Testimony of

David A. Moore, PE, CSP
President & CEO
AcuTech Consulting Group
Chemetica, Inc.
2001 N Beauregard Street
Alexandria, VA 22311
www.acutech-consulting.com

At a Hearing On

Inherently Safer Technology in the Context of Chemical Site Security

Before

The Senate Environment and Public Works Committee
Dirksen Senate Office Building
June 21, 2006

Introduction

Good morning, Mr. Chairman. My name is David Moore and I am the President and CEO of the AcuTech Consulting Group, a security and safety consulting firm based in Alexandria, Virginia. I have an extensive background in chemical safety and security with a specialty in the application and regulation of inherent safety for chemical plant security.

I was the lead author of 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"[1] and the American Petroleum Institute (API)/National Petrochemical and Refiners Association (NPRA) Security Vulnerability Assessment Methodology[2]. These are the most highly used security vulnerability analysis guidelines in these industries.

I completed a project in January, 2006, as the Sector Coordinator for the petroleum refining, chemical manufacturing, and liquefied natural gas sub sectors for the Department of Homeland Security (DHS) initiative to develop a common strategic vulnerability analysis process called 'Risk Analysis and Management for Critical Asset Protection (RAMCAP). We currently have other efforts ongoing in support of industry and government to reduce homeland security risks in the chemical sector including ongoing consultation to DHS for the chemical comprehensive review program.

My firm is actively involved in chemical process security consulting and training and in conducting Inherently Safer Technology (IST) studies for safety and security, some of which are done to address current regulations in effect in Contra Costa County, California, and the State of New Jersey. I have been consulting in chemical process safety since 1981 and formally in inherent safety regulation since 1999. Prior to that time there wasn't a regulation that required IST, but I was practicing the principles of inherent safety routinely. I was formerly a Senior Engineer with Mobil Corporation, who condoned the principles of inherent safety in every decision we made, and before that I was a Research Engineer with the National Fire Protection Association.

In particular, I have assisted companies in understanding the concepts of inherent safety through our consulting and training assignments, and have conducted dedicated and integral inherent safety analyses on chemical facilities and other industrial facilities handling hazardous materials. I have published twelve papers on inherent safety, the regulation of inherent safety[3], and inherent safety consideration in chemical security. I have made numerous presentations on the topic at professional conferences, training forums, and government venues.

Because of our experience we were selected by the AIChE CCPS® to update their classic book on inherent safety[4], which we are in process of at this time. For that I am working with the leading inherent safety specialists in the United States and internationally from industry and academia who serve as advisors to our team. I am a strong proponent of

inherent safety, the ultimate goal being to see all companies applying inherently safer principles throughout the design and operating lifecycle of projects.

Inherent Safety Technology Background

Inherent Safety (IS) is emerging as a key process risk management issue. Process safety professionals have embraced the concepts voluntarily for years and it is an established method for addressing process risks. Any chemical company could point to inherent safety considerations they have implemented, whether for a regulation or not. This is because it is a general philosophy rather than a science, and it is imbedded in the thought process of chemical and safety engineers as they design and operate safe plants. They could also speak to many other process risk management techniques that are effective at risk reduction, including passive, active, and procedural layers of protection. They tend to employ a mixture of these strategies for optimal risk reduction as is appropriate.

Inherent Safety is a well recognized process safety concept; a collection of basic strategies focused on process safety improvement through the reduction of hazards. "Hazard" is defined as a physical or chemical characteristic that has the potential for causing harm to people, the environment, or property.5 The IS concept is based on the belief that if one can eliminate or moderate the hazard, not only is the risk reduced, it may be possible to remove the risk altogether from consideration. Alternatively, an inherently safer system would make the hazard less likely to be realized and less intense if there is an accident.

It is a not necessarily a change in 'technology' that the term IS is referring to – it may involve less dramatic ideas than a change in technology such as a simplification of operating controls. I therefore refer to it as Inherent Safety (IS) to be inclusive of the full range of inherently safer strategies that were originally in mind. Technology may be mistaken to mean only process chemistry or the material used, rather than other aspects of IS.

IS includes four basic strategies for safety engineers to apply for process safety and risk management of chemical manufacturing plants, namely substitution, minimization, moderation, and simplification. These four strategies could be independent ideas or they may relate to one another, depending on the case by case situation. There is no defined and agreed upon way to consider them in a formal analysis methodology. Engineers are encouraged to consider them to the extent possible, but given the innumerable situations where they may be applied there cannot be a rule on what is an adequate consideration of IS.

In 1996 the AIChE CCPS® published the book "Inherently Safer Chemical Processes – A Concept Book", to clarify the concept and to help provide examples. Today it remains one of the leading practitioner's guides to understanding and applying inherent safety concepts. It is the leading reference mentioned in various regulatory actions and proposed actions.

Issues with Inherent Safety

Inherent safety is a challenge for all parties – the owner, chemist, operator, design engineer, regulator, and the public. There are limitations of inherent safety and technical and business constraints to its usage. There are examples of where inherent safety has been very useful and where opportunities may exist, but since it is a concept the blanket requirement of inherent safety poses issues.

- **Undocumented considerations**

IS is not new but regulation of IS is new. Most of industry is already practicing it but not formally documenting how they use inherent safety as a strategy for risk management. Engineers tend to make orderly, inherently safer decisions by practice for the most part. This has been expected of industry as a matter of principle, and there is evidence it is being practiced but without a degree of measurement of their actions or the benefits. One of the suspected reasons for this is the lack of formal and agreed IS analysis approaches, and the other is that these requirements simply haven't existed until recently to document the considerations.

- **Requires judgment and is potentially subjective**

It is precisely because IS is vague and involves considerable judgment that it is very difficult to define and implement to any degree of uniformity and objectivity. This is particularly true in the chemical sector where the diversity of chemical uses and processes and site specific situations prevents clear characterization of the industry and a one-sized-fits-all solution.

IS can also be very subjective – how 'safe or secure' is 'safe or secure enough' is a decision of the analyst conducting the study. There are no clear and objective guidelines on how to make these decisions as it is considered both a concept to apply as one sees fit and as opportunities arise.

The CCPS® book itself is indeed a concept book and it does not provide a clear delineation of what is inherently safer or how to judge whether an inherent safety analysis is comprehensive and complete enough. The reason for this is that the topic is so diverse that it is, in some cases, even ambiguous. There is an entire section of the book explaining the numerous conflicts and risk:risk tradeoff problems of IS. Also the state of the practice is not perfectly clear on how it should be defined, conducted, analyzed, assessed, or judged as adequately performed. The book doesn't solve the classical problems with IS of trying to objectively decide 'what is inherently safer' and how to measure whether a process is safe enough. This sums the state of the practice with IS and is an underlying basis of the problems of attempting to regulate it and to apply it to security issues.

In actual practice this has proven to be problematic because IS, at this stage in its development, is more of a conceptual methodology rather than a codified procedure

with a well established and understood framework for evaluation and implementation. This is somewhat a function of the state of the art of our understanding of IS.

- **Value and Perspective**

What is inherently safer to one person is not necessarily inherently safer to another – it is a matter of perspective. If one takes an insular view of what is inherently safer, it may not be the most inherently safe decision for society as a whole. For example, if a plant decides to lower its risk at a given fixed chemical plant site by reducing inventory or making an alternative product, this could simply either transfer the risk to more of the public through increased shipments of hazardous materials in the community or move the same operation to another location which may be more problematic.

Companies may be unclear on the value of IS or may be unable to easily prove that IS is beneficial to employ. Methods to prove the value of IS and to quantitatively measure whether a given process is 'as inherently safe as is practicable' are generally unavailable or unproven. Case studies showing the economic and other benefits are not available for a wide array of industrial situations.

Depending on the goals, the perspective may be that it is safe or secure enough as it is. For example, the plant is designed to operate at a given capacity and has been optimized through careful engineering design to produce the product safely, efficiently, and cost-effectively. Many IS-type considerations have already gone into the design or operating philosophy of the plant. When confronted with the need to conduct an IS study, they often find that there are few opportunities to improve on that design, short of a complete change of 'technology', even if another technology exists that is inherently safer. If it does exist they find it troubling to consider changing the technology when the gains may be questionable for safety or security. As such the net change may be limited.

- **Safety and Security Conflicts**

The need to introduce inherent safety as a strategy at all facilities subject to such a security regulation is questionable. This would result in a great deal of analysis to consider a single strategy has been applied, thereby causing a very large documentation problem and undoubtedly many technical and legal dilemmas. This is contrasted with a preferred approach of allowing industry to set security objectives to determine the relevant issues and vulnerabilities and make appropriate risk management decisions. It should be considered as a potential strategy rather than the first priority and allow the most effective homeland security strategies to be applied rather than force a particular one or a change in every technology.

In fact, *what is inherently safer is not necessarily what is inherently more secure.* For example:

- Moderation - a process that successfully applied an inherently safer technology may have changed a catalyst to end with a 'moderated' process – one that is operated at a lower pressure and temperature. This is commendable for safety, but may have little to do with security. The process may be disabled just the same, which is an issue of economic security, or it may release a flammable or toxic cloud which is just as significant.
- Minimization - In another case an owner may have reduced the inventory of a feedstock in a tank to reduce the consequences of an attack. The feedstock is a toxic substance, so this appears sensible, but the material is also a 'dual purpose' chemical that could be used to make an improvised chemical weapon. In that case simply reducing the volume may not matter for the threat of theft of the materials – in fact smaller quantities may be more man-portable thereby accommodating theft. The plant may need for frequent deliveries of the material, which also increases the chance of theft.
- Simplification - An owner may invest considerable sums of capital to improve the simplicity of the control system, thereby lessening the chance of human error as a cause of an accident. This may result in a control system that is easier to compromise.
- Substitution – A petroleum refiner may substitute hydrogen fluoride catalyst with sulfuric acid for alkylation (along with substantial process changes). While the individual offsite impacts may be reduced from storage the opportunities for disruption of the transportation chain are increased due to the additional deliveries of acid that are required. Besides the number of additional volumes of materials transited throughout the community, the site has increased vulnerability each time a vehicle has to enter the perimeter. Generally speaking security professionals try to find ways to reduce penetrations through a secured perimeter.

IS Regulatory Proposals and Complications

Inherent Safety is a common phrase from the chemical industry and is being considered and debated as a chemical process security concept for inclusion in proposed chemical security regulations[6]. IS is being considered by legislators as the first security strategy industry should use for reducing terrorist risk in the chemical sector. The newly appreciated concerns for terrorism have naturally highlighted the issue of the potential for attack on facilities handling hazardous materials. Out of this concern first sprung a potentially far-reaching proposed act titled the Chemical Security Act of 2001, S.1602. The Act was introduced on 10/31/2001 by Senators Corzine (D; NJ), Jeffords (D; VT), Boxer (D; CA), and Clinton (D; NY). Since then there have been several other proposals.

The proposed series of Chemical Security Act bills generally state that there are significant opportunities to prevent theft from, and criminal attack on, chemical sources and reduce the harm that such acts would produce by reducing usage and storage of chemicals by changing production methods and processes; and employing inherently safer technologies in the manufacture, transport, and use of chemicals;

These proposed regulations would have sweeping applicability and significant implications for design and operation of facilities handling hazardous materials. Many of the facilities mentioned to be included are from the USEPA Risk Management Planning regulated sources (40 CFR Part 68), which may not be either highly consequential or attractive to terrorists. Any new initiatives such as this have to be rational, measured, cost-effective, and fully justified.

The anticipated regulatory benefit seems to be that IS can remove the hazard entirely or reduce hazards to de minimis levels to where there is no interest in causing the attack. It is often expressed to be a possible strategy for security risk management, and sometimes is mistaken as a relatively obvious and simple approach to execute or regulate. Other proven security measures are often seemingly weighed as less effective or reliable.

These existing and proposed regulations typically end in a goal of IS consideration 'to the extent practicable' and sometimes allow cost or feasibility as a basis for justifying a change is 'practicable'. There is no standard measurement of what this means. While companies may believe they are moving toward inherently safer processes, they often find obstacles to the theoretically possible complete application of the four IS strategies.

Homeland security is not that simple and the implementation of IS is not that easily accomplished or even necessary for that purpose in all cases.

Problems with regulation of IS

- **Holistic security v. singular issues**

The problem is not IS, but the expectation of the value of regulation of IS. It forces industry to focus on a few safety strategies to the possible detriment of the complete approach to risk management. There seems to be an overemphasis of inherent safety as a singular strategy for security assurances in many of the proposed regulations.

Inherent safety has to be considered in light of other security risk management approaches where one is not necessarily preferable over another. That decision should be made on a case by case basis rather than blanket regulatory requirements. Most security experts would agree that it is about providing sufficient layers of security, combined with an understanding of the threat and risk-based approaches to limiting access to possible assets of interest to adversaries that is the desired homeland security approach.

Both chemical process security and inherent safety are complex topics that are not easily mandated. To isolate inherent safety as a particularly necessary one is good practice but not necessarily good government regulation. IST is not the panacea. It is not a "thing" that can be measured. It is a process towards safe manufacturing. It is a system of interdependent values and not something that can be distilled into a legislative definition and then regulated. Security management itself isn't a singular strategy. Furthermore, IS cannot be regarded as the sole design or operating criteria

as it must be integrated with other considerations. The real issue is risk, whether safety or security risks, that IS can be applied to.

- **Degree of regulatory compliance effort**

If IS is forced onto industrial facilities, there could be considerable dilemmas in interpretation, technical judgment, fairness, and liabilities. It isn't possible for everyone to fairly be dictated as to what is inherently safer. If the degree of inherent safety is left to discretion, there could be a very uneven treatment of the issue.

If the regulator was to make the judgment of what is practicable or the extent of practicality, there could be numerous issues develop. Do we want outside third parties to force changes in technology or operating philosophy on a company and to take on the liability of that decision when they may clearly lack the expertise for making this decision?

Since you can't measure it, how could you ever comply...how much IST is enough...what is compliance...how can you ever demonstrate that you adequately considered something so that it met some arbitrary definition. IST for every facility is not even feasible as there fewer options for some sites (where substitution of chemicals isn't possible since it is the only way or decidedly the best way or common practice for a given process).

No one is sure, therefore, of the degree of difficulty that requirements such are being proposed will cause but there will be, no doubt, considerable confusion due to the degree of ambiguity involved.

- **Diversion of scarce resources needed for homeland security**

Regulatory impacts may cause a possible diversion of attention to the complete set of security measures available to the industry given the threat, consequences, and vulnerabilities. It provokes an enormous effort with possibly little to no additional gain, possibly at the detriment to security as resources are expended on less critical issues. It may not get at the heart of the matter – the degree of risk primarily caused by the degree of vulnerability of the industrial facilities.

This is process for chemical engineers together with safety experts to examine on a case-by-base basis, not in a sweeping edict from Congress. I am very concerned that rather than addressing true homeland security issues of the chemical sector, many hours of effort and resources would be diverted to proving the a process was already inherently safe as is practicable. The potential for litigation trying to "prove" you considered something is enormous.

Although a process or plant can be modified to increase IS at any time in its life cycle, the potential for major improvements is greatest at the earliest stages of process development. At these early stages, the process engineer has maximum

degrees of freedom in the plant and process specification. The US infrastructure that is being considered for chemical security regulation initially under any future regulation that requires IS is existing plant.

- **Judging adequacy and effectiveness**

There is little guidance on how to judge effectiveness and completeness of inherent safety, particularly in a meaningful, fair and equitable way to all parties. This could prove to be a major dilemma for both industry and regulators as they try to justify that 'enough' inherent safety has been applied to be considered 'in compliance' with inherent safety requirements of security regulations. Experience has shown that regulators and industry have a difficult time interpreting inherent safety and agreeing on adequacy of efforts.

Given that inherent safety is a rather subjective concept, it makes the matter a difficult one to understand, implement, and regulate. Companies should be knowledgeable of inherent safety and actively encourage the use of it at every turn in a holistic approach to risk reduction.

Experience with IS Regulations

In actual practice IS implementation has proven to be problematic. The reason is that IS, at this time, is more of a theoretic concept rather than a codified procedure with a well established and understood framework for evaluation and implementation. Furthermore, it cannot be regarded as the sole design criteria as it must be integrated with other considerations. Industry

Today there is only one example of an implemented IS regulatory requirement for process safety and that is part of the Contra Costa County, California, local Industrial Safety Ordinance (ISO) enacted in 1998 which effects only eight chemical sites. As for security, the only one that exists is in New Jersey where the Governor enacted a Prescriptive Order in November of 2005 which includes the need to consider IS for chemical security for certain sites in the state. Neither regulation goes so far as to require a change in technology due to the enormous challenges and liabilities associated with that move.

- **Contra Costa County, California, Industrial Safety Ordinance**

The Contra Costa County, California, Industrial Safety Ordinance (ISO) became effective January 15, 1999. The ordinance applies to eight oil refineries and chemical plants that were required to submit a Risk Management Plan to the U.S. EPA[7] and are a program level 3 regulated stationary sources as defined by the California Accidental Release Prevention (CalARP) Program.

Part of the ISO requirements is the need for the regulated stationary sources to consider inherently safer systems when evaluating the recommendations from

process hazard analyses for existing processes and to consider inherently safer systems in the development and analysis of mitigation items resulting from a review of new processes and facilities. Contra Costa Health Services completed and issued a Contra Costa County Safety Program Guidance Document on January 15, 2000_4. This document included a definition of inherent safety and some rules for implementation of the ordinance.

Lessons Learned from the Contra Costa County, California, implementation of inherent safety requirements for their Industrial Safety Ordinance were presented in 2002 (Moore, 2002)[8].

- Companies found IS to be difficult if not infeasible to accomplish, particularly for existing processes;
- There are different perspectives on what is reasonable and what is feasible when it comes to decisions on the need for implementing IS;
- The guidance provided to ensure that IS was being considered consistently and fully was not informative enough, so there was some confusion and an education gap;
- The public and regulators often mistrust industry if anything less than a total technology change is implemented despite that IS includes a wide variety of ideas to meet the four strategies of minimization, substitution, simplification and moderation;
- Application of IS at only the most purely inherent level (first principles) is often at odds with practical and cost effective risk reduction, especially for existing construction;
- Guidance/training is needed for a team to know how to apply IS effectively.

- **New Jersey Prescriptive Order**

On November 21st, 2005, the State of New Jersey became the first State to require chemical plant security measures to protect against terrorist attacks. Acting Governor Richard J. Codey set new requirements for the 140 facilities that must comply with the Prescriptive Order, 43 of which are subject to the state's Toxic Catastrophe Prevention Act (TCPA) program. As part of the new requirements, these 43 facilities must review the potential for adopting inherently safer technology (IST) as part of their assessment.

This is very significant for three reasons – it sets precedent for State mandate of security of the chemical industry, it incorporates the need to evaluate IST more widely than any other regulation in the United States, and it forces industry to prove compliance to security ‘best practices’ they developed.

In 2003, the New Jersey Domestic Security Preparedness Task Force approved best security practices that were built upon the security code of the American Chemistry Council's responsible care program and the American Petroleum Institute's security guidelines, respectively. The best practices were developed by

the Task Force and its Infrastructure Advisory Committee, which includes representatives of the state's chemical and petroleum industry. Many New Jersey-based facilities have voluntarily begun to implement these practices. The Prescriptive Order action clarifies that the best practices for chemical facilities are now mandatory.

The 43 chemical facilities in the TCPA program must analyze and report the feasibility of:

- reducing the amount of material that potentially may be released;
- substituting less hazardous materials;
- using materials in the least hazardous process conditions or form; and,
- designing equipment and processes to minimize the potential for equipment failure and human error.

Best practices included provisions for the facilities to prepare an emergency incident prevention, preparedness and response plan and outline the status of implementing other security practices. The State standards also now require worker participation in the development of the security assessments and prevention and response plans at each facility.

Under the new requirements, chemical facilities had 120 days to develop an assessment of facility vulnerabilities and hazards that might be exploited by potential terrorists. The assessments must include a critical review of:

- security systems and access to the facility grounds (including the regular testing and maintenance of security systems);
- existing or needed security measures outside the perimeter of the facility that would reduce vulnerabilities to an attack on the facility;
- storage and processing of potentially hazardous materials;
- employee and contractor background checks and other personnel security measures; and,
- information and cyber security;

The Prescriptive Order timing is critical as the nation struggles with how to more completely manage terrorism risks and to sort out the need for regulations for industries that are otherwise unregulated today. At this point the effectiveness of this rule is still in question. What is clear is the degree of change that most complex, existing plants will incur due to the identification of IS opportunities will be very limited based on personal experience.

Research on the Evaluation of Inherent Safety

Some methods have been proposed to provide a benchmark for inherent safety. Most of these involve indices or fuzzy logic. While these are excellent developments in the right

direction, they are not fully validated or comprehensive enough to assure that the aforementioned issues are satisfied.

There is a need for metrics and rules for how to evaluate inherent safety before regulations can be effective. Without a fair and legitimate way to measure the total risk balance created by changes in the name of inherent safety it will be subjective and possibly unfair.

Complex process systems, particularly with a long history of safe performance, cannot suddenly be dictated that a system is inherently safer without a great deal of individualized risk-risk tradeoff evaluation. Inherent safety is not fully understood, so regulating it and forcing change against typical engineering practices (with a strong empirical basis of success) is not recommended

There have been many experts recognize that this may be creating many other problems by overly relying on one strategy vs. a holistic approach. Facilities should be given that flexibility all the while bounded by appropriate layers of safety to reduce risk to an acceptable level.

Public Perception of Inherent Safety

Often inherent safety is seen as 'obvious' and 'common sense' when in reality the issue may not be that simple. Risk-risk tradeoffs can have unfortunate results if not properly evaluated. Priorities to inherent safety may mean compromises elsewhere. Efforts to reduce risks often neglect the possibility that measures to reduce the "target risk" may introduce or enhance "countervailing risks." 1

An important point is that we need to consider risk management interventions, not a single risk reduction strategy alone. Like medications, any intervention can have side effects. Instead industry and government should advocate a proactive, holistic approach rather than heuristic, piecemeal reactions to homeland security.

Barriers Identified For Implementing IS

A workshop was held on the challenge of IS at the 17th Annual CCPS International Conference & Workshop on Risk, Reliability and Security in Jacksonville, Florida, on October 11, 2002, to address the concerns of implementing IS. Speakers from the USEPA, AIChE, Contra Costa County, and industry presented their experiences on the issue. In summary of that discussion, the audience agreed that there were barriers for effectively

[1] Harvard Center for Risk Analysis, "Risk/Risk Tradeoffs in Pesticide Regulation: Evaluating the Public Health Effects of a Ban on Organophosphate and Carbamate Pesticides", George M. Gray and James K. Hammitt, Harvard Center for Risk Analysis And Department of Health Policy and Management, Harvard School of Public Health 718 Huntington Ave, Boston, MA 02115, August 6, 1999.

implementing IS, and issues and challenges for any regulation of IS. Some of the constraints were reported to be as follows:

Adoption and implementation of IS by industry:

1. Existing facilities vs. new facilities – one dilemma is that the majority of the applications for IS are with the existing industrial installed base whereas the feasibility of applying IS to the fullest diminishes as the facility is actually built. This leaves many companies where new processes (and particularly new technologies) are rarely implemented resulting in few occasions to practice the methods.

> "Although a process or plant can be modified to increase IS at any time in its life cycle, the potential for major improvements is greatest at the earliest stages of process development. At these early stages, the process engineer has maximum degrees of freedom in the plant and process specification. The engineer is free to consider basic process alternatives such as fundamental technology and chemistry and the location of the plant. Imperial Chemical Industries (ICI) describes six stages of hazard studies, including three during the process design phase and three during construction, startup and routine plant operation. The identification of inherently safer process alternatives is most effectively accomplished between the first and second process design hazard studies (Preston and Turney 1991). At this stage the conceptual plant design meets the general rule for an optimization process - that a true optimum can be found only if all of the parameters are allowed to vary simultaneously (Gygax 1988)." (CCPS, "Guidelines for Engineering Design for Process Safety, 1993)" [9]

2. Unproven Value – Companies many be unclear on the value of IS or may be unable to easily prove that IS is cost-effective and worthwhile to employ, particularly for security. Methods to prove the value of IS and to quantitatively measure whether a given process is 'as inherently safe as is practicable' are generally unavailable or unproven. Agreed upon and practical tools for systematically conducting IS reviews under repeatable methodologies are not available with the exception of checklists or adaptation of safety analysis methodologies. Case studies showing the economic benefit are not available for a wide array of industrial situations.

3. Unclear vision of scope of IS – One can take a broad or a narrow view of IS. The narrow viewpoint only credits major changes in the degree of hazard whereas the broad viewpoint of inherent safety finds any change by the application of IS principles to be an advantage. All of the proposed regulations are very vague in their definition of inherent safety and industry experts themselves have mixed opinions on this point. Is reducing some inventory IS or is it only IS if the material hazards was substituted, which is the IS strategy that seems to be of most interest for the regulatory proposals reviewed?

Regulation of IS:

The constraints to the regulation of IS include many of the concerns above plus:

1. Criteria for making compliance decisions – An obstacle to clear cut regulation is the lack of consensus on appropriate IS metrics. Assuming that the regulation is performance-based, there must be metrics for consistent regulation. These criteria are very hard to define with a broad conceptual topic such as IS for the wide variety of chemical processes to be regulated. This dilemma was recently described by the Mary Kay O'Connor Process Safety Center – "Regulation to improve inherent safety faces several difficulties. There is not presently a way to measure inherent safety. Process plant complexity essentially prevents any prescriptive rules that would be widely applicable. It would seem that legislation could explicitly require facilities to evaluate inherently safer design options as part of their process hazard analysis. But inherent safety would be almost impossible to enforce beyond evaluation because there are unavoidable technical and economic issues." (Mannan, et.al, 2003[10])

2. Need to consider risk rather than only hazard - There is little sense to the idea of imposing a requirement for 'change for the sake of change', i.e., requiring that every hazardous situation be made inherently safer. Industry is interested in referencing a measure of acceptable risk which limits the need for additional risk reduction since beyond that level resources may be better spent on other matters.

3. Unclear how to measure performance or compliance – Will regulations require only fundamental strategies to be employed, such as a site reports it reduced some materials onsite, or will it be based on vulnerability to the chemicals that remain? The factors and process to measure the effectiveness of IS regulations is not defined so it becomes very subjective. – Inherent safety regulations would have to show measurable benefit. If there was a reduction or increase in the number of incidents it could be incorrect to infer whether IS was the leading factor or whether other measures were involved. It is, therefore, difficult to measure the effectiveness of IS regulations.

The USEPA representatives at the workshop reported that the EPA intends to include IS in their analysis of the effectiveness of the Risk Management Plan (RMP) regulation (USEPA, 1996)[11] when they review the next submittals of registrations and hazard assessments. This is likely to be challenging given the state of implementation of IS and EPA's own admission on their expectation for inherent safety in the Risk Management Planning regulation. When EPA promulgated the RMP rule, some commenters asked EPA to require facilities to conduct "technology options analyses" to identify inherently safer approaches. EPA declined to do so, stating that "PHA teams regularly suggest viable, effective (and inherently safer) alternatives for risk reduction, which may include features such as inventory reduction, material substitution, and process control changes. These changes are made as opportunities arise, without regulation or adoption of

completely new and unproven process technologies. EPA does not believe that a requirement that sources conduct searches or analyses of alternative processing technologies for new or existing processes will produce additional benefits beyond those accruing to the rule already. (FR, 1996[12])

4. IS means different things to different audiences - One person's opinion of IS is not another person's necessarily, and as a result risks could be simply transferred to others.

5. Macro v. Micro benefit – If IS regulations encourage individual plants to take the most inherently safe position to them, that is not necessarily the most inherently safe (or secure) position for the community they operate in thereby potentially increasing the societal risks. A common example is that of transportation risk, where the increased number of transits caused by lowering the onsite volume of a required feedstock increases the number of transits through the communities in the distribution chain. In addition, though, is the prospect that the total societal risk from a wide collection of inherently safer individual decisions leads to a redistribution of risk across the country – the analog of squeezing a balloon.

6. Economic Security - Another example of this concern is the possible lack of appreciation of the economic security of the chemical infrastructure in legislative discussions on inherent safety. At a national, state or local level, the economic impacts of an attack or disruption of the chemical infrastructure should be a key concern. If the plant is disabled for any reason, such as a distribution chain disruption, the lack of inventory may make the plant inoperative for a longer period of time than if it had accumulated and secured supplies necessary to function. It is more likely that plants will face supply issues due to natural or manmade disasters than be attacked and so the macro view of homeland security is compromised at the expense of a local viewpoint. These goals need to be balanced from a risk perspective with other hazard reduction goals.

Recommendations

Rather than attempt to regulate a vague and creative safety concept for chemical security, it should be left to industry and government to work together to consider the full spectrum of available security risk management strategies and to meet performance standards for security based on site specific needs. Inherent safety should not be seen as the most important strategy to implement. Risk should be the measure of security preparedness given consequence, vulnerability, and threat considerations.

References

1. Center for Chemical Process Safety (CCPS) (1993). *Guidelines for Engineering Design for Process Safety*. New York: American Institute of Chemical Engineers.

2. Hendershot, Dennis C., “Chemistry - The Key To Inherently Safer Manufacturing Processes”, Presented Before the Division of Environmental Chemistry, American Chemical Society, Washington, D. C. August 21-25, 1994, Paper No. ENVR-135.

3. Mansfield, D., Y. Malmen, and E. Suokas (1996). "The Development of an Integrated Toolkit for Inherent SHE." *International Conference and Workshop on Process Safety Management and Inherently Safer Processes*, October 8-11, 1996, Orlando, FL, 103-117. New York: American Institute of Chemical Engineers.

4. Gentile, M. and M.S. Mannan, "Development of an Inherent Safety Index Using Fuzzy Logic,"*Proceedings of the 4th Annual Mary Kay O'Connor Process Safety Center Symposium - Beyond Regulatory Compliance: Making Safety Second Nature*, College Station, Texas, October 30-31, 2001, pp. 510-526.

5. Mannan, M.S., "Challenges in Implementing Inherent Safety Principles in New and Existing Chemical Processes," White Paper, Mary Kay O'Connor Process Safety Center, College Station, Texas, August 2002.

6. Kletz, Trevor, “Green Intention, Red Result”, IChemE, Symposium Series No. 147., 2000

7. Environmental Protection Agency (EPA) (1996). "Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act Section 112 (r) (7)." *Federal Register* 61, 120 (June 20), 31668-730.

8. 61 Fed. Reg. 31699 (June 20, 1996).

9. Hendershot, Dennis C., “Putting Inherent SHE on the Map in the USA” , For presentation at the Conference on Inherent SHE: The Cost Effective Route to Improved Safety, Health and Environmental Performance London, 16-17 June 1997.

10. Mannan, M.S., W.J. Rogers, M. Gentile, and T.M. OConnor, "Inherently Safer Design: Implementation Challenges Faced by New and Existing Facilities," Hydrocarbon Processing, vol. 82, no. 3, March 2003, pp. 59-61.

[1] Guidelines for Managing and Analyzing the Security Vulnerabilities of Fixed Chemical Sites, American Institute of Chemical Engineers, August 2002

[2] "Security Vulnerability Assessment for the Petroleum and Petrochemical Industries", American Petroleum Institute, August, 2004.

[3] Moore, David A., "Experiences in the Regulation of Inherent Safety", Mary Kay O'Connor Process Safety Center, Texas A&M University System, 2002 Annual Symposium, Beyond Regulatory Compliance, Making Safety Second Nature, October 29 - 30, 2002, College Station, Texas.

[4] Bollinger, R. E., D. G. Clark, A. M. Dowell, R. M. Ewbank, D. C. Hendershot, W. K. Lutz, S. I. Meszaros, D. E. Park, and E. D. Wixom (1996). *Inherently Safer Chemical Processes: A Life Cycle Approach*, ed. D. A. Crowl. New York: American Institute of Chemical Engineers.

[5] Center for Chemical Process Safety, Inherently Safer Chemical Processes: A Life Cycle Approach, Center for Chemical Process Safety, AIChE, 1996.

Collins Bill, Chemical Security Act of 2005,

[7] Environmental Protection Agency (EPA) (1996). "Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act Section 112 (r) (7)." *Federal Register* 61, 120 (June 20), 31668-730.

[8] Moore, David A., "Experiences in the Regulation of Inherent Safety", Mary Kay O'Connor Process Safety Center, Texas A&M University System, 2002 Annual Symposium, Beyond Regulatory Compliance, Making Safety Second Nature, October 29 - 30, 2002, College Station, Texas

[9] Center for Chemical Process Safety (CCPS) (1993). *Guidelines for Engineering Design for Process Safety*. New York: American Institute of Chemical Engineers.

[10] Mannan, M.S., "Challenges in Implementing Inherent Safety Principles in New and Existing Chemical Processes," White Paper, Mary Kay O'Connor Process Safety Center, College Station, Texas, August 2002.

[11] Environmental Protection Agency (EPA) (1996). "Accidental Release Prevention Requirements: Risk Management Programs Under Clean Air Act Section 112 (r) (7)." *Federal Register* 61, 120 (June 20), 31668-730.

[12] 61 Fed. Reg. 31699 (June 20, 1996).