# Integrating safety and security systems at chemical facilities

Mohamed A. Hashim[1], Galal A. M. Awadh,
Badr I. Abdul Razzak[2],Mohammed A. Ghalib

**Abstract**

Vulnerability of chemical plants has always been a matter of concern to society and industry. Such vulnerability makes it imperative to control hazardous situations which origin could be intentional or not. This paper discusses hazard control at chemical facilities from both a safety and security perspective and introduces the concept of integrated safety and security systems and its applicability at chemical facilities.

**Introduction**

In the past decade the concept of safety has expanded beyond safe production of chemicals to include security (1). While safety evolved on a regular basis with events like the Bhopal tragedy triggering major changes and more systematic approach to minimise risks, on the other hand security of chemical facilities came in the forefront only after the 9/11 event with new challenges. Security concerns have shifted from internal security to thinking about threats from external sources to assure business continuity, to minimize impacts in the event of an attack and to make sure the surrounding community is safe. The new reality of the post-9/11 world has given momentum to industry and government initiatives aimed at enhancing the security of industrial facilities such that non-traditional threat scenarios for physical plant security as well as cyber security are now considered. The most appropriate and practical approach is to integrate safety and security management systems as both systems have been found to be compatible to a large extent. The goal of an integrated safety and security system is to enhance both aspects to match the increased risk levels of a chemical plant. Moreover, it ensues that safety and security are managed at both managerial and engineering levels under a proper framework which also include control and continuous improvement mechanisms. In the following sections the various aspects of safety and security are discussed, the functionality of an integrated system is brought forward and specific applications in the

[1] ) ***Faculty of Agriculture, Plant Protection Department, University of Sana'a, Sana'a Yemen***
[2]**) *Faculty of Education, Chemistry Department, University of Hodeidah, Hodaidah, Yemen***

chemical industry are elaborated. Finally, major hurdles encountered in integrating safety and security systems are outlined (2).

**Safety v/s Security**

Though a first impression may lead to believe that safety and security are related, a closer look will show that both terms have different meanings and the approach when dealing with safety and security also differs. CCPS (2000) defines safety risks as "a measurement of injury, environmental damages, or economic losses in terms of the likelihood of incidents and the extent that the instances cause injuries or loss." A safety risk is more or less related to an "accidental" event while a security risk has an "intentional" connotation. Security risks are considered to be qualitative expressions and they differ greatly from safety risks. A definition for a security risk is "the likelihood that a threat will cause an exploitation or specific type of vulnerability to a particular target or targets to cause a specific type of consequence" (CCPS,2003).

In terms of risk assessment the approach also differs such that when carrying out a safety assessment the risk is based upon the probabilities and consequences. However, for a security vulnerability assessment threats will be detected and evaluated by utilizing vulnerabilities, consequences, and the attractiveness of the specific target (3). Both approaches will yield either complementary or different risk mitigation measures to be taken with regards to safety and security. A comparison on risk assessment for safety and security is shown in table 1.0.

| **Risk Assessment** | |
|---|---|
| **Safety** | **Security** |
| **Hazard Identification:**<br>Data available<br>Hazard Identification tools available<br>Methodical | **Threats Identification:**<br>Data may not be available<br>Relies on intelligence / national threat levels<br>Varies with time and geopolitical situations |
| **Probability:**<br>Based on experience/past events<br>Reliability data | **Probability:**<br>Unknown |
| **Vulnerability:**<br>Not assessed (considered in hazard identification) | **Vulnerability:**<br>Assessing the strength/weakness of a plant and the corresponding protection level. |
| **Consequence Analysis:**<br>Identifies real and worst case scenarios | **Consequence Analysis:**<br>Identifies only worst case scenarios |

**Table 1.0: Summary of Comparison between Safety and Security Risk Assessment**

To ensure a consistency in the implementation of safety and security systems an integrated approach is recommended as it will provide cost efficient solutions and ensure that safety and security interact smoothly, due priority is given to both to ensure a balanced approach.

**Security vulnerability analysis (SVA)**

During the recent years various methodologies were developed to assess the vulnerability of chemical plants that may come under a terrorist attack. Many large facilities and various trade organizations have developed their own SVA programs (4). A complete security vulnerability analysis includes a review of information about the facility including site security, the surrounding community, neighbouring facilities, existing site facilities, employees, visitors/contractors, the chemicals used at the site, and how chemicals are stored and used. A SVA tool is aimed at assessing security risks of a chemical facility based upon potential threats and vulnerabilities, the probability of a successful attack occurring, and the severity of consequences resulting from a successful attack. The SVA also includes appropriate safety and emergency response measures that could prevent or mitigate the consequences of an attack and provide valuable insight into level of protection required. Any site vulnerability assessment will ultimately lead to a site security plan with all aspects of security covered.

A typical weakness to most security plans is the lack of a comprehensive risk and vulnerability assessment and most only address security from an electronics systems perspective (access control, CCTV, automated gates etc.). Some definitions related to site vulnerability assessment:

***Consequence analysis*:** consequence analysis identifies the worst reasonable consequences that could be generated by specific threat scenarios. Both causality and financial impacts resulting from different damage scenarios are estimated and ranked on a standard consequence scale.

***Vulnerability analysis*:** vulnerability analysis seeks to determine the strength or weakness of targeted asset and inherent protective systems to a specified threat. This involves analyzing the existing capabilities and countermeasures at the asset or entire facility, and their effectiveness in reducing the overall vulnerability to the threat scenarios evaluated.

***Threat assessment***: a threat assessment comprises of two analyzes, one performed by the asset owner and one performed by government. In this step, the asset owner is limited to an assessment of their facility/asset attractiveness.

***Risk assessment***: security risk can be estimated by considering the analysis and aggregation of consequence, vulnerability and threat. The owner/operator risk assessment creates a foundation for selecting strategies and tactics to defend against terrorist attacks by establishing priorities based on risk.

***Risk management***: risk management is the deliberate process of understanding risk and deciding upon and implementing action (e.g. defining security countermeasures, consequence mitigation features etc.) to achieve an acceptable level of risk at an acceptable cost. Risk management is characterized by identifying, evaluating, and controlling risks to a level commensurate with an assigned or accepted value.

**Safety Risk Assessment**

Risk Assessment, the process of evaluating the risks to safety and health arising from hazards at work, forms an integral part of the Occupational Safety and Health Management System, whereby all hazards are identified and evaluated taking into consideration existing control measures. The exercise is carried out by competent persons in the field. The ultimate aim is to eliminate or minimise risks at work through tightening of control measures. Such risk assessments are backed by available safety, probability and reliability data to facilitate decision making.

Generally safety risks assessments are focused on workplace hazards but has been expanded to include a wider off site consequence analysis for public safety as is the case for major hazardous installations (commonly referred to as Seveso sites). It is observed that the SVA adopts a similar approach as for safety risk assessment but contains more unknown variables. However, emergency planning and response occur at the same level. Safety management is geared towards:

(i) **Prevention** by using inherently safe design methods;
(ii) **Control** by including primary response systems;
(iii) **Mitigation** by using secondary response systems to limit impact and;
(iv) **Buffer** by isolating facilities away from populations.

Some Definitions:

***A Hazard***: A hazard is ‘an inherent physical or chemical characteristic that has the potential for causing harm to people, property, or the environment’. In chemical processes, ‘It is the combination of a hazardous material, an

operating environment, and certain unplanned events that could result in an accident'.

***Risk:*** 'Risk is defined as the combination of the severity and probability of an event. Risk can be evaluated qualitatively or quantitatively.

***ALARP:*** The Alarp (as low as reasonably practicable) principle recognizes that there are three broad categories of risks:

• *Negligible risk:* Broadly accepted by most people as they go about their everyday lives, these would include the risk of being struck by lightning.

• *Tolerable risk:* We would rather not have the risk but it is tolerable in view of the benefits obtained by accepting it. The cost in inconvenience or in money is balanced against the scale of risk, and a compromise is accepted.

• *Unacceptable risk:* The risk level is so high that we are not prepared to tolerate it. The losses far outweigh any possible benefits in the situation.

**Reducing the Risk**

Chemical manufacturing facilities represent a real threat for a terrorist attack (5),(6). Such facilities routinely process materials that are toxic, flammable, explosive, volatile and sometimes manufactured under extreme temperature and pressure conditions. These facilities are often sited near inhabited areas and provide an attractive target for wrong doers. Furthermore, the relatively low security control available can also increase the attractiveness of these sites. So far the industry has no means to prevent an attack and can only rely on the authorities. However, industry may apply existing safety risk mitigating tools to mitigate or even eliminate security risks. Safety and security can be integrated at different levels of a plant operation starting from its design to its operational and management systems. In both cases risk reduction options should guarantee a ''performance'' in favour of the ALARP approach (As Low As Reasonable Practicable) (7).

**Design Based Security and Safety**

Hazard avoidance is better than hazard control. Hence, inherently safer designs avoid hazards altogether, instead of simply controlling the hazard from occurring. A chemical plant should be designed to prevent the possibility of hazardous events. This can be done specifically by reducing the amounts of dangerous substances and the numbers of hazardous operations within chemical plants (Herndershot, 2010). Inherently safer design can be broadly classified but not limited to the following concepts:

**(I) Intensification**

Process intensification refers to minimisation of hazardous chemical in the plant. This includes reduced inventories, generate "just in time", avoid long storage times in reactors, change from high volume batch reactors to continuous (e.g plug flow) reactors, minimise piping.

**(II) Substitution**

Replace hazardous substances with safer materials. Substitution might not be applicable in all cases as most of the time quality of product dictates the process. However, common substitutions include the use of water based solvents in place of organic solvents, use of cyclohexane in place of benzene, use of membrane technology for separation processes, low toxicity reactants and solvents, use catalysts etc.

**(III) Attenuation**

Attenuation refers to the use of hazardous materials under the least hazardous conditions. Process parameters like temperature and pressure may be lowered if possible, use of gravity or differential pressure in process to transport unstable material, refrigerated storage instead of pressure storage

**(IV) Limitation**

Limitation changes designs or conditions to reduce potential effects. This includes smaller diked areas around storage tanks, favour single stage reactors in lieu of multistage reactors, mounded storage, segregate reactive chemical, increase safety distance from sensitive areas, proper plant layout to avoid domino effects etc.

**Simplification**

Simplification reduces complexity to reduce the opportunity for error and can be achieved by using resistant materials such as inox, eliminate extra equipment, minimize number of control loops etc.

Inherently safer design is also supplemented by:

- Control Systems
- Alarms and Interlocks
- Shutdown Systems
- Protection Systems and Devices / Fail safe design
- Response Plans

Since the inherently safer design method covers all aspects of a chemical plant in a holistic way it will not only yield an immense amount of benefits and be cost-efficient, but it will also ensure that plants are more secure, leading to secure chemical operations. When applying inherently safer design principles both intentional and non intentional disasters are able to be prevented in a cost-effective mannerism.

**Hazard Analysis and Security**

Several hazard analysis techniques are available to identify and evaluate hazards from a safety perspective (8). However, these tools can also be adopted for a security review. Basically, the hazard analysis techniques make an important distinction between two basic approaches. These are called deductive and inductive.

In the **deductive** method the final event is assumed and the events that could cause this final event are then sought. A good example of a deductive method is Fault tree analysis or FTA. The technique begins with a top event that would normally be a hazardous event. Then all combinations of individual failures or actions that can lead to the event are mapped out in a fault tree. This provides a valuable method of showing all possibilities in one diagram and allows the probabilities of the event to be estimated. Deductive methods are useful for identifying hazards at earlier stages of a design project where major hazards such as fire or explosion can be tested for feasibility at each section of plant. It's like a cause and effect diagram where you start with the effect and search for causes.

So-called 'what if' methods are **inductive** because the questions are formulated and answered to evaluate the effects of component failures or procedural errors on the operability and safety of the plant or a machine. For example, 'What if the flow in the pipe stops?' This category also includes (9)

• Failure Mode and Effects Analysis or FMEA

• Hazop studies

These techniques are becoming increasingly popular in security risk assessment as they provide a logical reasoning sequence for determining causal factors, initiating events and their consequences. These techniques may be carried out concurrently with a security vulnerability assessment and the findings would complement the assessment by identifying safety/security loop holes. These methods are shown in table 2.0.

| Name of Method | Method | Advantages | Disadvantages | Security Application |
|---|---|---|---|---|
| Preliminary Hazard Analysis (PHA) | Inductive. Used at design stage | Detection of hazards at design stage.<br>Allow protection systems to be designed in Economical | It is based on experience<br>It is not systematic<br>Applies when there is limited information | Security related hazards may be included Protection system designed |
| Hazop | Inductive. Structured analysis tool | Systematic<br>Provides high level of confidence in detection of hazards.<br>It can analyse a combination of failures<br>It provides an insight into operability features | Need moderate level of skill Time consuming and costly | May include sabotage (process change) |
| What if analysis | Deductive | Fast<br>Can analyse a combination of failures<br>Flexible<br>Low skill level | It is based on experience<br>It is not systematic | Threats may be considered |
| Checklist | Deductive | Fast & easy | All hazards must be included | To check security compliance |
| Fault Tree Analysis (ETA) | Inductive. Structuring the consequence back to the causes | Graphical view of the causes and effects<br>Good for quantifying risks and seeing the primary predominant causes | Not suitable for initial identification of hazards<br>Not structured | Scenarios may be security related |
| Failure Mode and Effect Analysi (FMEA) | Deductive method. Starts with components of system or process and presumes failures<br>Hazards are deduced from result | Good for complex equipment | Not suited to processes because deviations and hazards may not be due to any failure of components | Consequence of a sabotage |

**Table 2.0:** Plant functioning and management.

The results of PHA, HAZOP, What-If, ETA, FMEA or checklist analyses will also provide an indication of how well the engineering aspect of the plant is functioning and managed. The level of thought for engineering effort for both process safety and security concerns will be demonstrated. Furthermore, these analyses will highlight areas where a particular facility production may be vulnerable (10). This may be particularly important where subversive or militant public or internal labor unrest may be suspected. Since these reports may provide indications of key vulnerability points in the process, suitable controls on the distribution of the information of the report are necessary in these instances.

**Layers of Protection Analysis (LOPA)**

Another tool for safety risk assessment is the Layers of Protection Analysis (LOPA). A layer of protection analysis (LOPA) is a powerful analytical tool for assessing the adequacy of protection layers used to mitigate process risk. LOPA builds upon well-known process hazards analysis techniques, applying semi-quantitative measures to the evaluation of the frequency of potential incidents and the probability of failure of the protection layers.

Layers of protection analysis (LOPA) is a semi-quantitative methodology that can be used to identify safeguards that meet the independent protection layer (IPL) criteria established by CCPS1 in 1993. While IPLs are extrinsic safety systems, they can be active or passive systems, as long as the following criteria are met:

***Specificity:*** The IPL is capable of detecting and preventing or mitigating the consequences of specified, potentially hazardous event(s), such as a runaway reaction, loss of containment, or an explosion.

***Independence:*** An IPL is independent of all the other protection layers associated with the identified potentially hazardous event. Independence requires that the performance is not affected by the failure of another protection layer or by the conditions that caused another protection layer to fail. Most importantly, the protection layer is independent of the initiating cause.

***Dependability:*** The protection provided by the IPL reduces the identified risk by a known and specified amount.

***Auditability:*** The IPL is designed to permit regular periodic validation of the protective function.

Examples of IPLs are as follows:
• Standard operating procedures,
• Basic process control systems,
• Alarms with defined operator response,
• Safety instrumented systems (SIS),
• Pressure relief devices,
• Blast walls and dikes,
• Fire and gas systems, and
• Deluge systems.

The applicability of LOPA for security protection is obvious. It provides a proper tool for the identification and evaluation of protective security and safety systems at a chemical facility. The layers of protection also bring forward the level of risk in a plant in a real case scenario. It provides valuable information for emergency planning especially when evacuation of inhabited areas may become a concern following an unwanted incident related to either safety or security. Failures of the independent layers of protection will help emergency responders anticipate new scenarios and hence decide upon the best option to adopt to deal with the situation (fight or flight).

**Standard Operating Procedures**

Standard operating procedures (SOPs) form an integral part of the chemical industry. SOPs contain all procedures for the safe running of a chemical plant and are crucial for safe conduct of operations. Typical SOPs relate to plant start up, normal shut down and emergency shut down. Actions required to address abnormal situations are also mentioned. The SOP normally form part of a larger safety management system. This provide an ideal medium to include security related procedures since there will be a safety and security interface that will prevent any confusion as when both are separate. Hazard control procedures such as

(i) Safe work permits
(ii) Lock out/ Tag Out (sensitive electric panels, valve locks etc.)
(iii) Confined space entry

also provide opportunities to prevent security threats if strictly applied in the plant as authorisation and control of hazards are the basis of these permit systems.

**Chemical Storage and Transport**

Security should be a priority for all chemical storage areas. Security is required and is essential for many reasons. First, basic chemical inventory and management principles require secured storage. Therefore access to chemical storage sites must be controlled and monitored. Second, unrestricted access can result in people placing chemicals in the store room in the wrong, incompatible location, which can increase the danger of an accident in the chemical storage area. Lastly, chemicals represent feedstocks or source materials for illegal activities such as illicit drug manufacturing, bomb making, etc. Unrestricted access can result in pilferage and increased liability (11). Fortunately, dictated more for economic reasons than for security reasons, most chemical industries maintain a good record on the flow of materials in and out their warehouses. However, traceability of sensitive chemicals delivered in bulk amounts need to be improved.

**Security Management Systems**

The ultimate responsibility for the safety and security of a facility lies with senior management. A company's senior management should therefore ensure the appropriate process hazard or vulnerability analysis reviews are undertaken. Management should fully realize that monetary commitment (manpower and financial expenditures) are required to initiate, perform, and follow up the review. Hence, it is important that the company have a security policy to communicate its commitment to security to all stakeholders.

Management should acknowledge the risk results of the process hazard or vulnerability analysis reports and ensure action is taken in accordance with the company's policy. Such findings should be reflected in the site security plan and approved by management. Presently, most corporations have adopted EH&S management systems. The efficiency and effectiveness in managing EH&S functions, their integration with new security systems, and their link to well established quality practices have become very important in improving a company's business operations and reducing the cost of production.

Standards that may be used as guides to establish an integrated environment, health, safety and security at chemical facilities include, but are not limited to, Occupational Safety and Health Administration's (OSHA) "Process Safety Management of Highly Hazardous Chemicals Standard" (the PSM standard) and"Voluntary Protection Program" (VPP), and the

Environmental Protection Agency's (EPA) "Rule for Risk management Programs for Chemical Release Prevention" (the RMP rule).

A well-designed and managed EHS&S management system is one of the best proactive protection systems since it:

• empowers employees through training,
• enables observation and resolution of issues in a timely manner,
• reflects up-to date information,
• brings-out new sources of problems to management's attention,
• provides an invisible control over all operations at every stage of a plant's life.

Finally, using an integrated tool for the proactive management of safety, health, environment and security would make the work load of EH&S professionals much more efficient and manageable.

**Challenges**

Integrating security and safety in a chemical facility is a complex and challenging task. It is impacted by regulations, chemical properties and reactivities, storage and process conditions and control measures available. Furthermore, the cost and services involved may be extensive leading to little motivation in the industry for implementation. There is a feeling that security is a waste of resources and only a government problem. Hence there is a need to sensitize the industry on the benefits that accrue from having a security and safety management system. Integration of safety and security can only become possible if spearheaded by government by providing the necessary regulations, standards, assistance, proper framework and incentives to industry.

**Conclusion**

The chemical sector is comprised of various facilities, that all come with their own sets of risks. Safety and security use a similar mechanism that is risk based, to address safety and security. Furthermore, various hazard evaluation techniques applicable for safety risk assessment can be applied proactively to deal with security related issues. This helps in the prevention of chemical disasters. Finally, by integrating safety and security within the processing and chemical industries, secure and safer chemical industrial parks and chemical plants can become a reality.

## References

(1)- Bill Lessig, Chemical Facility Integrates Security and Process Control to Reduce Risk and Increase Safety, (Honeywell Specialty Materials, Geismar, 2005), 2-3.

(2)- Keith Stouffer, Joe Falco, Karen Scarfone, Guide to Industrial Control Systems, (National Institute of Standards and Technology, June 2011), 3-8.

(3)- Security Aspects of Uni- and Multimodal Hazmat Transportation Systems (Holtrop & Kretz, 2008).

(4)- Security Guidelines for the Petroleum Industry, April 2005.

(5)- Lisa Gilbert, Chemical Insecurity, U.S PIRG, Federation of State PIRGS (Washington: Public Interest Research Group, 2010).

(6)- Tom Coburn, *Chemical Insecurity*: *An Assessment of Efforts to Secure the Nation's Chemical Facilities from Terrorist Threats*, U.S Senate, Homeland Security & Govt Affairs Committee. Retrieved on October 24, 2014.

(7)- *So What is ALARP*, Risktec Solutions Limited, Issue 4 (Autumn 2003) Retrieved on October 22, 2014.

(8)- Tom Anderson, Rogério de Lemos, and Amer Saeed, "Analysis of Safety Requirements for Process Control Systems", Predictably Dependable Computing Systems (Springer Berlin Heidelberg, 1995), 27-40.

(9)- An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems, *Risk and Safety Working Group (RSWG)*, GEN International Forum, Version 1.1 (June 2011), 33.

(10)- Dennis P. Nolan, Safety and Security Review for the Process Industries: Application of HAZOP, PHA, What-IF and SVA Reviews (Waltham: Gulf Professional Publishing, 2012).

(11)- Frank R. Spellman and Revonna M. Bieber, Chemical Infrastructure Protection and Homeland Security (Lanham: Government Institutes. 2009), 71.