DESIGN FOR PROCESS SECURITY

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

Helen Lou
Department of Chemical Engineering, Lamar University
Beaumont, TX 77706

Abstract

Chemical process security has been an area of interest due to the potential of process industries as a possible terrorism target. As a result, model-based process security analysis methods that try to detect process vulnerabilities in a fundamental way have been proposed. The design aspect of the problem, however, has not been addressed yet. In this work, an adverse-MPC approach, which enables estimation of security vulnerability for a given process is proposed, and is coupled by a secure-design problem that retrofits the design to minimize the vulnerability. The proposed method is realized using a bi-level formulation, where the security evaluation is posed as a constraint in the outer design problem. The method described in this work enables design of processes that are inherently less vulnerable to security threats. Further, the method can be extended to combine economics into the security problem, hence enabling design of optimal designs in terms of both security and cost efficiency. The algorithm can also be utilized for design of robust security systems. The application potential of the approach is demonstrated by a runaway reactor example.

Keywords

Process Security, Process Design, Adverse Control, Model Predictive Control

Introduction

The security in chemical industries has been an issue of rising interests, as chemical processes often feature high toxic and/or flammable materials, high-pressure equipment, and highly exothermic reactions. The inherent nature of these processes renders them operationally more risky, environmentally more harmful, and potentially more vulnerable compared to other industries when abnormal or destructive situations arise. In the extreme cases, toxic release and loss of life may occur unexpectedly and rapidly, particularly when a premeditated attack is made by an adversary who has sufficient technical background on chemical process operation. Obviously, such vulnerabilities have to be identified and addressed (Margiloff, 2001; Cunningham, 2002; Ragan *et al*., 2002).

* Corresponding author; Tel: 313-577-3771; Fax: 313-577-3810; E-mail: yhuang@wayne.edu)

Chemical plant security can be categorized into three major items: physical security, cyber security, and process security. Physical and cyber security can be assured through improving plant infrastructure and thus are technically relatively straightforward. In analysis of process security, however, the relationships between process operation and process security have to be quantified, which requires a fundamental understanding of the system. 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. Thus, the most challenging tasks for process security are: (a) to assess process

security, and (b) to improve process design to minimize vulnerability.

Recently, Lou *et al*. (2003) defined process security from the process operation point of view, and outlined the difference between process safety and process security. Very recently, Uygun *et al*. (2003) introduced a novel process security analysis method. The process security problem is formulated as a minimum-time dynamic optimization problem, and Pontryagin's minimum principle is employed to simplify the problem and transform it into a number of much simpler static optimization problems. This allows very quickly evaluating reasonably tight upper and lower bounds on for the minimum time that the process will go to disaster under a security threat (Minimum Time to Disaster-MTD); hence it is a justifiable engineering solution to the rather difficult problem of predicting how a saboteurs mind works. However, the exact value of MTD is not evaluated.

In this work, an Adverse Model Predictive Control (AMPC) method is introduced for prediction of the exact value of MTD (rather than an interval). The AMPC problem is then utilized in a bi-level dynamic retrofit design algorithm that enables design of secure processes.

Process Security Problem

To discuss process security, first let us examine how to define process security levels.

Definition 1 (Uygun *et al*., 2004). 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 referred to as *critical variables*. 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.

Accordingly, the mathematical definition of process security is given as:

$$\tau = \min_{\mathbf{d}(t)} \int_0^{\tau} dt \tag{1}$$

$$\text{s.t. } \frac{d\boldsymbol{y}}{dt} = \boldsymbol{f}(\boldsymbol{p}, \boldsymbol{y}, \boldsymbol{d}) \tag{2}$$

$$y(\tau) = y_{c,d} \tag{3}$$

where $\boldsymbol{y}$ is the vector of system variables, $\boldsymbol{d}$ is the vector of disturbances, and $\boldsymbol{p}$ is a constant vector of design parameters. Process security models (Eqn. 2) have different requirements that normal process models. They should be able to describe the system to the limit of disaster. Also, it should be noted that in a security-threatening situation, both manipulated variables and disturbances may be the causes of security threat; hence they are both included as disturbances. Uygun *et al*. (2004) further discuss that some state variables are also directly vulnerable to security threats and hence should be treated as disturbances as well.

Accordingly, process security is defined as follows:

Definition 2 (Uygun *et al.,* 2003)**.** A process is secure if:

$$\tau \geq \tau^r \tag{4}$$

where τ, named 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, named the *resolution time*, is the minimum time needed for detecting the threat, making decisions, and taking necessary countermeasures to eliminate the threat. While the exact value of resolution time depends on the process and is somewhat difficult to determine, any value above 15 minutes, as a rule of thumb, is acceptable and above an hour can be considered to be secure.

Adverse MPC

Equations (1-3) form a very familiar minimum-time problem. However, the system model is very likely to be nonlinear. Hence analytical solution of this problem is likely to be unobtainable. Here, we propose a nonlinear MPC approach for the solution of this problem. Basically, MPC can be expressed as the following control-vector parameterization:

$$\boldsymbol{d}(t) = \boldsymbol{d}\big|_k \qquad k = 1, \cdots, n \tag{5}$$

where n is the number of manipulated variable adjustments. Note that the parameterization may introduce a sub-optimality to the solution due to globality problems that may arise in nonlinear MPC. In this regard, AMPC should be used in tandem with the γ-analysis method (Uygun *et al.*, 2004), which produces a reliable confidence interval that can be used to validate the results of AMPC. In this work, the nonlinear MPC problem was solved via a sequential approach (Bequette, 1991) in MATLAB.

Design for Security

The AMPC approach described above enables the estimation of MTD. It is then possible to design a system such that MTD is maximized. The bi-level formulation that results for the secure-design problem is than given as:

$$\max_{\boldsymbol{p}} \ \tau(\boldsymbol{p}) \tag{6}$$

$$\text{s.t. } \tau(\boldsymbol{p}) = \min_{\boldsymbol{d}(t)} \int_0^{\tau} dt \tag{7}$$

$$\frac{d\boldsymbol{y}}{dt} = \boldsymbol{f}(\boldsymbol{p}, \boldsymbol{y}, \boldsymbol{d}) \tag{8}$$

$$y(\tau) = y_{c,d} \tag{9}$$

In the design problem above, Eqn. (6) is the objective function which is formulized here as maximization of MTD. For the general case, different objectives – including cost terms for instance- can be utilized.

The design problem given in Eqns. (6-9) is a bi-level dynamic optimization problem that is difficult to solve. Uygun and Huang (2002) developed an iterative linear-approximation approach that is similar to Sequential Linear Programming. It enables the solution of this type of problems in a more efficient way. However, application to large-scale problems may prove difficult. As such, we will limit our attention to retrofit problems in this work.

Example Case

Figure 1 depicts a jacketed CSTR system that is originally given by Luyben (1990), and also studied for process security by Uygun *et al*. (2003).

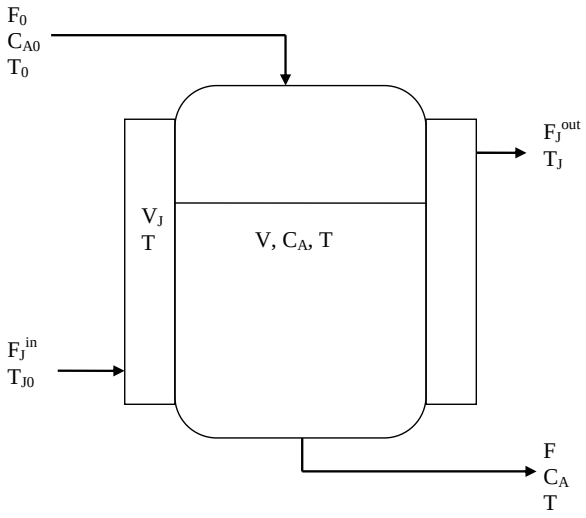

Figure 1. Sketch of a non-isothermal CSTR with a cooling jacket.

In this example, it is considered that the volumetric holdups and concentration can be manipulated from outside hence are considered as disturbance variables. Accordingly, the process security model is given below:

$$\frac{dT}{dt} = \frac{F_0}{V}(T_0 - T) - \frac{\lambda k C_A}{\rho C_P} - \frac{U A_H}{\rho C_P V}(T - T_J) \tag{10}$$

$$\frac{dT_J}{dt} = \frac{F_J^{IN}}{V_J}(T_{J0} - T_J) + \frac{U A_H}{\rho_J C_J V_J}(T - T_J) \tag{11}$$

where

$$k = A e^{-E/RT} \tag{12}$$

Table 1. Variable Ranges and Parameters.

Variable name	**Minimum**	**Nominal**	**Maximum**
Reactor feed (F_0) (m^3/h)	0	1.13	1.98
Reactor output (F) (m^3/h)	0	1.13	1.98
Jacket feed (F_J^{in}) (m^3/h)	0	1.41	2.83
Jacket output (F_J^{out}) (m^3/h)	0	1.41	2.83
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)	0.66	1.36	1.98
Coolant volume in jacket (V_J) (m^3)	0.07	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 = 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	
A=7.08 10^{10} h^{-1}			

The system parameters and variable ranges are listed in Table 1. It should be noted that the minimum values for reactor and jacket volumes are different compared to the values used by Uygun *et al*. (2003) to render the design problem more interesting. Since a 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. For the retrofit of system, three design parameters are considered as degrees if freedom: Heat exchanger design ($U \cdot A_H$) (between 30 times to 1/30 of the original value), coolant properties ($\rho_J \cdot C_J$) (50% to 200 % of the original), and reactor content properties ($\rho \cdot C_P$) (±20 %), which is assumed to be slightly variable by addition of an inert component or recycling some of the product.

Table 2. Retrofit Results.

	Original Design	**Retrofit Design**
τ	87.99	112.08
$U \cdot A_H$	71,230	2,136,904
$\rho \cdot C_P$	2,515.08	3,0181.09
$\rho_J \cdot C_J$	4,181.05	8,362.82

The results of retrofit design are displayed above in Table 2. Figure 2 depicts the temperature profile in the worst-case conditions for the original and retrofit designs.

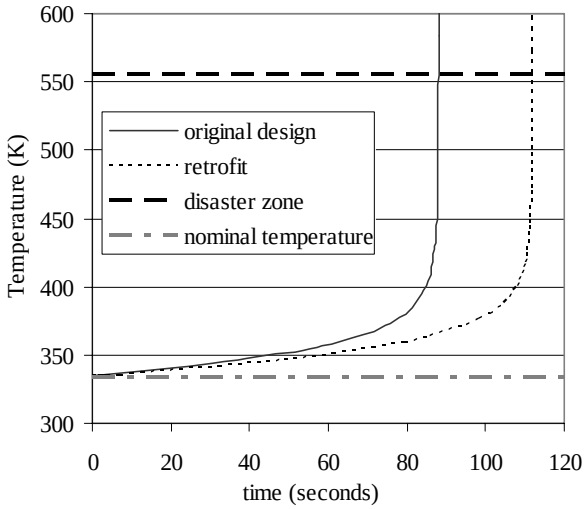

Figure 2. Temperature profiles.

The retrofit study increases the Minimum Time to Disaster for the process by 27 per cent. This improvement, however, is not nearly enough to render the process secure. For this example, the primary design factor is the heat exchanger; however, it does not have a significant effect on MTD. The coolant properties and reactor content density can only be modified to a limited extent. As such, the CSTR configuration does not seem to hold enough options to create a secure design. An alternative reactor configuration, such as a tubular reactor may be advised.

Conclusions

In this work, an adverse-MPC approach has been introduced for analysis of security vulnerability level of a given process. Further, the adverse control scheme has been employed in a design algorithm that enables design of secure processes. The example case studied demonstrates that retrofit of a given process is possible by this scheme, although the improvement in the example case has not been sufficient to render the problem secure.

The primary goal of this work is to emphasize that process security can be integrated as a goal in rigorous design algorithms. However, further development of both the adverse MPC idea and the design algorithm is necessary. Particularly promising is the adverse MPC subject: While it has been realized as a straightforward nonlinear MPC application in this work, minimum-time problems are known to lead to bang-bang controllers. If a non-iterative solution to the adverse control problem can be formulated, the design problem would be significantly simplified. This in turn would enable much larger secure-design problems, including superstructure methods with binary design decisions.

Acknowledgements

This work is in part supported by the National Science Foundation under Grants CTS-0211163, CCLI-0127307, and CTS-0407494.

References

Bequette, B.W. (1991). Nonlinear control of Chemical Processes: A review. *Ind. Eng. Chem. Res., 30(7)*, 1391-1413.

Cunningham, S. (2002). 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.

Lou, H. H., R. Muthusamy, and Y. L. Huang. (2003). Process Security Assessment: Operational Space Classification and Process Security Index. *Trans. IChemE. Part B. Process Safety and Environmental Protection, 81(6)*, 418-429.

Luyben, W. (1990). Process Modeling, Simulation and Control for Chemical Engineers, McGraw Hill, New York, NY.

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

Ragan, P. T., M. E. Kiburn, S. H. Roberts, and N. A. Kimmerle. (2002). Chemical Plant Safety: Applying the Tools of the Trade to a New Risk. *Chem. Eng. Prog.*, *98(2)*, 62-68.

Uygun, K. and Yinlun Huang. (2002). Integration of Design and Control: A Bi-Level Optimization Approach. AIChE 2002 Annual Meeting, Indianapolis, Indiana.

Uygun, K., H. H. Lou, and Y. L. Huang. (2003). Process Security Analysis: γ-Analysis and Σ-maps. *AIChE J*., *49(9)*, 2445-2452.

Uygun, K., H. H. Lou, and Y. L. Huang. (2004). Fast Process Security Assessment Theory. in press, *AIChE J.*