Journal of Hazardous Materials 115 (2004) 163–167

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

# Initial perspectives on process threat management

James R. Rob Whiteley [a,*], M. Sam Mannan [b,1]

[a] *Chemical Engineering, Oklahoma State University, 423 Engineering North, Stillwater, OK 74078-5021, USA*
[b] *Mary Kay O'Connor Process, Safety Center, Texas A&M University, College Station, TX 77843-3122, USA*

Available online 22 July 2004

**Abstract**

Terrorist and criminal acts are now considered credible risks in the process industries. Deliberate attacks on the nation's petroleum refineries and chemical plants would pose a significant threat to public welfare, national security, and the US economy. To-date, the primary response of government and industry has been on improved security to prevent attacks and the associated consequences. While prevention is clearly preferred, the potential for successful attacks must be addressed. If plant security is breached, the extent of the inflicted damage is determined by the available plant safety systems and procedures. We refer to this "inside the gate" response as *process threat management*. The authors have initiated a joint industry/academia study to address:

1. the level of safety provided by existing plant equipment and safety systems in response to a terrorist act, and
2. identification of process (rather than security) needs or opportunities to address this new safety concern.

This paper describes the initial perspectives and issues identified by the team at the beginning of the study.


*Keywords:* Process safety; Hazard analysis; Chemical facility vulnerability assessment; Counter terrorism; Process threat management

## 1. Introduction—the process threat management problem

After the tragic events of 11th September 2001, terrorist and criminal acts are now considered credible incidents in the process industries. Deliberate attacks on the nation's petroleum refineries and chemical plants would pose a significant threat to employee and public welfare, national security, and the US economy. To-date, the response of both government and industry has been to focus on improved physical and cyber security to prevent attacks and the associated consequences.

While prevention is clearly preferred, the potential for successful attacks must be recognized and addressed. If plant security is breached, the extent of the inflicted damage is determined by the available plant safety systems and procedures. We refer to this "inside the gate" response as *process threat management*.

The purpose of this paper is to begin consideration of the terrorist or criminal threat from a process, rather than security, point of view. All process plants are designed to deal with unintentional events such as equipment failure, loss of utilities, fire exposure from spills, etc. that threaten safe operation of the facility. While existing safety systems will respond to any predefined process deviations, they were not designed to address acts of sabotage or a thinking adversary. From a process perspective, a new capability must be developed to counter the threat of deliberate acts to process plants.

This paper is organized as follows. An overview of the post-11th September response by industry and government is presented first. The overview material includes a listing of the different security vulnerability assessment tools that have been developed to assist owner/operators. Other work related to the process threat management problem is then reviewed. The focus of the paper then shifts to the new process safety implications of terrorist or criminal acts. The material presented consists of initial thoughts concerning: (1) the level of safety provided by existing plant equipment and safety systems and (2) identification of process (rather than security) needs and opportunities to address this new safety concern.

* Corresponding author. Tel.: +1 405 744 9117; fax: +1 415 744 6338.
*E-mail addresses:* whitele@ceat.okstate.edu (J.R.R. Whiteley), mannan@tamu.edu (M.S. Mannan).
[1] Tel.: +1 979 862 3985.

0304-3894/$ – see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2004.05.011

## 2. Post-11th September response of industry and government

### 2.1. Site security and vulnerability assessment

Industry responded swiftly to the new threat of domestic terrorism. Site Security Guidelines for the US Chemical Industry were developed jointly by the American Chemistry Council (ACC), the Chlorine Institute, and the Synthetic Organic Chemical Manufacturers Association (SOCMA) [1] and issued before the end of 2001. Similar guidelines for the petroleum industry were published by the American Petroleum Institute (API) in 2003 [2]. The American Chemistry Council made enhanced security activities mandatory for its members in January 2002. The most recent additions to the ACC Responsible Care® security code require independent third-party verification.

Development of security vulnerability assessment methodologies was initiated by several industry groups with results published in 2002 and 2003.

- The American Institute of Chemical Engineers (AIChE) Center for Chemical Process Safety (CCPS), Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites, August 2002.
- Synthetic Organic Chemical Manufacturers Association, SOCMA Manual on Chemical Site Security Vulnerability Analysis Methodology and Model, November 2002.
- American Petroleum Institute/National Petrochemical and Refiner's Association, Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, May 2003.

The federal government moved quickly along a parallel path. The National Institute of Justice, working with Sandia National Laboratory, developed the following methodology.

- National Institute of Justice/Sandia National Laboratory, A Method to Assess the Vulnerability of US Chemical Facilities, November 2002.

Each of the methodologies listed above employ traditional risk assessment techniques and provide a well-defined, systematic framework to identify security threats, risks, and vulnerabilities.

In April 2002, the chemical industry established a link to the National Infrastructure Protection Center (NIPC), based at FBI headquarters in Washington, DC, by creating the Chemical Sector Information Sharing and Analysis Center (ISAC). The ISAC communication network allows the NIPC to quickly analyze and share information with the chemical industry. The ISAC network is operated by the American Chemistry Council's CHEMTREC® emergency response communications center.

### 2.2. Federal policy and legislation

Petroleum refineries, chemical plants, and related facilities have been designated as part of the nation's critical infrastructure [3]. Within the US government, the President initially named the Environmental Protection Agency (EPA) as the Lead Federal Agency for reducing the vulnerability of the chemical industry and hazardous materials sector. This responsibility is reflected in the EPA's Strategic Plan for Homeland Security [4] released in 2002.

To date, no new legislation for the purpose of protecting the public from potential terrorist attacks at chemical plants has been passed by the US Congress. Senator Jon Corzine introduced bills for this purpose in the US Senate in October 2001 (S 1602) and January 2003 (S 157), but neither has been passed. In May 2003, Senator Jim Inhofe introduced a bill (S 994) on behalf of the Bush Administration. The Inhofe bill differs significantly from the Corzine bill in two respects: (1) the Corzine bill includes a requirement that companies consider inherently safer technologies as an alternative to security measures and (2) the Inhofe bill assigns oversight to the Department of Homeland Security rather than the EPA. Industry supports the Inhofe bill.

### 2.3. News media and public awareness

The potential impact of a terrorist attack due to release of toxic material in a densely populated area has been broadly publicized by the news media. A frequently quoted study by the US Army Surgeon General concludes that as many as 2.4 million people could be killed or injured in an attack against a US toxic chemical plant [5,6]. Another frequently quoted study is a 1999 report by the Agency for Toxic Substances and Disease Registry [7]. News releases from environmental activist organizations frequently reference EPA records indicating that worst case releases from 123 chemical facilities in the US threaten a million or more nearby residents and that each of over 700 plants put at least 100,000 people at risk. Most of these potential incidents are associated with uncontrolled vapor release of chlorine, sulfuric acid, hydrogen fluoride, or sulfur dioxide.

Public concern regarding the potential for a catastrophic release is undoubtedly raised by reports from government agencies citing inadequate facility security. Two recent examples include a March 2003 report from the US General Accounting Office (GAO) [8] and a January 2003 report from the Congressional Research Service [9]. During the same period, the Department of Homeland Security issued at least one warning [10] that "Al Qa'ida operatives may attempt to launch conventional attacks against the US nuclear/chemical-industrial infrastructure to cause contamination, disruption, and terror. Based on information, nuclear power plants and industrial chemical plants remain viable targets." A February 2003 article by Weinstock [11] described the ease with which reporters or activists were able to enter chemical facilities.

### 2.4. Summary of work performed to date

Improving physical site security has been the main response to the 11th September tragedy. Much attention has been paid to the three G's—guards, gates, and guns.

The need to provide cyber security to protect plant data acquisition and control systems has also been recognized [12,13]. A summary of the government and chemical sector initiatives in cyber security is presented in an electronic newsletter prepared by the Critical Infrastructure Protection Project [14].

There has been little published in journals and magazines associated with the process industries. The articles that have been published address security or vulnerability assessment [15–19]. Baybutt [20], Baybutt and Ready [21] makes a clear case that traditional risk assessment methods used for US Occupational Safety & Health Administration mandated process safety management must be augmented to address deliberate acts.

## 3. Process response to a terrorist or criminal act

Reported work has focused almost exclusively on security and prevention of attacks. While prevention is clearly preferred, the potential for successful attacks must be addressed. If plant security is breached, the extent of the inflicted damage is determined by the available plant safety systems and procedures.

The previously referenced vulnerability assessment methods all acknowledge the need for analysis "of a manufacturing process's response to a terrorist attack." There is a wide body of literature on how to perform traditional process hazard analyses [22–27]. However, when developed, these techniques did not consider deliberate acts and the associated implications on performance of plant equipment and safety systems. Consequently, there is uncertainty regarding the level of protection provided against this new type of destabilizing event.

The public has high expectations regarding safety in plant operations. This is due in part to long-standing industry initiatives and programs such as Responsible Care®. When considering the threat of deliberate acts against process plants, it is likely that societal expectations exceed the capability of existing plant safety systems. To maintain a proactive post-Bhopal, India, approach, work is required to:

1. determine the level of safety provided by existing plant equipment and safety systems in response to a terrorist act, and
2. identify process (rather than security) needs and opportunities to address this new safety concern.

The authors are currently in the midst of such a study using a single refinery unit as the test case. The remainder of this paper describes process concerns and issues that emerged at the beginning of the study. Generalized findings from the study will be published when the work has been completed.

### 3.1. Bases for analysis

Traditional safety systems are designed to deal with one unpredictable (unintentional) event followed by a sequence of consequences predictable in advance. In a terrorist or criminal act, multiple events of unpredictable nature over an unknown time frame must be considered. The additional complexity introduced by deliberate acts requires development of new analysis and response methods to maintain and improve existing levels of safe operations. The deliberate nature of a terrorist or criminal act introduces four factors that are outside the scope of the traditional process safety paradigm.

*F-1*: Safety events previously considered statistically implausible must now be considered.
*F-2*: The number of event combinations and sequences that must be considered during analysis of a real-time event has increased exponentially.
*F-3*: The default operating state produced by the existing safety system may no longer be achievable or the best choice.
*F-4*: Temporal or dynamic effects have been introduced that require real-time response planning.

The fundamental questions that need to be answered include:

*Q-1*: If no changes are made in the existing process safety systems, what type of performance can be expected in response to a criminal attack? Is a reduction in impact possible? If yes, how?
*Q-2*: How can existing process hazards analysis (PHA) methods be exploited and/or modified to address process threats? Are new tools needed? If yes, what are the required capabilities?
*Q-3*: What should be the operating strategy during an attack? Can existing plant automation (regulatory control system, advanced control systems, safety instrumented systems) be employed in new ways to minimize damage from terrorist attacks? Is new or additional automation needed?

The starting point for any additional analysis should be the results generated by the traditional PHA. That is, we want to leverage existing results and methodologies to the maximum extent possible with minimum additional effort.

In this paper, we are restricting our attention to the case of an existing plant. The broader case involving a grass roots design is not considered. Also, we are primarily focusing on the terrorist rather than activist threat. We differentiate terrorists and activists based on the assumed objectives of the two groups. We characterize a terrorist as a thinking adversary whose goal is maximum damage and loss of

life. We assume activists are primarily interested in business disruption without intentional loss of life.

### 3.2. Considerations impacting an analysis

When considering the response of an existing plant to a terrorist attack, several issues immediately emerge. One of the first is how to characterize an attack. Using a modeling metaphor, what is the sequence of inputs? Conceptually, there are an unlimited number of attack scenarios and associated input sequences. The problem can appear overwhelming as the finite number of safety events that we had to deal with pre-11th September has been uncapped. We need some method to identify a critical subset of the possible scenarios. Results of a security vulnerability assessment (SVA) using any of the methods listed in Section 2.1 will be helpful, but, do not provide the answer to the problem. The vulnerabilities identified in a SVA represent end points for scenarios in the critical subset of input sequences. What is needed is a tool or methodology for integrating SVA and HAZOP results to automatically produce scenarios in the critical subset.

An alternative approach to generating the critical subset would be to work back directly from the limitations of the existing plant safety system. Such a method would be "process-based" rather than "asset-based" (SVA methods). Development of an analysis method using this approach would likely provide benefits for traditional safety analysis and design purposes.

When analyzing the response of the plant to a specific attack scenario (input sequence), the same methods and calculations employed for traditional safety analysis should be used. The physical phenomena (compressible flow, flashing, dispersion, etc.) are the same. The sequence and combination of calculations may be different reflecting event sequences not previously considered, but we do not perceive any major deficiencies in the fundamental tool set used for safety analysis.

During initial identification of worst-case scenarios, sabotage of safety systems, control systems, and plant utilities emerge as common factors. The need for HAZOP modifications to address these scenarios appears essential.

Event trees may be useful for evaluating intentional incident pre-cursors. These pre-cursors might be identified by "what-if" analysis or modified guidewords in HAZOP. As an example, consider "reverse flow intentional." Is it possible? If so, are additional safeguards required? Event trees could be used to screen nodes and identify process vulnerability. The event trees would not need to be quantitative at this level.

The greatest danger to a plant may occur when there is insider collusion. Changing the position of normally open or closed valves in a pressure relief of safety-instrumented system prior to an attack would be potentially devastating. There may be opportunities to apply new technology ("smart" carseals or locks that signal when broken) or modify operating, maintenance, and management procedures to reduce the potential for this concern.

Besides the possibility of a pressure relief system being blocked out, terrorist events may also create a situation where the required relief rate exceeds the capacity of a safety relief valve. Mechanical failure of equipment or piping would be likely in this case. From a consequence management standpoint, it would be preferred if the failure points were predefined. Just as atmospheric storage tanks are designed with frangible roofs (intentionally weak weld seam between the tank roof and walls), it may be desirable to provide nozzles, manways, or piping with similar characteristics.

From a risk management standpoint, a terrorist event increases the potential for loss of containment. It may be useful to map inventories of material in the process in terms of explosive energy or fire. New terrorist event scenarios may produce equipment siting impacts not previously deemed credible.

Mitigation of some of the safety issues created by a terrorist attack may be achieved only through use of procedural systems. Traditional safety systems (passive and active) are designed to deal with one unpredictable (unintentional) event followed by a sequence of consequences predictable in advance (off-line). In a terrorist or criminal act, multiple intentional events of unpredictable nature over an unknown timeframe must be considered. The implications on plant operation are illustrated in the following simple analogy.

*Traditional (unintentional) safety event*: An operator is driving a car when one of the front tires experiences a sudden blowout after unintentionally running over a nail. The operator is not sure why the tire failed but has no reason to expect other problems. The operator can anticipate the consequences and makes steering and speed adjustments to bring the car to a stop at the side of the road. This is similar to the response of the passive safety systems used to provide over-pressure protection in most plants.

*Terrorist or criminal (deliberate) safety event*: The operator is driving a car when a terrorist suddenly jumps from the side of the road and throws a spike strip in front of the car to cause a deliberate blowout of one or more tires. The result is the same as with the unintentional blowout but the operator has reason to expect additional hostile action. Rather than bring the car to a stop, the operator may choose to slow the car to a controllable speed but continue driving in a direction and manner that maximizes his perceived chances for survival. The responses of the passive safety systems are utilized in this case but continued operation of the process (car) is required. At present, the automation used to control process plants is incapable of actively "driving away from danger" without manual intervention from the operating staff.

There are two points to be taken from this analogy. The first is that the concept of the traditional "fail-safe" condition for a plant may not be applicable to a plant under terrorist attack. The second is that some type of planning ability is

required to produce a response that minimizes the impact of a thinking adversary.

Currently, the operator represents the sole source of reactive planning ability. However, the use of micro-processor equipped "smart instruments" provides future potential to build automated self-defense capabilities into a process. For plants that employ advanced process control (APC), there is also potential of creating a quantitative safety objective function to replace the traditional economic objective function during a criminal attack. Development of either type of automated response system would require a method to verify asset (equipment and piping) integrity. Such a system would be of use to the operations staff as well.

## 4. Conclusions

Essentially all of the post-11th September efforts to protect process plants from terrorist threats have focused on enhanced physical and cyber security. There remains a need to understand how existing plant safety systems would respond to a terrorist or criminal attack. It is important to recognize that security vulnerability assessments (SVAs) do not answer this question. A SVA provides valuable information but does not replace a process hazards analysis (PHA). Work is required to: (1) determine how existing PHA methods could be modified to address the threat of terrorist acts and (2) determine what changes in equipment, policy, and procedures could be implemented to minimize the impact of a terrorist attack (process threat management).

## Acknowledgements

The extensive contributions of Prof. Jan Wagner at Oklahoma State University are gratefully acknowledged.

## References

[1] American Chemistry Council, Chlorine Institute, and Synthetic Organic Chemical Manufacturers Association, Site Security Guidelines for the US Chemical Industry, 2001.
[2] American Petroleum Institute, Security Guidelines for the Petroleum Industry, 2003.
[3] President's Office of Homeland Security, http://www.whitehouse.gov/pcipb/physical_strategy.pdf, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, 2003.
[4] Environmental Protection Agency, EPA Announces Homeland Security Strategic Plan, One of Many Efforts to Ensure Agency's Ability to Protect, Respond and Recover, EPA Newsroom, http://www.epa.gov/epahome/headline_100202.htm (2 October 2002).
[5] E. Pianin, Study Assesses Risk of Attack on Chemical Plant, Washington Post, http://www.washingtonpost.com/ac2/wp-dyn/A10616-2002Mar11 (12 March 2002), p. A08.
[6] A. Kostant, Terrorist Attack on Chemical Plants could Endanger Millions, Environmental Media Services, http://www.ems.org/chemical_plants/zz.ems.02.06.20.html (20 June 2002).
[7] Department of Health & Human Services—Agency for Toxic Substances and Disease Registry, http://www.mapcruzin.com/scruztri/docs/cep1118992.htm, Industrial Chemicals and Terrorism: Human Health Threat Analysis, Mitigation and Prevention, 1999.
[8] J.B. Stephenson, http://www.gao.gov/new.items/d03439.pdf, Homeland Security: Voluntary Initiatives are under Way at Chemical Facilities, but the Extent of Security Preparedness is Unknown, GAO-03-439, US General Accounting Office, 2003.
[9] L.-J. Schierow, http://www.ncseonline.org/NLE/CRSreports/03Jan/IB10067.pdf, Chemical Plant Security, Order Code RL31530, Congressional Research Service, The Library of Congress, 2003.
[10] National Infrastructure Protection Center, Homeland Security Information Update, Information Bulletin 03-003, 2003.
[11] M. Weinstock, http://www.govexec.com/features/0203/0203s2.htm.
[12] D.J. Teumim, Chem. Eng. Prog. 98 (2002) 69.
[13] R.F. Dacey, Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities, in Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, United States General Accounting Office, Washington, 2001.
[14] http://www.gmu.edu/departments/law/techcenter/programs/cipp/cip_report.html.
[15] E.M. Marszal, Chem Eng 110 (2003) 42.
[16] D. Heinold, D. Smith, http://www.ensr.com/newsroom/insight/insight_articles/2002_v3/v3a1.htm.
[17] J. Schwartz, Adhes. Age 45 (2002) 12.
[18] P. Baybutt, Chem. Eng. 110 (2003) 48.
[19] P.T. Ragan, M.E. Kilburn, S.H. Roberts, N.A. Kimmerle, Chem. Eng. Prog. 98 (2002) 62.
[20] P. Baybutt, Process. Saf. Prog. 21 (2002) 269.
[21] P. Baybutt, V. Ready, Homeland Defense J. 2 (2003) 1.
[22] M.S. Mannan, D. Hendershot, T.A. Kletz, in: R.G. Anthony (Ed.), Fundamentals of Process Safety and Risk Management, vol. 69, Suppl. 1, Marcel Dekker Inc., New York, 2002, p. 49.
[23] D.A. Crowl and J.F. Louvar, Chemical Process Safety: Fundamentals with Applications, Prentice Hall, Englewood Cliffs, NJ, 1990.
[24] Center for Chemical Process Safety, Guidelines for Chemical Process Quantitative Risk Analysis, American Institute of Chemical Engineers, New York, 1989.
[25] Center for Chemical Process Safety, Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples, American Institute of Chemical Engineers, New York, 1992.
[26] Center for Chemical Process Safety, Guidelines for Consequence Analysis of Chemical Releases, American Institute of Chemical Engineers, New York, 1999.
[27] G. Wells, Hazard Identification and Risk Assessment, Institution of Chemical Engineers, Rugby, Warwickshire, UK, 1996.