Process Security Analysis: γ-Analysis and Σ-Map

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 77710

Chemical processes are often operated under high pressures, at high temperatures, and with fast material flows and complex manufacturing mechanisms. Thus, their operation is always more risky, environmentally more harmful, and potentially more dangerous than other types of manufacturing activities when abnormal or destructive situations arise. In the extreme, catastrophes, such as explosions, toxic release, and loss of life, will occur unexpectedly and rapidly, particularly when a premeditated attack is made by an adversary who has sufficient technical background on chemical operations. Obviously, such security-threatening situations must be detected early, the potential impacts on production must be precisely evaluated, and operational solutions must be quickly derived. However, systematic and effective methodologies are not available for the chemical process industries today. Scientists and engineers are greatly challenged to swiftly develop a knowledge base of process security that can fundamentally help the industry perform process-security analysis, assessment, and improvement (Margiloff, 2001; Cunningham, 2002; Ragan et al., 2002).

Process security is an extended concept and practice of process safety. Over the past decades, various process-safety techniques and tools have been developed and implemented in the industries. HAZOP (HAZard and OPerability analysis), LOPA (Layer Of Protection Analysis), and FTA (Fault Tree Analysis) are among the most popular ones (Dimitriadis et al., 1996; Lees, 1996; Allen and Shonnard, 2002; Crowl and Louvar, 2002). They are effective in identifying process malfunctions and deriving solutions to ensure safe production. The scientific tools for safety enhancement are mainly probability analysis and logical reasoning about the root causes of adverse conditions. Existing safety technologies are almost exclusively based on steady-state information. Solutions generally are derived on experience, and they are usually statistical and qualitative (Dimitriadis et al., 1996; Dowell, 1998).

Correspondence concerning this article should be addressed to Y. L. Huang.

Different from process safety that follows likelihood, process security concerns adverse events caused by factors of harmful intentions. The occurrence of a process-security problem is a possible but not a probable situation. Therefore, the solution to this type of problem cannot rely on probability. To avoid any severe consequence, a fast and accurate assessment and a timely and effective action are the must-have requirements. Their effectiveness depends upon the fundamental understanding of process behavior, particularly process dynamics, beyond the normal operation zone.

Operation Zone Classification

A process may display very different types of behavior in the operation zones. Lou et al. (2003) note that most of the available process models characterize normal operations; hence, their suitability for characterizing system behavior in abnormal regions should be carefully verified. Based on this argument, they suggest partitioning the process input and output spaces into four major zones: (1) Zone I—the normal operation zone; (2) Zone II—the security-alerting zone where a security-sensitive process change must be dealt with; (3) Zone III—the security-threatening zone where an effective security-assurance action must be taken immediately; and (4) Zone IV—the security-disaster zone where the changes are irreversible and a severe consequence results. Figure 1 depicts the operation zone classification for a general process. For simplicity in discussion, the union of Zones I, II, and III is denoted as the security space throughout this work.

The mapping of both the input and output spaces can be crucial in process security analysis. Output-based security monitoring provides a feedback security control, while input-based monitoring enables feedforward measures, therefore, it is highly desirable to have the input space mapping of the security zones. The output security zones can be relatively easily mapped, since they are usually based on equipment limits; however, the exact mapping of the input space is prob-

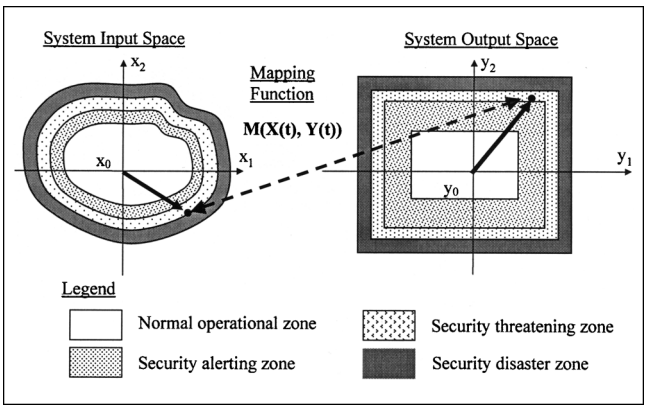

Figure 1. Space mapping of inputs and outputs: a 2-D example.

lematic. Note that a process security model can be a mapping function between the input and output spaces, but the construction of the zone borders, especially in a multidimensional case, requires excessive system simulations.

Process-Security Analysis

A fundamental basis for process-security analysis is the characterization of process behavior in the entire security space. This characterization requires a modeling effort beyond the normal practice.

Process-security model

Consider a general process-security model that can describe a process in all operation zones (Zones I, II, and III) before entering the security-disaster zone (Zone IV)

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

where y is the vector of output variables, u is the vector of manipulated variables, d is the vector of disturbances.

It is possible to use either a single model for the entire security space, or a group of models, each of which is valid for an individual operational zone. This does not affect the applicability of the analysis method. For the sake of simplicity, the discussion is focused on a multiple-input, single-output system. However, the method described below is applicable to more complex systems. Minor necessary modifications to achieve that will be discussed later in the text.

γ-Analysis

A mathematical framework for process-security study introduced here is with the assumption that a process-security model is available. The principal idea in γ-analysis is to investigate the gradient of system dynamic equations (the time derivatives) directly, rather than going through the integration process, which is a time consuming task. However, a mathematical description of process security should be introduced first.

Definition 1. Process security, in the context of this work, is defined as the ability of the system to retain a secure operation when suffering subtle attacks. The attacks are mathematically represented as disturbances ($\boldsymbol{d}$) and crippled control and safety systems ($\boldsymbol{u}$) in the process-security model.

A security threat is an event that can lead to a disaster if no effective countermeasure is taken, typically happening in an interval of minutes or seconds. Brute-force attacks, such as bombing and hostile takeover, are within the scope of the existing security methods for infrastructure enhancement (Ashcroft et al., 2001). In this work, process security is mathematically defined as

$$\text{A process is secure if } \tau \geq \tau^{\min} \tag{2}$$

where τ is the minimum time required by the process to move from the nominal operation point (in Zone I) to the security disaster zone (Zone IV); and $\tau^{\min}$ is the time needed for detecting the threat, making decisions, and taking necessary countermeasures to eliminate the threat. The length of this time lag between the occurrence and the resolution is determined by a number of factors, including the nature of the process, equipment, and personnel, among others. Note that having a zero $\tau^{\min}$ would make all processes secure by default. Therefore, a nonzero requirement is imposed.

Remark 1. The reference point for defining the minimum time, τ, is the nominal operation point, y_0. Therefore, τ is independent of the current status of the process

$$\tau \neq \tau(t) \tag{3}$$

The minimum time needed for moving to the disaster zone from a different reference point, $y(t)$, is defined as

$$\tau^{\text{opr}} = \tau^{\text{opr}}(y(t),u(t),t) \tag{4}$$

It is worth noting that both τ and τ^{opr} are the functions of process structure. Thus, alternative designs under the same security threat may have different τ and τ^{opr} values, in general.

Remark 2. The evaluation of the exact values of τ or τ^{opr} requires extensive dynamic simulations for searching all possible threat profiles.

Definition 2. The maximum speed of a process moving from the nominal operating point (y_0 in Zone I) to the security disaster zone (Zone IV) is denoted as Γ. It has the following form

$$\Gamma = \frac{|y_{IV} - y_0|}{\tau^{\min}} \tag{5}$$

Note that Γ is finite, since $\tau^{\min}$ is nonzero by definition. Rearranging the preceding equations gives

$$\tau^{\min} = \frac{|y_{IV} - y_0|}{\Gamma} \tag{6}$$

The Security Theorem. Let

$$\gamma = \max_{y,u,d,t} f(y,u,d,t) \tag{7}$$

$$\text{s.t.} \quad y,u,d,t \in [\text{physical limits}] \tag{8}$$

Then

$$\text{the process is secure if } \gamma \leq \Gamma. \tag{9}$$

Before proving the theorem, the concept of process critical time is introduced below.

Definition 3. The process critical time, ω, as the worst-case estimate of τ, is defined as

$$\omega = \frac{|\, y_{IV} - y_0 \,|}{\gamma} \tag{10}$$

Note that *dy/dt* is the speed the system moves from one state to the other. Since *dy/dt* cannot exceed γ, the system cannot move from the nominal point (y_0) to Zone IV more quickly than ω.

Remark 3. ω is an underestimate of the actual time to disaster (τ), that is, $\tau \geq \omega$, provided the maximization problem is solved to globality.

Remark 4. ω is a process constant; it is determined by the process limits and inherent process behavior. A nonconstant estimate of the time to Zone IV for on-line security evaluation will also be formulated later.

Proof of Theorem. If $\gamma \leq \Gamma$, combining Eqs. 6 and 10 yields

$$\omega \geq \tau^{\min} \tag{11}$$

Also, from Remark 3, we have

$$\tau \geq \omega \tag{12}$$

Combining Eqs. 11 and 12 gives

$$\tau \geq \omega \geq \tau^{\min} \tag{13}$$

and, therefore

$$\tau \geq \tau^{\min} \tag{14}$$

Thus, by Definition 1, the process is secure.

Remark 5. γ is defined as the maximum of the time derivative function, since usually security-threatening events occur at high temperatures and pressures. For other cases, where a low value is problematic, or both high and low values are problematic, the following alternative formulations can be utilized, such as

$$\gamma = |\min_{y,u,d,t} f(y,u,d,t)| \tag{15}$$

or

$$\gamma^2 = \max_{y,u,d,t} [f(y,u,d,t)]^2 \tag{16}$$

Remark 6. In the Security Theorem, the constraints in Eq. 8 are critical in defining process-security boundaries. Thus, they should be determined carefully and precisely. Most functions can be driven to divergence (that is, to $\pm\infty$) if the variables are allowed to, but this behavior does not contain any information related to process security. It is important to observe whether the process can be rendered disastrous through physically possible interventions. Therefore, all variables should be physically limited. For instance, the feedstream flow rate cannot exceed what the pipes can handle. The system behavior in the security space is of particular importance; beyond that, the process will be in Zone IV, which is in an unrecoverable situation. A process-security model is not expected to remain meaningful for Zone IV.

Definition 4. The minimum time for the system to reach y_{IV} (Zone IV) from the current operating point, $y(t)$ in Zones I, II, or III, is named the process operational security time, ω^{opr} , which is defined as

$$\omega^{\mathrm{opr}}(t) = \frac{|\, y_{IV} - y(t)}{\gamma} \tag{17}$$

Remark 7. ω^{opr} is a worst-case estimate of how fast the process can move from the current operating point to the disaster zone; therefore, it is a time-dependent measure.

Remark 8. ω^{opr} is a worst-case estimate for the security-action available time, as defined by Lou et al. (2003).

Definition 5. The recovery time of the system from the current operating point, $y(t)$, to the nominal operating point, y_0, is estimated by

$$\omega^{\mathrm{rec}}(t) = \frac{|\, y_0 - y(t)\,|}{\gamma} \tag{18}$$

Remark 9. ω^{rec} is an optimistic estimate for the actual recovery time, τ^{rec}, that is, $\tau^{\mathrm{rec}} \geq \omega^{\mathrm{rec}}$.

Enhancing accuracy

ω and ω^{opr} are the worst-case estimates to the actual time to the disaster for a process. However, the ease of the calculation comes at the cost of the accuracy. The accuracy of the predictions can be enhanced easily when necessity arises. The principal idea is to divide the output zone into multiple regions in a grid, and to evaluate separate values of γ^j and ω^j, where superscript j denotes the index for each of these smaller intervals. Then, the process critical time, ω, will simply be the sum of regional critical times over the index j. As the number of regions increase, the accuracy will also increase. At the limit, for a single-output system, ω becomes an exact estimate of τ, but at the cost of solving an infinite number of optimization problems. The issues of optimal decision for the number of regions and grid placement will not be addressed here, although the similarity between this approach and numerical discretization and integration techniques should be underlined.

General systems

The analysis outlined earlier can be applied to the systems of higher complexity. Prior to the description of the method, significantly security-sensitive variables should be distinguished from others when a multiple-input multiple-output (MIMO) process is considered.

Definition 6. A critical variable is a process output that is used directly to define Zone IV. In chemical processes, temperature and pressure are the usual critical variables.

Multiple Outputs. For a process with multiple output variables, one γ should be defined for each critical output, that

is

$$\gamma_i = \max_{y,u,d,t} f_i(y,u,d,t) \tag{19}$$

Each γ_i is the maximum speed the system can have along the direction of the ith critical variable. Accordingly, the process critical time, ω_i, for the variable, y_i, can be defined as

$$\omega_i = \frac{|\, y_{IV,i} - y_{0,i} \,|}{\gamma_i} \tag{20}$$

In this case, the process critical time for the entire system is

$$\omega = \min_i \omega_i \tag{21}$$

Remark 10. The process critical time estimated by Eq. 21 is an underestimate, even if an infinite number of regions is used, since it assumes a system moving along a single output direction without any movement along others. Note that the system can move along different directions simultaneously, unless the outputs are completely decoupled. This movement along other directions will take some additional time for the system to reach Zone IV. Thus, the estimated time is less than the actual time to a disaster. The Σ-maps, which are to be introduced in the following section, can be used to identify the interdependencies among the output variables explicitly. Also note that Eq. 20 is defined based on the assumption that the security limits for the critical variables are not correlated, that is, Zone IV is defined by a hyperrectangle.

Differential-Algebraic Systems. In general, a system will have a multitude of state variables ($\boldsymbol{x}$) as well as output variables ($\boldsymbol{y}$). A general MIMO system can therefore be formulated as

$$\frac{d\boldsymbol{x}}{dt} = \boldsymbol{f}(\boldsymbol{x},\boldsymbol{u},\boldsymbol{d},t) \tag{22}$$

$$\boldsymbol{h}(\boldsymbol{x},\boldsymbol{u},\boldsymbol{d},t) = \boldsymbol{0} \tag{23}$$

$$\boldsymbol{y} = \boldsymbol{g}(\boldsymbol{x}) \tag{24}$$

where $\boldsymbol{h}$ is the vector defining the relationships used in the differential equations, typically correlations for parameter estimation; $\boldsymbol{g}$ is the vector relating the state variables ($\boldsymbol{x}$) to the output variables ($\boldsymbol{y}$). In this case, a γ-analysis problem can be expressed as

$$\gamma_i = \max_{x,u,d,t} \left(\frac{dg_i(\boldsymbol{x})}{d\boldsymbol{x}} \cdot \boldsymbol{f}(\boldsymbol{x},\boldsymbol{u},\boldsymbol{d},t) \right) \quad i = 1,2,\ldots \tag{25}$$

$$\text{s.t.} \quad \boldsymbol{h}(\boldsymbol{x},\boldsymbol{u},\boldsymbol{d},t) = \boldsymbol{0} \tag{26}$$

$$\boldsymbol{x},\boldsymbol{u},\boldsymbol{d},t \in [\text{physical limits}] \tag{27}$$

Note that this is a constrained optimization problem.

Remark 11. The proposed analysis method is applicable to general dynamic systems, therefore naturally including linear systems. Furthermore, due to the linearity property, linear systems have their maximum rate of changes at a combination of the maximum/minimum bounds of variables, which simplifies the optimization task. However, it should be noted that it is unlikely for a single linear model to describe a process over the entire security space. Using multiple linear models is possible, but unless the system displays extreme nonlinearity, the inherent error that comes with such approximation schemes is not justified.

Remark 12. In the development of the γ-analysis, it is assumed that all control/safety systems are either off-line or act as disturbances in a manner that affects the system adversely, rather than their expected regulative effects. However, it could be useful to run what-if scenarios considering some of these regulatory systems being on-line, especially for the design of safety systems. It is quite possible to account for the response of such systems in the estimation of process critical time, due to the use of optimization as the basis of the γ-analysis. Detailed descriptions will not be presented here, but in summary, the only necessary modification is to include the effect of these control/safety systems as additional constraints in the optimization. For instance, a P-only controller could be included in the following manner

$$\gamma = \max_{y,u,d,t} f(y,u,d,t) \tag{28}$$

$$\text{s.t.} \quad y,u,d,t \in [\text{physical limits}] \tag{29}$$

$$u = u^0 + K(x - x^{\text{set}}) \tag{30}$$

This would result in the calculation of process critical time when a controller is working. Safety systems could be included in a variety of ways, such as additional bounds on variables or on/off controllers. The only difficulty would be encountered when the control action cannot be expressed analytically (such as model predictive control systems). In such cases, an explicit control law that approximates the actual control response should be used.

Due to the ease of use and computational speed of γ-analysis, a large number of what-if scenarios could be run very quickly and be used in the design of safety/security systems, as well as an on-line situation assessment.

Σ-Map

While the γ-analysis establishes a rate-of-change-based measure of process security, a more thorough inspection over the entire security space is also highly desirable. In this regard, the process security map, or simply Σ-map, is introduced. The basic idea is to reveal the rates of change (dy/dt) of critical variables over the entire operation zones. The Σ-map illustrates the relationship between dy/dt and two-system variables in a 3-D surface plot form: the function dy/dt (variable 1, variable 2) is plotted over a range of the system variables of interest. The remaining system variables are fixed at the values that maximize dy/dt; thus, the Σ-map illustrates the value of γ vs. varying system variables. This serves as a tool to visualize the system behavior, as it will be exemplified in the case study that is investigated in the next section.

It should also be noted that the mapping between the input and output spaces is crucial in process-security analysis, but difficult to establish. Given the output space, the input space should be mapped to identify different security zones (Lou et al., 2003). Σ-Maps produce an estimate of the space

Table 1. Variable Ranges and Parameters

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_{A_0}) (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_{J_0}) = 294.44 K		C_p = 3.14 kJ/ kg K	
E = 69,780 kJ/ kmol		ρ = 800.95 kg/m^3	
U = 3,066.3 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	
α = 7.08 10^{10} h^{-1}			

mapping for the inputs automatically. It is possible to observe the regions where the rates of change in output variables are low, moderate, or high, and classify the mapping of both spaces accordingly. However, this method will relate the changes of outputs to inputs, rather than outputs to inputs.

Case Study: Nonisothermal CSTR

Figure 2 depicts a jacketed CSTR system where an exothermic reaction takes place. The original case (Luyben, 1990) is slightly modified to render the example more interesting for security analysis. The system model is given below

$$\frac{dV}{dt} = F_0 - F \tag{31}$$

$$\frac{dV_J}{dt} = F_J^{\mathrm{IN}} - F_J^{\mathrm{OUT}} \tag{32}$$

$$V\frac{dC_A}{dt} + C_A\frac{dV}{dt} = F_0C_{A0} - FC_A - VkC_A \tag{33}$$

$$V\frac{dT}{dt} + T\frac{dV}{dt} = F_0T_0 - FT - \frac{\lambda VkC_A}{\rho C_p} - \frac{UA_H}{\rho C_p}(T - T_J) \tag{34}$$

$$V_J\frac{dT_J}{dt} + T_J\frac{dV_J}{dt} = F_J^{IN}T_{J0} - F_J^{OUT}T_J + \frac{UA_H}{\rho_J C_J}(T - T_J) \tag{35}$$

where

$$k = \alpha e^{-E/RT} \tag{36}$$

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 process security zone, that is, Zones I through III. For the process-security analysis, the feedback-control system is considered to be crippled. The critical output variable is the temperature in the reactor (T), as it is the primary security threat in a possible runaway reaction. The results of γ-analysis, performed in GAMS with different numbers of regions, is displayed in Table 2. The ω value converges toward a value slightly less than 2 s as the number of regions increase. This analysis indicates that the reactor temperature can reach disaster zones very rapidly.

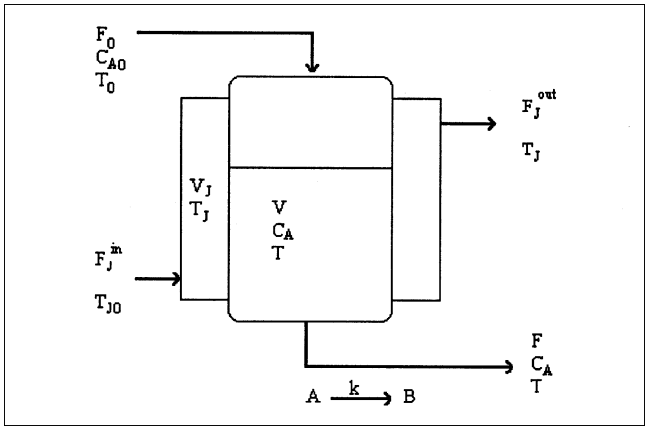

Figure 2. Nonisothermal CSTR with a cooling jacket.

The Σ-maps for the reactor temperature rate of change (dT/dt) as a function of system variables are depicted in Figure 3. The Σ-maps reveal the exponential dependence of rate of change of temperature on the reactor temperature (Figures 3a and 3c), which indicates a runaway reaction, as expected from the small ω value. The volume of liquid in the reactor has a negligible effect compared to the temperature and reactant concentration as it can be observed in Figures

Table 2. Process Critical Time Evaluation for the Case Study

No. of Regions	ω (s)
1	0.09
2	1.11
5	1.40
10	1.53
20	1.63

3c and 3d, and coolant temperature and feed temperature are also insignificant compared to the reactor temperature as illustrated in Figures 3e and 3f.

An interesting observation is that around the runaway point, the rate of change of temperature is not affected by the inputs F and F_0 at all (Figure 3b). The reason is that at the maximum point, $T = T_0 = 555.56$ K, and as it can be traced in Eqs. 31 and 35, when input and reactor temperatures are equal, the flow terms cancel each other. Naturally, the flow rates will have an indirect effect through volume of liquid in reactor (see Eq. 31), but as already discussed, variable V itself is not significant on the temperature rate of change at high temperatures.

The two variables of interest, therefore, are the reactant concentration and reactor temperature, which both have significant effects as depicted in Figure 3a. However, Figure 3a also illustrates that the rate of change can be a significant percentage of its maximum, even around the nominal point

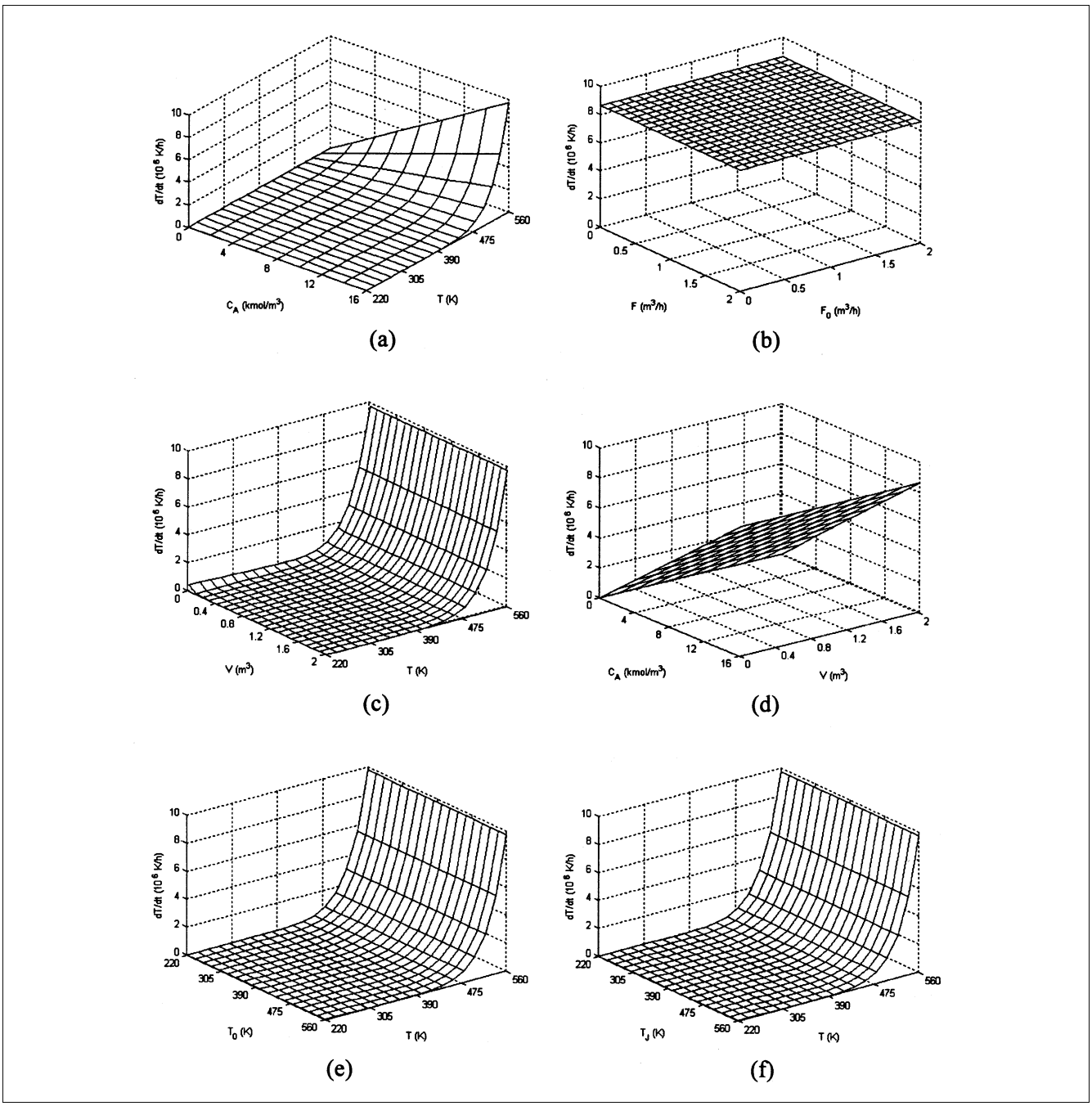

Figure 3. Process security maps of the rate of change of reactor temperature with different system variables.

(a) Reactant concentration and reactor temperature, (b) reactor flow in and flow out, (c) liquid volume in reactor and reactor temperature, (d) reactant concentration and volume of liquid in reactor, e) inlet temperature and reactor temperature, (f) reactor temperature and coolant temperature.

of concentration ($dT/dt \approx 2\times10^6$ K/h at $C_A = 3.92$ kmol/m^3) at sufficiently high temperatures. Therefore, the runaway reaction can occur without a change in the reactant concentration; hence, C_A is not a limiting factor. A low concentration will increase the time to disaster (approximately four times its original value, if concentration is fixed to the nominal point), but this does not change the original conclusion from the γ-analysis that a runaway reaction can occur rapidly. Rather, the Σ-maps validate our conclusion; the system has a serious security vulnerability.

To further illustrate the use of the developed tools, an "on-line" process security assessment is conducted. Let's consider the situation when T is 513.3 K. Using the pre-calculated γ values (20 regions), we can obtain

$$\omega^{\text{opr}} = 0.982 \text{ s}$$

This leads to the conclusion that the process is only 0.982 s away from a disaster. The process recovery time can also be evaluated as

$$\omega^{\text{rec}} = \frac{|513.3 - 333.3|}{\gamma} = 0.651 \text{ s}$$

This result indicates that the system will not have recovered to the nominal operation before 0.651 s. Note that the pre-calculated γ values are utilized; hence, the calculation of ω^{opr} and ω^{rec} can be performed very quickly, without need for additional optimizations.

Discussion and Conclusions

This work has introduced a number of tools and decision criteria for process-security analysis. As demonstrated in the case study, these tools can be used in tandem to identify possible process-security problems, to analyze correlations between critical process inputs and security-sensitive outputs, and to find the principal factors leading to the security-threatening possibilities.

γ-Analysis, constituted of the security theorem and first three definitions, presents a method for quickly evaluating process security for any given system. The need for deriving analytical or numerical solutions to the system differential equations is circumvented by the direct use of the time derivative functions. The optimization scheme for evaluating γ enables screening for all possible combinations of disturbances and manipulated variable changes without the need for extensive trial-and-error procedures with simulations. The process critical time, ω, is a process constant that gives a quantitative measure for system security; it is easy to understand, evaluate, and compare with the requirements. These measures can also be implemented within a process design algorithm for improved process security.

The Σ-maps are a visual tool to analyze the system and to deduce additional information about the process and its likely exposure to security threats, as exemplified in the case study. Contrary to the γ-analysis, which is numerical and can be automated readily, the Σ-maps present a human-oriented tool for the study of existing industrial cases, or use in developing secure processes, by engineers. The major focus of future work should be extracting the information deducible from the Σ-maps via purely computational methods.

Due to the ease of use, the developments introduced in this work are particularly attractive in assessing the security vulnerability at the plant level, such as in chemical plants or refineries. However, in certain multidimensional cases, the method can lead to low process-critical time estimations. Therefore, the process-security prediction accuracy should be monitored closely through the use of Σ-maps. Several methods for accuracy improvement and error estimation are currently under development.

Acknowledgment

This work is supported in part by the National Science Foundation under Grants CTS-0211163 and CCLI-0127307.

Literature Cited

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

Ashcroft, J., D. J. Daniels, and S. V. Hart, *Chemical Facility Vulnerability Assessment Methodology*, U.S. Department of Justice, Washington, DC (2001); http://www.ojp.usdoj.gov.

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

Cunningham, S., "What Can the Industrial Chemical Community Contribute to the Nation's Security?," Workshop on National Security & Homeland Defense: Challenge for the Chemical Science in the 21st Century, National Academies of Sciences and Engineering, Irvine, CA (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).

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

Lou, H. H., R. Muthusamy, and Y. L. Huang, "Process Security Assessment: Operational Space Classification and Process Security Index," in press, *Trans I.ChemE* (2003).

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

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

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).

Manuscript received Nov. 27, 2002, and revision received Feb. 12, 2003.