases the critical variable.*" In effect, as will be proven below, this requires that the value of the derivative function is always smaller (or unchanged) when the noncritical variable is fixed to its nominal value. Note that in Definition 6, the inequality is required only on the average values. Thus, Definition 7 is much more strict compared to the original definition.

Lemma 2. *A strictly synergistic variable satisfies synergy condition.*

Proof of Lemma 2. We focus on the single noncritical variable case first. In this case, the system is considered as

$$\frac{dy_c}{dt} = f_c(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d}) \tag{42}$$

$$\frac{dy_n}{dt} = f_n(\boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d}) \tag{43}$$

Note that y_n denotes the single noncritical variable. Consider the effect of a change of Δy_c on y_n initially caused by a perturbation of the inputs. This induces a total change in the derivative function of the critical variable, given by

$$\Delta f_c = \left[\left(\frac{\partial f_c}{\partial y_n} \right) \left(\frac{\partial y_n}{\partial y_c} \right) + \frac{\partial f_c}{\partial y_c} \right] \Delta y_c \tag{44}$$

By comparison, when the noncritical variables are fixed, the change attributed to a change in critical variable is

$$\Delta f_c\big|_{y=y^0} = \left[\left(\frac{\partial f_c}{\partial y_n}\right)\left(\frac{\partial y_n}{\partial y_c}\bigg|_{y_n=y_{n,0}}\right) + \frac{\partial f_c}{\partial y_c}\right]\Delta y_c \tag{45}$$

However, because y_n is fixed, the term $\partial y_n/\partial y_c\,|_{y_n=y_{n,0}}$ equals zero. Subtracting Eq. 45 from Eq. 44 with this in mind yields

$$\Delta f_c - \Delta f_c\big|_{y_n=y_{n,0}} = \left(\frac{\partial f_c}{\partial y_n}\right)\left(\frac{\partial y_n}{\partial y_c}\right)\Delta y_c \tag{46}$$

The strict synergy condition is

$$\left(\frac{\partial f_c}{\partial y_n}\right)\left(\frac{\partial y_n}{\partial y_c}\right) \geq 0 \tag{47}$$

Note that because $y_{c,d} > y_{c,0}$, in transition from nominal operation to disaster, $\Delta y_c > 0$. With Eq. 47, it can be stated that

$$\Delta f_c - \Delta f_c\big|_{y_n=y_{n,0}} \geq 0 \tag{48}$$

Also note that, by definition

$$f_c\big|_{y_n=y_{n,0}}(\boldsymbol{y}_0) = f_c(\boldsymbol{y}_0) \tag{49}$$

As given in Eq. 49, the derivatives are equal at the nominal point. By Eq. 48, an increment of Δf_c always exceeds the increment of $\Delta f_c\,|_{y_n=y_{n,0}}$. Therefore, Eqs. 48 and 49 can be combined to yield

$$f_c \geq f_c\big|_{y_n=y_{n,0}} \qquad \forall\ \boldsymbol{y}, \boldsymbol{u}, \boldsymbol{d} \in [\textit{physical limits}] \tag{50}$$

For multiple noncritical variables, the necessary condition in Eq. 41 becomes

$$\left(\frac{\partial f_c}{\partial y_{n,j}}\right)\left(\frac{\partial y_{n,j}}{\partial y_c}\right) \geq 0 \qquad j = 1, 2, \cdots, m \tag{51}$$

where m is the number of noncritical variables.

Accordingly, in this case, Eq. 46 is slightly different, that is

$$\Delta f_c - \Delta f_c\big|_{y_n=y_{n,0}} = \sum_{j=1}^{m}\left(\frac{\partial f_c}{\partial y_{n,j}}\right)\left(\frac{\partial y_{n,j}}{\partial y_c}\right)\Delta y_c \tag{52}$$

Each term in the summation is greater than zero, according to the necessary condition in Eq. 51. By following the same logic above, it can be stated that

$$f_c \geq f_c\big|_{y_n=y_{n,0}} \tag{53}$$

and, therefore, Lemma 2 is again valid. ■

Remark 10. The above analysis, including Definition 7, is based on the condition $y_{c,d} > y_{c,0}$. If the reverse is true, the inequality in Definition 7 should be reversed, and the maximization problems should be modified as explained in Remark 2.

Security Threat Analysis

The *security limit time* (ω^s), along with the *process critical time* (ω), provide valid and reliable upper and lower bounds on the minimum time to disaster (τ). This allows performing process security assessment for chemical systems. However, the γ-analysis method enables further analysis of the process for a more thorough process security assessment, that is, the quantification of the effects of each variable on the system and the path to disaster. With respect to its purpose, this is similar to an event tree/fault tree analysis, but is not probabilistic, and enables quantitatively assessing the effect of each variable *directly* on process security. The analysis method to be described below first requires an introduction of input and threat vectors.

Input and threat vectors

In the γ-analysis method, the disturbances and manipulated variables are treated similarly and are designated as the inputs. Therefore, the input vector is defined as

$$z = \begin{bmatrix} \boldsymbol{u} \\ \boldsymbol{d} \end{bmatrix} \tag{54}$$

A more important product of this optimization problem, however, is the maximizing values of the inputs, $\boldsymbol{u}^*$ and $\boldsymbol{d}^*$. These two vectors are combined to form the threat vector, denoted z^*. The following augmented vector form is used here

$$z^* = \begin{bmatrix} \boldsymbol{u}^* \\ \boldsymbol{d}^* \end{bmatrix} \tag{55}$$

Remark 11. Note that in Eq. 55, all manipulated variables ($\boldsymbol{u}$) are considered to be under adverse control. It is possible to let some of these variables assume normal (regulatory) control and study the effect, which is particularly useful in test and design of safety and security systems. These correctly working (that is, resuming regulatory action) controls should not be included in vector $\boldsymbol{u}$, but imposed as constraints for optimization. Uygun et al. (2003) discussed this point in further detail.

Note that based on the number of regions used in the accuracy enhancement method (Eqs. 10–15), a new z^* is calculated for each subregion, which does not necessarily have the same values. In this case, it can be stated that

$$z^*(y) = \{z^{*,i},\ \forall\ y \in [y_c^{i,\min}, y_c^{i,\max}]\} \tag{56}$$

where superscript i denotes the subregion in the grid and $z^{*,i}$ represents the worst-case input for that particular subregion. Equation 56 can be used accordingly to evaluate the threat profile and simulate the system.

Remark 12. Threat vectors are particularly helpful in identifying specific trends in the threat profiles. For instance, some variables remain constant at a maximizing value, indicating a direct proportionality. In more complex systems, a specific trend line, such as an oscillating input, may be detected, which could yield important insights about the attacks and system characteristics.

System priority list

In analyzing the sources of security threats, it is important to quantify the importance of each variable on process security. The necessary information here is the total effect of a variable on the time to disaster. The information should also be normalized so that it is possible to compare the security impacts of different variables. The method described below is basically for solving the γ-analysis problem with the variables fixed at their nominal values. The suggested measure is the *significance* as defined below.

Definition 9. The effect of a certain variable on the system security is referred to as the *significance*, and is defined as

$$\alpha_x = \frac{\omega^x - \omega}{\omega} \tag{57}$$

Here, ω^x is the value of the process security time obtained when variable x is fixed to its nominal value. This variable can be any disturbance source.

The significance values relay the following information: "*If a certain variable cannot be manipulated in a security attack scenario by the saboteurs, then the process critical time* (ω) *would increase by a factor of* α." Equation 57 yields the effect of each variable in a normalized manner, so that a comparison of the variables, as well as a comparison of different cases, is possible. A large value of significance indicates that the variable can drastically affect the minimum time to disaster. It should be noted that it is possible to have a significance value of infinity for a variable if (and only if) the situation described in Lemma 1 (having a negative or zero value for γ) is observed. This situation indicates that this variable is crucial for a disaster condition to occur. A zero value, on the other hand, indicates that the variable is not important with respect to process security.

One vital aspect of the significance values should be underlined: The *significance* value reflects the effect of a variable on the critical variable, but not on other system variables. The significance value is calculated based on the worst-case–based assumptions; it is not a measure of the normal operating condition.

Note that when the accuracy enhancement method (Eqs. 10 through 15) is used, the critical variable cannot be fixed at its nominal value. It is possible not to use the enhancement method and also report a significance value for the critical variable, but this is not recommended because of accuracy-related concerns. As a rule of thumb, it is suggested that at least 100 subregions should be used for analyzing a problem.

Another important point to note is that in calculation of significance values, the *security limit time* concept is actually being used to capture the total impact of fixing every single variable. This enables a quick evaluation of the *security limit time* based on different variables (and different assumptions) using the *priority list*. Consider two system variables, $y_{n,k}$, and $y_{n,l}$. If the *security limit time* assuming $y_{n,k}$ is the only invulnerable variable, $\omega^s = \omega^{y_{n,k}}$, and the significance values for both variables are known, then $\omega^{y_{n,l}}$ can be evaluated by using Eq. 57 for both significance values

$$\frac{\alpha_{y_{n,k}}}{\alpha_{y_{n,l}}} = \frac{(\omega^{y_{n,k}} - \omega)/\omega}{(\omega^{y_{n,l}} - \omega)/\omega} \tag{58}$$

Rearrangement yields

$$\omega^{y_{n,l}} = \omega + \frac{\alpha_{y_{n,k}}}{\alpha_{y_{n,l}}}(\omega^{y_{n,k}} - \omega) \tag{59}$$

where $\omega^{y_{n,l}}$ is the unknown value and $\omega^{y_{n,k}}$ is the *security limit time* based on variable $y_{n,k}$.

Before further discussions of the information made available by the *priority list*, a number of other information matrices need to be introduced.

Combined significance matrix and nonlinear contribution matrix

The significance values reveal the dependency of the *process critical time* on process variables. These significance values can be used to create a linear and separable approximation to γ-values. However, the combined affects may also be important. This effect can be quantified through a procedure similar to that used in obtaining the *priority list*, by fixing two variables to their nominal values. The combined significance can thus be calculated as

$$\lambda_{x_1x_2} = \frac{\omega^{x_1x_2} - \omega}{\omega} \tag{60}$$

where x_1 and x_2 are any two variables (input and/or system variables).

Naturally, fixing a variable twice does not have any additional effect, so that

$$\lambda_{x_ix_i} = \alpha_{x_i} \tag{61}$$

The *combined significance matrix* (CSM) is a symmetric matrix where the elements in the first diagonal are the elements of the *priority list*. In essence, the combined significance values in the off-diagonal relate to the derivative with respect to the two variables used in calculations, that is

$$\lambda_{x_1x_2} \propto \text{avg}\left[\frac{\partial^2\omega}{\partial x_1 \partial x_2}\right] \tag{62}$$

Note that because the extreme points (that is, y_0 and y^*) are being used in calculation of the combined significance, the average value of the derivative, rather than the value at a specific point, is evaluated. Accordingly, for a linear and separable system, the following relationship should hold true

$$\lambda_{x_1x_2} = \alpha_{x_1} + \alpha_{x_2} \tag{63}$$

Accordingly, the CSM allows the calculation of the nonlinear contribution, denoted as $\mu_{x_1x_2}$, of the combined effect as follows

$$\mu_{x_1x_2} = \lambda_{x_1x_2} - \alpha_{x_1} - \alpha_{x_2} \tag{64}$$

The individual nonlinear contribution values can be combined to form a *nonlinear contribution matrix* (NCM). The diagonal elements in the NCM are naturally zero as a result of Eqs. 61 and 63. It is possible to evaluate the multiple combination affects as well, although these can also be approximately calculated from the NCM. Creating variations of the NCM (by simultaneously fixing multiple variables) is straightforward and will not be further discussed here, but can be used as seen necessary.

Process security assessment

In this work, five new process analysis/decision-making criteria have been introduced: *security limit time*, *threat vector*, *priority list*, *combined significance matrix* (CSM), and *nonlinear contribution matrix* (NCM). These criteria can be used, together with the *process critical time*, to form a security-threat analysis methodology. This methodology can be used not only for process security vulnerability assessment, but also for outlining the path for process operational security enhancement. The following list introduces three steps of analysis, each using a different combination of the available criteria.

(1) *Step 1: Evaluate the limits.* Use the *process critical time* (ω) and the *security limit time* (ω^s) to evaluate the limits of the actual time to disaster (τ). If $\omega^s < \tau^r$, then the process is not secure. If $\omega > \tau^r$, then the process is secure. Other scenarios are inconclusive.

This analysis forms the core of the fast security assessment theory introduced in this work and is applicable, provided an appropriate security model is available. It enables quick process security assessment (one complete evaluation typically takes <1 min); thus, it is practical to run different scenarios for sensitivity analysis. This property can be used, for instance, to test and design control/safety/security equipment by running scenarios where some of the equipment is working and observing their effectiveness in preventing disasters.

(2) *Step II: Investigate the threat.* The *threat vector* and the *priority list* enable identifying the sources of security threats and quantifying the importance of each. The *priority list* quantifies the direct effect of each variable on process security, and therefore facilitates understanding of the factors that are important in process security, rather than relaying on information about how this effect is realized. The *threat vector*, on the other hand, is used to observe any unusual correlations and trends in the process variables as the system moves toward a disaster point. Such trends will not always be observed; they can convey crucial information in terms of system vulnerability.

Together, the *threat vector* and the *priority list* help understand how various factors and variables affect the system. The *priority list* is by default a hierarchical list of what to do in an emergency because a variable with great significance indicates that its control considerably slows down the transition to disaster. The *threat vector* and the *priority list* can also be used to eliminate the variables that have no or little importance for further security studies. Further, the *priority list* can be used as a starting point for designing a more secure process, and/or retrofitting existing systems, which of course is the ultimate goal in process security studies.

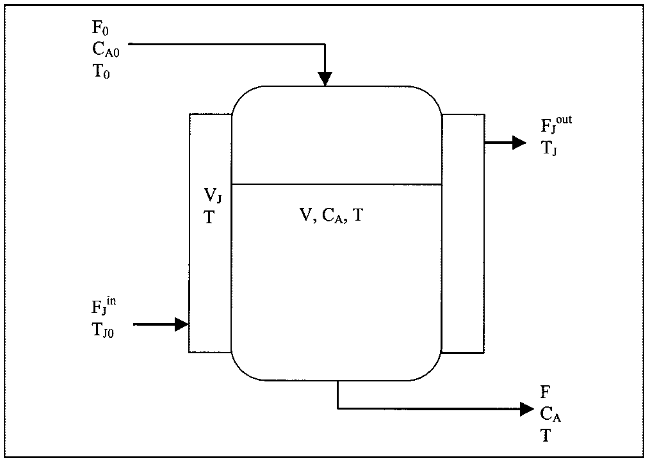

Figure 1. Nonisothermal CSTR with a cooling jacket.

(3) *Step III: Identify combined effects.* It is possible that a certain combination of variables account for security risks in operation. For instance, for an exothermic reaction with two reactants, the reactant concentrations are likely to be significant factors, but this effect will be observed only if both reactants are in abundance. CSM and NCM can be used to observe such correlations. Significant entries in the NCM should be taken into consideration during process design as well.

The three-step procedure above facilitates maximum use of the information gathered by the security threat analysis method. Naturally, Step 1 is the primary component of security assessment, but as elaborated above, the other two steps convey very important information about the vulnerabilities of the system. This enables a thorough analysis, thus improving system design.

The security assessment method introduced offers the primary advantage of producing quantitative evaluations based on the process model, which is not offered by commonly used safety techniques. The evaluations are computationally efficient; thus, this method is much faster compared to simulation–optimization-based strategies.

Case Studies on Process Security

To demonstrate the efficacy of the developed security assessment methodology, two examples are investigated. A process security model derivation is also performed in the second example, which exemplifies some of the discrepancies between security modeling and conventional process modeling.

Analysis of a nonisothermal CSTR operation

Figure 1 shows a jacketed continuously stirred tank reactor (CSTR) system, originally given by Luyben (1990), but with slight modifications to render it more interesting for security analysis. The nominal system model is given below

$$\frac{dV}{dt} = F_0 - F \tag{65}$$

Table 1. Variable Ranges and Parameters for Example 1

Variable Name	Minimum	Nominal	Maximum
Reactor feed flow rate (F_0) (m^3/h)	0	1.13	1.98
Reactor output flow rate (F) (m^3/h)	0	1.13	1.98
Jacket feed flow rate (F_J^{in}) (m^3/h)	0	1.41	2.83
Jacket output flow rate (F_J^{out}) (m^3/h)	0	1.41	2.83
Reactor feed temperature (T_0) (K)	222.22	294.44	555.56
Temperature in reactor (T) (K)	222.22	333.33	555.56
Temperature in jacket (T_J) (K)	222.22	330.33	555.56
Inlet concentration (C_{A0}) (kmol/m^3)	0	8.01	16.02
Concentration (C_A) (kmol/m^3)	0	3.92	16.02
Volume of liquid in reactor (V) (m^3)	0.02	1.36	1.98
Coolant volume in jacket (V_J) (m^3)	0.002	0.11	0.198

Parameters

Jacket feed temperature (T_{J0}) = 294.44 K	Cp = 3.14 kJ/kg K
E = 69,780 kJ/kmol	ρ = 800.95 kg/m^3
U = 3066.3 kJ/h m^2 K	C_J = 4.19 kJ/kg K
A_H = 23.23 m^2	ρ_J = 997.98 kg/m^3
R = 8.314 kJ/kmol K	λ = −69,780 kJ/kmol
A = 7.08 × 10^{10} h^{-1}	

$$\frac{dV_J}{dt} = F_J^{IN} - F_J^{OUT} \tag{66}$$

$$V\frac{dC_A}{dt} + C_A\frac{dV}{dt} = F_0C_{A0} - FC_A - VkC_A \tag{67}$$

$$V\frac{dT}{dt} + T\frac{dV}{dt} = F_0T_0 - FT - \frac{\lambda VkC_A}{\rho C_P} - \frac{UA_H}{\rho C_P}(T - T_J) \tag{68}$$

$$V_J\frac{dT_J}{dt} + T_J\frac{dV_J}{dt} = F_J^{IN}T_{J0} - F_J^{OUT}T_J + \frac{UA_H}{\rho_J C_J}(T - T_J) \tag{69}$$

where

$$k = Ae^{-E/RT} \tag{70}$$

The system parameters and variable ranges are listed in Table 1. It is assumed that this model can characterize the system behavior in the entire operational zone. The existing feedback control system is considered to be crippled, so the manipulated variables are also treated as disturbances. For process security modeling, only the reactor temperature (T) and the jacket temperature (T_J) are considered as invulnerable variables. Because pressure correlation is not available, the critical variable is taken as reactor temperature (T) that, in fact, is the primary variable of concern in a possible runaway reaction scenario.

The γ-analysis is performed using a general algebraic modeling system (GAMS; Brooke et al., 1998). In evaluating the *security limit time*, the jacket temperature (T_J) is taken as the only invulnerable variable, given that the reactant concentration and the liquid volume can be altered from outside. The *process critical time* (ω) and the *security limit time* (ω^s) are calculated using different numbers of regions, as displayed in Table 2. The accurate values of ω and ω^s are 1.71 and 73.27 s, respectively. Such a time interval for the minimum time to disaster indicates serious process security vulnerability. This conclusion is in agreement with that of Uygun et al. (2003), suggesting that the process was severely vulnerable to security attacks based on the lower bound (1.71 s) only.

Table 2. Process Critical Time and Security Limit Time for Example 1

No. of Regions	ω (s)	ω^{nf} (s)
1	0.089	0.090
4	1.256	12.036
10	1.527	20.949
20	1.620	48.506
50	1.675	57.570
100	1.693	64.559
1000	1.710	72.509
2000	1.711	72.929
10,000	1.711	73.274

The *priority list* in Table 3 demonstrates that two variables, the jacket temperature (T_J) and the volume of liquid in the reactor (V), constitute 99% of the total significance. Interestingly, the reactant concentration (C_A) has a low significance value (0.432), which indicates that a runaway reaction is possible even at the normal operation concentration. A major result of the *priority list* is the information that the system requires some initial heat to push it toward the disaster, and this cannot be accomplished by only increasing the reactant concentration. A large significance value for volume (17.45) is observed, as expected, because a low volume of materials can be heated much more quickly, which means the initial heat necessary for the disaster path can be introduced much more quickly.

The jacket temperature is considered as an invulnerable variable in calculation of the *security limit time*; thus its effect (a retardation of about 71 s) is already evaluated. Because the significance values are obtained using the same principle with the *security limit time*, the *priority list* can be used to evaluate the effect of postulating other system variables as invulnerable variables. In this case, given that C_A has a significance value of 0.432, the retardation attributed to fixed concentration is 43.2% of the *process critical time* (ω): an extra time of about 0.7 s. A similar calculation yields the effect of V as about 30 s.

The NCM is displayed in Table 4. In the NCM, the pair of jacket temperature (T_J) and the reactant concentration (C_A) has a very large positive combined effect, indicating that if these two variables are simultaneously kept under control, then the transition to disaster cannot happen before about 322 s. This indicates that, whereas the nominal reactant concentration is

Table 3. Priority List (1000 Subregions) for Example 1

Variable Name	Significance	Percent Significance
Reactor feed flow rate (F_0)	0.021	0.036
Reactor output flow rate (F)	0.000	0.000
Jacket feed flow rate (F_J^{in})	0.000	0.000
Jacket output flow rate (F_J^{out})	0.000	0.000
Inlet concentration (C_{A0})	0.000	0.000
Reactor feed temperature (T_0)	0.051	0.087
Volume of liquid in reactor (V)	17.450	29.396
Coolant volume in jacket (V_J)	0.000	0.000
Concentration (C_A)	0.432	0.727
Temperature in jacket (T_J)	41.407	69.754

Table 4. Nonlinear Contribution Matrix (100 Subregions) for Example 1

	F_0	F	F_J^{in}	F_J^{out}	C_{A0}	T_0	V	V_J	C_A	T_J
F_0	0.000	0.000	0.000	0.000	0.000	−0.001	0.281	0.000	0.101	17.810
F	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
F_J^{in}	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
F_J^{out}	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C_{A0}	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
T_0	−0.001	0.000	0.000	0.000	0.000	0.000	0.673	0.000	0.023	52.887
V	0.281	0.000	0.000	0.000	0.000	0.673	0.000	0.000	11.990	15.190
V_J	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
C_A	0.010	0.000	0.000	0.000	0.000	0.023	11.990	0.000	0.000	146.652
T_J	17.810	0.000	0.000	0.000	0.000	52.887	15.190	0.000	146.652	0.000

enough to realize runaway conditions, this is valid if heat can be introduced to the system by the jacket. Otherwise, the system vulnerability is significantly less drastic. The feed temperature (T_0) also has a significant positive combined effect with jacket temperature, which confirms the previous conclusion that the system needs an initial push through external heat sources, and the reactant concentration alone is not sufficient to drive the system to disaster conditions.

The information given by the *priority list* and the NCM can have multiple uses. First, none of the inputs has any important effect on the thermal runaway. Therefore, any safety/security system must directly and rapidly alter the system variables: the jacket temperature (T_J), the liquid volume (V) in the reactor, and the reactant concentration (C_A). These short stopping measures are likely to succeed, whereas conventional control systems are not. It is recommended that a rapid coolant flush system be installed in the jacket because this can create some significant extra time in a disaster situation, although it is not a complete solution to the problem.

Naturally, these conclusions drawn from the *priority list* and the NCM are not surprising for a simple system like this. The advantages, however, are twofold. First, the evaluation on process security is *quantitative*. For instance, the effect of volume holdup in the reactor (V) is about 42.1% (that is, 29.40/69.75) of the jacket temperature (T_J). This renders a quantitative security-oriented decision-making process possible. Second, the *priority list* and the NCM are evaluated automatically. For a large and complex system, where connections are less obvious and the conclusions are difficult to draw based on engineering judgment, these tools allows quick filtering of the important factors and variables to assist in decision making.

Analysis of a semibatch polymerization process

Figure 2 depicts a problem that was previously studied by Kneale and Forster (1968). This problem was more recently studied by Shacham et al. (2000) for process-hazard assessment, which is an excellent example of using simulation for safety assessment. The system uses the following highly exothermic polymerization reaction that produces a polyol lubricant starting from n-butanol and propylene oxide

$$C_4H_9OH + (n+1)C_3H_6O \rightarrow C_4H_9(OC_3H_6)_nOCH_2CHOHCH_3 + \textit{Heat} \tag{71}$$

The reactor initially contains a certain amount of catalyzed alcohol. The oxide feed is then started. A typical batch operation takes 33.3 h. In operation, a large quantity of volatile oxides exists, which can be triggered as a security threat by an adversary.

System Model. The original system model is given as (Ingham et al., 2000)

$$\frac{dM}{dt} = F - V \tag{72}$$

$$C\frac{dM}{dt} + M\frac{dC}{dt} = F - V - r \tag{73}$$

$$\frac{dX}{dt} = r \tag{74}$$

$$Mc_P\frac{dT}{dt} = Fc_P(T_0 - T) - V\lambda - r(-\Delta H_{rxn}) - Q \tag{75}$$

where

$$r = kCM \tag{76}$$

$$k = A\exp\left(-\frac{E}{RT}\right) \tag{77}$$

$$Mw = \frac{M_0 + X}{N} \tag{78}$$

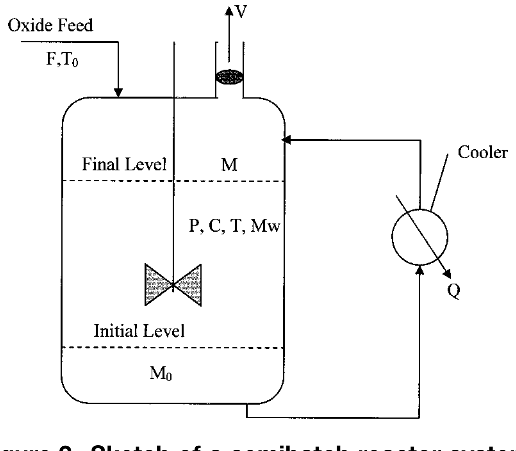

Figure 2. Sketch of a semibatch reactor system.

Table 5. Variable Ranges and Parameters for Example 2

Variable Name	Minimum	Initial	Nominal	Maximum
Reactor feed rate (F) (kg/min)	0	100	100	400
Vapor discharge rate (V) (kg/min)	0	0	1000	8000
Reactor feed temperature (T_0) (K)	274	353	353	673
Cooling rate (Q) (kJ/min)	0	0	369,600	2,225,000
Mass in reactor (M) (kg)	4400	4400	89,400	800,000
Concentration of oxide (C) (kg/kg)	0	0	0.383	1
Reactor temperture (T) (K)	274	353	385	673
Polymer molecular weight (Mw) (kg/mol)	74	74	927.922	6727
Reactor pressure (P) (kPa)	100	100	675.377	3000

Parameters

Initial alcohol charge (N) = 59.46 kmol	Cp = 3.14 kJ/kg K
Initial molecular weight = 74 kg/kmol	E = 21,000 kJ/kmol
λ = 670 kJ/kg	$A = 9 \times 10^9$ min^{-1}
R = 1.987	ΔH_{rxn} = 997.98 kJ/kg oxide

Table 5 lists the notation used in the system, as well as the system parameters and variable bounds used in this study. In this system, the reactor pressure is the critical variable, which can be evaluated by the following correlation

$$P = 100 \times C\left[\exp\left(-\frac{3430}{T} + 11.7\right) + 1.45 \times 10^{-3} Mw\right] \tag{79}$$

In the system model, Eq. 72 corresponds to the variation of the total mass in the reactor (M) with time. The concentration of oxides is given by Eq. 73, where C is the oxide mass per total mass in the reactor. The mass of oxide reacted is calculated by Eq. 74. Equation 75 enables the calculation of the temperature in the system. The molecular weight of the polymer can be calculated using the correlation in Eq. 78. It is assumed that the system model can reliably characterize the system behavior in the entire operational zone.

Process Security Modeling. Process security and the γ-analysis have some different requirements on the system model. In this example, some of these differences are illustrated.

First of all, it is important to note that the cooling system is modeled simplistically (the heat transfer unit, which cools down the reactor contents through a recirculation system, is not modeled in detail). Yet, the model is capable of predicting malfunctions in the cooling system through changing the heat removed by recirculation (Q).

An interesting feature of this process is the bursting disc, which will rupture if the pressure goes beyond a limit of 800 kPa, thus allowing discharge of the oxide vapor and preventing pressure buildup, and thus avoiding explosion. The discharge velocity is normally a function of the system pressure, temperature, and a valve coefficient (Ingham et al., 2000). For the purpose of process security, the discharge valve and the cooling system are subject to security attacks. Therefore, these variables will be considered directly as disturbances, instead of using their descriptions in the original model (Ingham et al., 2000). The bounds on cooling duty are calculated, assuming that a heat transfer unit of 200 m^2 and an overall heat transfer coefficient of 1000 W/m^2·K are available.

Unlike the first example, the critical variable is not directly defined by a differential equation. The method of tackling such problems was outlined by Uygun et al. (2003), by which the time derivative of the critical variable is calculated and its correlation to the available differential equations is established. The pressure is a function of three state variables, that is

$$P = P(T, C, Mw) \tag{80}$$

From the chain rule,

$$\frac{dP}{dt} = \frac{\partial P}{\partial T}\frac{dT}{dt} + \frac{\partial P}{\partial C}\frac{dC}{dt} + \frac{\partial P}{\partial Mw}\frac{dMw}{dt} \tag{81}$$

Combining Eqs. 74 and 78 yields the following time derivative of polymer molecular weight

$$\frac{dMw}{dt} = \frac{d\left(\frac{M_0 + X}{N}\right)}{dt} = \frac{1}{N}\frac{dX}{dt} = \frac{r}{N} \tag{82}$$

By using Eqs. 72 and 73, the derivative for oxide concentration will be

$$\frac{dC}{dt} = \frac{1}{M}\left(F - V - r - C\frac{dM}{dt}\right) = \frac{F - V - r - C(F - V)}{M} \tag{83}$$

The time derivative of temperature is already defined by Eq. 75. With the partial derivatives in Eq. 81 substituted, the pressure can be expressed as

$$\frac{dP}{dt} = \left[100 \times C\exp\left(-\frac{3430}{T} + 11.7\right)\left(\frac{3430}{T^2}\right) \times \left(\frac{Fc_P(T_0 - T) - V\lambda - t(-\Delta H_{rxn}) - Q}{Mc_P}\right)\right]$$

$$+\left[100 \times 1.45 \times 10^{-3} C \frac{r}{N}\right] + \left[100 \times \left(\exp\left(-\frac{3430}{T} + 11.7\right) + 1.45 \times 10^{-3} Mw\right)\left(\frac{F - V - r - C(F - V)}{M}\right)\right] \quad (84)$$

This allows defining the pressure directly as the critical variable.

Additional Limitations. There are two additional requirements to use this model in γ-analysis, both attributed to having the physical limits in Eq. 79 that cannot be described directly by the variable bounds, as also mentioned in Remark 4. Note that in the γ-analysis method, all variables are subject to change independently of each other. However, in the model described by Eqs. 72 through 79, the variables Mw, M, and C are correlated because of total mass conservation, which requires that

$$Mw \times N + C \times M = M \quad (85)$$

If Eq. 85 is not imposed as a constraint, it is possible to obtain a result that has, for instance, 20 tons of polymer, but a total mass of 5 tons, which is naturally an unrealistic situation.

Another important point is that, despite the calculation of a separate time derivative, the pressure, as described in Eq. 79, is not an independent variable. This correlation, therefore, still has to be imposed on the problem as an equality constraint.

Problem Formulation. The γ-analysis problem for this system, with the additions described above, is formulated as follows

$$\omega = \sum_{i=1}^{n} \frac{\Delta P}{\gamma^i} \quad (86)$$

where

$$\gamma^i = \max \frac{dP}{dt} \quad (87)$$

s.t.

$$P \in [P_0 + (i - 1)\Delta P, P_0 + i\Delta P] \quad (88)$$

$$\Delta P = \frac{|P_d - P_0|}{n} \quad (89)$$

$$P = 100 \times C\left[\exp\left(-\frac{3430}{T} + 11.7\right) + 1.45 \times 10^{-3} Mw\right] \quad (90)$$

$$Mw \times N + C \times M = M \quad (91)$$

Table 6. Process Critical Time and Security Limit Time for Example 2

No. of Regions	ω (s)	ω^{nf} (s)
1	15.8	18.3
4	103.9	360.0
10	118.3	861.8
20	130.7	1079.3
50	137.6	1213.2
100	139.8	1257.4
1000	141.8	1296.9
2000	141.9	1299.1
10,000	142.0	1300.9

Choice of Nominal Point. As this example is a semibatch operation, the nominal point is not defined directly by the operation itself. Also, choosing the initial condition as the nominal point is misleading for process security analysis because there is no oxide in the system initially. Accordingly, a different choice of nominal point is necessary to take advantage of the security threat analysis methodology. For this example, a hypothetical nominal point has been chosen (see Table 5). This point corresponds to the maximum temperature obtained in normal operation (385 K) as reported by Shacham et al. (2000), and is observed to be a critical boundary, given that it is the most probable point for divergence from the nominal operation (as discussed below in the analysis of the *priority list*). This condition is based on the situation in the reactor in normal operation, at approximately 850 min of batch processing. One exception is that, to be able to observe the effect of the safety discharge (V), it is assumed that a disc rupture has occurred and a discharge rate of 1000 kg/min is attained. One important note is that the pressure in the system at this point is 675.4 kPa. In calculation of the *priority list*, CSM, and NCM, this value has been taken as y_c^0. Accordingly, the formula in Eq. 59 cannot be used here for direct calculation because the initial condition used in calculation of *process critical time* and *security limit time* is different from the values used for evaluation of significance values.

Results. The results of the γ-analysis are displayed in Table 6. The *process critical time* is 142 s. The *security limit time*, using the molecular weight (927.92 kg/mol, the nominal value) as the invulnerable variable, is evaluated as 1301 s, or roughly 22 min. These results indicate possible security vulnerability for the process, but relatively mild compared to that of the first example. The reason for not using temperature as an invulnerable variable will be discussed shortly.

There are several interesting results for this case, which can be observed from the *priority list* in Table 7 and the system profiles in the disaster scenario in Figure 3. The temperature has a significance of infinity, indicating that the system cannot reach the disaster conditions if its temperature is maintained below 385 K. This also means that the *security limit time*, if temperature is considered an invulnerable variable, will be infinite. Therefore, any security attack would have to involve an increase in temperature beyond the normal operation limits.

Another important result, which can be obtained from the system profiles in Figure 3, is that the molecular weight (Mw) is kept at its minimum value, which means no polymerization has occurred. Combining this information with the large value of *security limit time* obtained with a large molecular weight enables drawing the following conclusion: a security attack should happen with low polymer molecular weights, below 1000 kg/mol. Note that, although inhibiting the reaction would ensure low molecular weights, because the exothermic reaction is the only major heat source in the system (the feed temper-

Table 7. Priority List (1,000 Subregions) for Example 2 (Based on Nominal Condition)

Variable Name	Significance	Percent Significance*
Reactor feed rate (F)	1.024	8.144
Vapor discharge rate (V)	5.333	42.420
Reactor feed/recycle temperature (T_0)	0.678	5.397
Cooling rate (Q)	0.491	3.903
Mass in reactor (M)	2.369	18.841
Concentration of oxide (C)	0.591	4.701
Reactor temperature (T)	∞	∞
Polymer molecular weight (Mw)	2.086	16.594

*Temperature not included in calculation.

ature is relatively minor as reflected by the significance values), such an action would also prevent disaster possibilities. Therefore, molecular weight and temperature form an autocontrol pair that works to reduce inherent vulnerabilities: a security attack would have to increase the system temperature, but before a high polymer molecular weight is obtained, which as a large molecular weight decreases the pressure (as a consequence of the total mass conservation imposed by Eq. 91). Although such a situation is not impossible, as demonstrated by a *security limit time* of 22 min, it is obviously difficult unless an external source of heat, not represented in the model, is available. Also note that Figure 3 depicts that the total system mass and concentration have to be increased gradually so as to maximize the rate of increase of pressure.

Other entries in the priority list indicate that the discharge rate, if the bursting disc is operable, has a very high significance, and would normally prevent any disaster scenario. System mass and feed rate also have effects comparable to the molecular weight. The cooling rate, which has a relatively low significance, is also an important factor because of its obvious effect on the system temperature.

As displayed in Table 8, the NCM shows that the largest nonlinear combined effect is obtained with C and V. Because both entries are positive, this finding confirms that the safety discharge (V), if operable, will prevent the occurrence of disaster conditions. Note that if the discharge tube was too small, which would yield a small maximum for V, the significance value would also be much smaller, and we would be able to

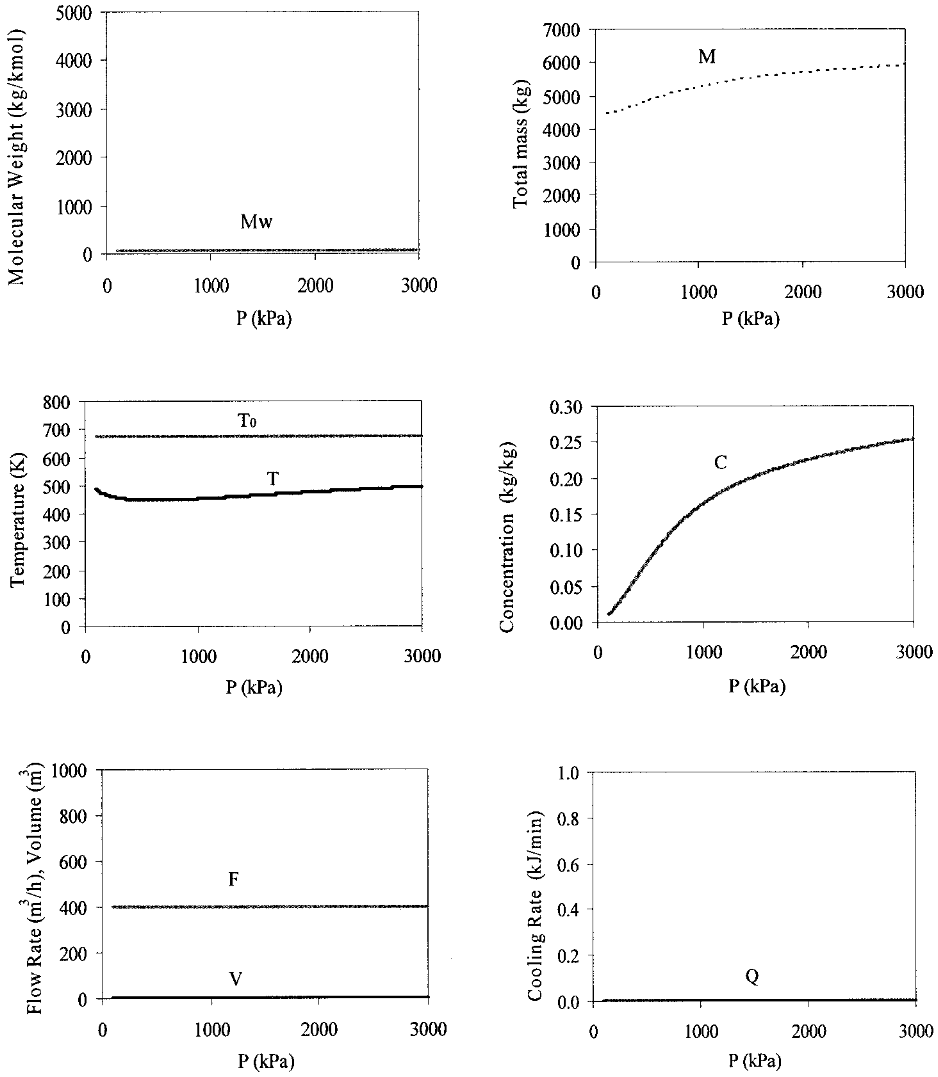

Figure 3. System profiles for disaster scenario (Example 2, 1,000 subregions).

Table 8. Nonlinear Contribution Matrix (100 Subregions) for Example 2

	F	V	T_0	Q	M	C	T	Mw
F	0.000	0.773	0.057	1.878	−0.446	0.689	0	−0.382
V	0.773	0.000	0.847	0.732	−1.796	7.767	0	−0.467
T_0	0.057	0.847	0.000	2.032	−0.193	2.470	0	−0.143
Q	1.878	0.732	2.032	0.000	−0.104	1.268	0	−0.067
M	−0.446	−1.796	−0.193	−0.104	0.000	1.632	0	0.185
C	0.689	7.767	2.470	1.268	1.632	0.000	0	1.903
T	0	0	0	0	0	0	0	0
Mw	−0.382	−0.467	−0.143	−0.067	0.185	1.903	0	0.000

detect such a shortcoming through the use of significance values. As a comparison, when the maximum safety discharge (V) is set as 30 kg/min, the significance obtained using this value is 0.045, which is negligible compared to its current significance of 5.333. Also note that because temperature (T) has infinite significance, no combined effects can be calculated for any pair involving the temperature. Feed temperature and flow rate also have some significant entries, obviously as a result of the fact that the feed can be used to introduce some additional heat into the system.

In summary, the process demonstrates a mild vulnerability to security attacks. It has been shown that a disaster situation will not arise unless the temperature goes beyond the normal operation conditions. Also, it has been observed that such an attack will be effective only with low molecular weights in the system, which means early in the operation. The analysis confirms that the bursting disc, if operable, would prevent the occurrence of a disaster situation. Therefore, the basic result obtained is that a security threat to this system would have to involve blocking the discharge, and probably require introducing heat into the system by additional means.

For this system, it is recommended that robust temperature monitoring is operative, and an emergency temperature control system (that is, a secondary heat sink) is installed on the process. A secondary pressure relief valve would also increase the odds of preventing a possible disaster condition. The system temperature and the bursting disc operability are critical and should be monitored at all times against the possibility of a process security threat.

Discussions and Conclusions

This work has introduced a theory for fast and comprehensive process security analysis and assessment. The methodology developed using the theory introduced enables a rapid evaluation of a confidence interval on the minimum time to disaster and, further, an identification of the sources that can lead to disaster. These evaluations produce a quantitative assessment of the impact of each variable and, consequently, create an ordered list of actions to take in a disaster situation. As demonstrated in the examples, the suggested assessment method can be applied to different systems (that is, continuous or batch processes) with ease.

A significant component in the methodology introduced is the *security limit time.* This measure is mathematically proven to be an upper bound for the minimum time the process can go to disaster situations, provided a synergy condition is satisfied. As demonstrated earlier in the case studies, *security limit time* produces reasonably tight upper limits for the actual time to disaster. Combined with the *process critical time* that is a proven lower bound, the *security limit time* measure enables estimation of a guaranteed interval for the actual worst-case scenario, thus allowing a reliable process security assessment for a system.

Also, the *priority list* introduced allows a quantitative comparison of the effect of all variables, in terms of significance to process security, on the system in disaster conditions. This will also help develop security monitoring and counterattack measures. To complement the *priority list*, a *nonlinear contribution matrix* (NCM) was introduced. This matrix consists of nonlinear effects of the combined change of any two variables on the system. This additional information allows much more accurate assessment of the security vulnerabilities, given that any nonlinear effects not evaluated in the *priority list* can be captured by the NCM.

To use the introduced tools and measures, a three-step security vulnerability assessment procedure was suggested. This procedure provides a comprehensive analysis of a system in terms of process security, as well as providing a pathway for designing process security enhancement systems. Although an industrially usable interface is not available at this time, the systematic procedure introduced here presents a complete foundation, and the development of such a tool is merely a technicality. To this end, a prototype security assessment software, based on the examples presented in this work, is being developed (Piluso et al., 2003).

Because of the ease of use and low computational requirements, the developments introduced in this work are particularly attractive in assessing the security vulnerability at the plant level. Because mathematically proven upper and lower bounds are evaluated, a reliable process security assessment can be accomplished. The γ-analysis technique enables replacing extensive simulation studies, which are extremely time consuming and typically not reliable because of the limitations of the commercially available simulators in modeling security threat scenarios, with a quick and reliable security assessment methodology.

One bottleneck still remaining is the estimation of the actual minimum time to disaster. Although this study has introduced a method for evaluating a guaranteed confidence interval, a quick, reliable, and *accurate* estimate is yet to be developed. The γ-analysis method is a promising framework in terms of its simplicity and low computational requirements, and it can be used in development of a method for reducing the gap between the *process critical time* and the *security limit time*.

The low computational requirements also render the γ-analysis method an ideal method for analysis of distributed-parameter systems, which is typically encountered in detailed analysis of security-sensitive equipment. Tackling the spatial variations of the critical variable is the problem that needs to be solved for applications to distributed-parameter systems.

Acknowledgments

This work is in part supported by the National Science Foundation under Grants CTS-0211163 and CCLI-0127307. The authors also acknowledge valuable suggestions and comments on the work from Prof. W. D. Seider of University of Pennsylvania.

Literature Cited

Allen, D. T., and D. R. Shonnard, *Green Engineering: Environmentally Conscious Design of Chemical Processes*, Prentice-Hall, Upper Saddle River, NJ (2002).

Brooke, A., D. Kendrick, A. Meeraus, and R. Raman, *GAMS: A User's Guide*, Scientific Press, Palo Alto, CA (1998).

Center for Chemical Process Safety (CCPS), *Guidelines for Hazard Evaluation Procedures*, AIChE, New York (1992).

Center for Chemical Process Safety (CCPS), *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, AIChE, New York (2002).

Crowl, D. A., and J. F. Louvar, *Chemical Process Safety: Fundamentals with Applications*, 2nd Edition, Prentice-Hall, Upper Saddle River, NJ (2002).

Cunningham, S., "What Can the Industrial Chemical Community Contribute to the Nation's Security," Paper presented at the Workshop on National Security and Homeland Defense: Challenge for the Chemical Science in the 21st Century, National Academies of Sciences and Engineering, Irvine, CA, January 14–16 (2002).

Dimitriadis, V. D., J. Hackenberg, N. Shah, and C. C. Pantelides, "A Case Study in Hybrid Process Safety Verification," *Comput. Chem. Eng.*, **20**, s503 (1996).

Dowell, A. M., III, "Layer of Protection Analysis for Determining Safety Integrity Level," *ISA Trans.*, **37**(2), 155 (1998).

Edwards, D. W., and D. Lawrence, "Assessing the Inherent Safety of Chemical Process Routes: Is There a Relation between Plant Costs and Inherent Safety?" *Trans. IChemE*, **71**(B), 252 (1993).

Heikkila, A. M., M. Hurme, and M. Jarvelaien, "Safety Considerations in Process Synthesis," *Comput. Chem. Eng.*, **20**, s115 (1996).

Hendershot, D. C., "Designing for Safety in the Chemical Process Industry: Inherently Safer Design," Paper presented at Accident Precursors Workshop: Linking Risk Assessment with Risk Management, July 17–18, 2003, National Academy of Engineering, Washington, DC (2003).

Ingham, J., I. J. Dunn, E. Heinzle, and J. E. Prenosil, *Chemical Engineering Dynamics*, 2nd Edition, Wiley-VCH, Weinheim, Germany (2000).

Kneale, M., and G. M. Forster, "An Emergency Condensing System for a Large Propylene Oxidation Reactor," *IChemE Symp. Ser.*, **25**, 98 (1968).

Lees, F. P., *Loss Prevention in the Process Industries*, 2nd Edition, Butterworths, London, UK (1996).

Lou, H. H., R. Muthusamy, and Y. L. Huang, "Process Security Assessment: Operational Space Classification and Process Security Index," *Trans. IChemE Part B: Process Safety & Environ. Protect.*, **81**(6), 418 (2003).

Luyben, W., *Process Modeling, Simulation and Control for Chemical Engineers*, 2nd Edition, McGraw-Hill, New York (1990).

Margiloff, I. B., "Geopolitics and Chemical Engineering," *Chem. Eng. Prog.*, **97**(12), 7 (2001).

National Institute of Justice (NIJ), *Chemical Facility Vulnerability Assessment Methodology*, U.S. Department of Justice, Washington, DC, November (2002).

Palaniappan, C., R. Srinivasan, and I. Halim, "A Material-Centric Methodology for Developing Inherently Safer Environmentally Benign Processes," *Comput. Chem. Eng.*, **26**, 757 (2002).

Piluso, C., K. Uygun, and Y. L. Huang, "Development of a Process Security Assessment Toolbox for Chemical Reaction Systems," Paper presented at The AIChE Annual National Meeting, San Francisco, CA, November 16–21 (2003).

Ragan, P. T., M. E. Kiburn, S. H. Roberts, and N. A. Kimmerle, "Chemical Plant Safety: Applying the Tools of the Trade to a New Risk," *Chem. Eng. Prog.*, **98**(2), 62 (2002).

Shacham, M., N. Brauner, and M. B. Cutlip, "Open Architecture Modeling and Simulation in Process Hazard Assessment," *Comput. Chem. Eng.*, **24**(2–7), 415 (2000).

U.S. General Accounting Office (U.S. GAO), *Homeland Security, Voluntary Initiatives are Under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*, Report to Congressional Requesters, Washington, DC, March (2003).

Uygun, K., H. H. Lou, and Y. L. Huang, "Process Security Analysis: γ-Analysis and Σ-Maps," *AIChE J.*, **49**(9), 2445 (2003).

Manuscript received Jul. 14, 2003, and revision received Feb. 15, 2004.