CHAPTER 1

INTRODUCTION TO SECURITY RISK ASSESSMENT AND MANAGEMENT

INTRODUCTION

This course was developed out of a training outline and the course Col. Arlow and I taught together in Manama, Bahrain. Pieter’s background is South African Defense Force, and he was responsible for the security of the World Cup in 2011. Dave’s background is civilian, industrial chemical, and environmental consulting. Together, we believe that this book will provide a different and practical approach that combines security theory with practice. We hope that it is not just another book that is put on the shelf and used occasionally, but read and considered, and one where our suggestions are put into place.

Security is not just one group’s business; it is everybody’s business. The combination of security, safety, and environmental protection are critical to the operation of a modern-day chemical or industrial plant. Despite the heightened focus on security by the US Department of Homeland Security and Transportation Security Administration, in many instances, it amounts to little more than a theater of the absurd because the United States is only marginally more secure and it is more a chance of luck than of their expensive, large, and restrictive efforts to increase travel security in particular and homeland security in general. Paperwork does little to provide security.

BUSINESS DEFINITION

The business definition of security is quite straight forward. Webster’s Dictionary provides us with the basis for security: “freedom danger, risk of loss, and trustworthy and dependable.” That is a very good start. The definition of security crosses a number of lines in the modern industrial plant and has many different definitions. Plant security can be anything from the guard force who keeps out the unwanted intruders to the executive protection service and to the corporate watchdog that looks after the financial and corporate affairs of the plant or the corporation to make sure that there is no theft or leaking of secrets at the highest level of the company.
With the advent of the Internet and the digital age, the job of security has been made, if anything, tougher because of the ease of communications and the proliferation of digital devices and the Internet. The communication is much easier, but then so is the ability to penetrate networks and obtain information or compromise security systems in a variety of ways. One has to look no further than the Stuxnet virus and how it delayed the development of the Iranian atomic program by attacking the centrifuges needed to refine the uranium. The success of the virus/worm delayed the development by up to 2 years.

SECURITY VERSUS RISK

In order to get a better working definition of security, we should also have a working definition of risk. Risk is the chance of loss or injury. In a situation that includes favorable and unfavorable events, risk is the probability of an unfavorable event or outcome. We measure risk by examining the certainty that a particular bad outcome or outcomes will occur.

Risk comes in many forms. There is financial risk, enterprise risk, risk of self-organized criticality (failure), risk of injury, internal risk (theft, fire, economic loss, etc.), industrial/jurisdictional risk, operational risk, and several other types of often unforeseen and uncontrollable events that create damage. Within the various operations of a corporation, many of these have specific departments to address those risks. For example, safety, health, and environmental departments address specific risks for worker safety and environmental contamination; the IT security department manages risk for intellectual- and computer-related data. We are more concerned with the risks associated with external events such as terrorism, earthquakes, tornadoes, fire, etc. These are external risks. Internal risks might include sabotage and plant accidents resulting in fire, spills, explosion, etc.

Within the scope of plant security, one is primarily concerned with events that are external to or imposed upon the plant, natural occurrences, and man-made occurrences, some of which are preventable and others not. Our working definition will include such elements as terrorism, external attacks, naturally occurring events such as tornadoes and hurricanes, and some limited scenarios for sabotage. Events such as spills, fire, and accidents may be equally unpredictable, but they are often addressable by proper design of facilities, installation of engineering controls, and management of personnel through procedures and training. Logically, we must also look into some of the process control and operational functions as a modern plant uses a variety of computer and wired and wireless control systems that are often open to sabotage or external influences.

FRAMEWORK FOR RISK MANAGEMENT

The basic framework for risk management is a cost-associated function where the general sequence starts with identification of the assets at risk, evaluation of the likelihood of their occurrence, development of a cost and a probability associated
with the occurrence of an attack or an event, and estimation of the costs to reduce the risk to manageable levels. This is a cyclic process, illustrated by Figures 1.1 and 1.2. We measure and estimate the cost of a particular event occurring so that we can provide a financial plan for the plant or facility. We develop scenarios and the cost of those occurrences. For example, if we assume an attack by a hostile force, we try to estimate the damage and costs associated with that attack. We may create several scenarios and the associated costs. Things like standoff weapons such as a grenade launcher, a rocket, or a bazooka might have a damage level (cost) of C1 for the first scenario, C2 for the second scenario, etc. C1 might be for a mortar. C2 might be for a car bomb. The objective is to make these scenarios as realistic as possible when one views the likelihood of the attack.4

An attack can be any unplanned event and is subject to wide interpretation. Natural meteorological events can be an attack. So can an intruder into the plant. Terrorism is an attack, but then so is a civil unrest. Sabotage is a type of attack, but it is special and separate because it is imposed internally rather than from outside. However, a good risk management plan may want to consider sabotage as an element of a response plan.

Once we have a range of costs and scenarios, we can begin to determine the risk based on the probability of the events. This is often the most difficult and controversial part of the exercise because different assumptions on the likelihood of the event can produce dramatically different outcomes and costs. This is also complicated by the prospect of expenditures for increasing security and estimates as to how much specific improvements will reduce risk.

Just because a plant has not had an electronic intrusion (which they know of) does not mean that one will not happen tomorrow. Similarly, adverse weather events...
may have a record going back 30 years or more with no incidents, but that does not prove anything except that nothing has happened in that time period. History is often a very poor predictor of future events, and one needs to be careful about piling assumptions upon assumptions when and where events occur. The concept of a “once in 100-year storm,” popular in flood prediction and rainfall frequency analysis and other similar events, does not mean anything, except that the event was not expected with high frequency. Two of those events could occur back to back in subsequent days.

In some cases, the risk assessment is relatively easy with probabilities in the percentile ranges $P=1\%$ ($P=10^{-2}$), while in many other cases, the probability of an event is on the order of 0.0001% ($P=10^{-6}$) or even less. When estimated costs and damages are high, in the millions of dollars, we have a challenge multiplying a very small probability by a very big cost. Added to this is the idea that costs are ever increasing, and the range of uncertainties is dependent upon a partial or limited database.

Fundamental to the understanding of risk are the concepts of vulnerabilities, assets, and threats. Those three components come together to form the basis for risk.

Assets are the physical structures, the data, the production, the inventory, and almost anything that has a value. Vulnerabilities are the possible methods of

---

**Figure 1.2** A second view of the risk analysis process. The risk analysis matrix is usually in color. Red indicates high risk, yellow indicates moderate risk, and green indicates lower levels of risk, but we have chosen to use stripes, dots, and white spaces to highlight the risk levels, respectively.
degrading or devaluing the assets. It is often helpful to think of vulnerabilities as the
means that threats can accomplish the damage. Threats are the possible events that
acting through the vulnerabilities can degrade or destroy the assets. The conjunction
of all three is the risk. A word picture might help explain the concept.

A threat could be a terrorist attack by mortar or grenade or car bomb, or infiltr-
tation, or sabotage. The vulnerability might be that the main processing reactor at
the facility would be damaged and that would lead to an explosion that destroyed
the plant and created a fire in the storage areas, destroying them as well. The assets are
the reactor, the plant, the storage areas, the inventory, and the data and might include
the financial losses due to loss of revenue or accounts receivable from lost produc-
tion. The assets would potentially be in the millions of dollars, but with careful
planning and engineering controls, the assets could be separated to reduce the vulner-
ability on the scenario:

Risk = Threat \times Vulnerability \times Assets \text{ and is expressed in monetary terms}

Or to express risk in another way:

Risk = Threat \times Vulnerability \times \text{current or replacement cost of asset}

The cost of an asset depends upon the accounting method employed and the tax
structure and other variables. Generally, replacement cost for an asset needs to be
updated every few years. The discussion in the following addresses some of this in
very general terms.

If the threat is low and expressed in annual terms, the risk may be a few thou-
sand dollars per year or may be diminishingly small depending upon the statistical
basis employed to calculate the likelihood or probability of the threat. As we go
through this book, we will try to address some of the concerns and attempt to
illustrate methods to reduce the uncertainties using accepted techniques and
statistical methods.

“Traditional” risk assessment programs exist to identify hazards arising
from work activities to ensure suitable risk control measures are in place. However,
incidents continue to happen, either as a result of inadequate risk assessments or
failures in the necessary risk control measures.\footnote{7}

**VALUE AT RISK**

Several of the financial companies tend to look at risk a bit differently. The concept
of value at risk (VaR) has been defined as “the predicted worst-case loss at a specific
confidence level (e.g., 95%) over a certain period of time (e.g., 1 day).” This model
is being used by organizations such as Chase Bank where they take a daily snapshot
of their international trading positions to determine their exposure.

The components of value can include such items as earnings, market, pro-
jected revenue, cash flow, and asset value: in short, everything. With older facil-
ities, which may have been fully or partially depreciated, these items may be of
substantially greater value than the facility itself. It should also be noted that the
VaR needs to be benchmarked against a known quantity. The VaR could be actual
or virtual, and may include project sales growth against a baseline or something
else. The financial management of the corporation needs to be involved in deciding what is the VaR.

For example, if an attack destroys the manufacturing plant causing lost production for the principal product, the VaR might include the replacement cost of the facility, plus the value of the lost market position (sales and revenue) and lost contracts. The inclusion of these other elements in the VaR will inflate the apparent replacement costs and could conceivably cause the management of the facility and corporate management to acknowledge the value of the facility in different and perhaps improved terms.

**CALCULATION OF RISK**

There are various methods of calculating the probable risk. Depending upon the accounting and valuation method employed, the risk manager can use linear or nonlinear valuation methods. The methods most commonly used include techniques such as Monte Carlo simulation, parametric simulation, and historical simulation. Monte Carlo methods involved application of statistical parameters and are substantially computer intensive. Parametric and historical simulations use a combination of formulas and may involve case histories for individual cases. In the case of a plant facility, cited earlier, the valuation may require a combination of methods such as Monte Carlo methods for market risk and parametric and historical simulation methods for physical asset risks.9

**RISK ASSESSMENT VERSUS RISK MANAGEMENT**

Risk assessment and risk management are two different things. The former involves a worst-case scenario, perhaps tied to financial programming and projections, while the latter involves preparing action plans, implementing and measuring performance, and proscribing actions and objectives to minimize damage or losses. These management plans can be proactive, based on risk assessments; active, based on safety audits and site inspection; and reactive, based on incident investigation and analysis.

The selection of a particular achievable risk evaluation level is somewhat arbitrary by the plant, but note that it does tie to reality over time. A risk confidence level of 95% would indicate that the company could sustain significant losses once in every 20 days or so. While a 99% confidence interval would indicate a significant loss once every quarter. Obviously, these loss rates are unsustainable when it comes to the physical facility. The projections are more for financial risks and market risks rather than physical risks. Sustainable physical risk rates are on the order of 0.0027% (one loss in 10 years or less), and many facilities throughout the world sustain a physical risk of 0.000059% (one major loss in 30 years) or less. So a combination of loss rates and factors must be used to make an accurate calculation.

Many risks, especially those to the physical plant, are considered insurable. However, many are not. One good example of an uninsurable major risk can be found considering Superfund and CERCLA10 Litigation. The literature and the case law are
rife with cases where the insurance company had to pay for cleanup of sites contaminated by a company, and many of the insurance companies have demanded pollution riders on their policies or have denied claims for damages and cost recovery from past operations. The claims are frequently made based on real or alleged damages to local populations, health effects, and diminished values for property. A number of these claims, however, are based on continuing practices rather than a specific past incident.

At this point, it is also good to consider something else from the financial services industry, stress testing. In the realm of security, the stress test has a physical form. The military uses red teams, groups of individuals who are routinely cut loose from the plant structure with the specific instruction to attempt to penetrate the plant security and organize attempted security breaches and incidents. This can go to the point of planting a fake bomb, penetrating secure areas, spoofing software, and introducing harmless viruses into the operating systems of the plant. These red team activities are limited only by the ingenuity of the persons on the team and the resources available, but they should be coupled with regular drills, especially for the security personnel.

For example, the fire department runs or should run regular drills where they test their response by getting out the hoses and practicing fighting real fires. At airports, the fire companies regularly have drills that use an aircraft shell and douse it in fuel and then practice putting it out. But, there are a number of types of drills that can test the plant security and that may be appropriate. How often do we run spill drills? Similarly, if security is important, how ready is the security force able to respond to multiple incidents such as a fire or a spill and an intruder?

The literature is full of instances where refineries and other facilities with large tank storage have had spills that led to fires and explosions in the tank farms. The point is that industry has regular firefighting drills, but when do they have security and other disaster drills? These are stress tests of the system, and the answer is, unfortunately, not so frequently. People stay sharp when they are challenged and regularly exercised on topics of concern, and increased awareness benefits everyone in the plant.

Note that in some areas, risk prevention may cross over into activities normally considered as the province of plant safety, and vice versa. If an employee is injured on the job or cannot perform his/her function, it does represent a risk to the plant finances. Similarly, the risk of employee theft or asset diversion or sabotage is also a risk. The principal difference between these and some of the previous risk factors mentioned earlier is the idea of preventable risk versus nonpreventable risk. Preventable risk, such as employee risk, is often covered by safety training, procedures, and equipment. Theft, diversion of assets, and financial misappropriation are often covered by corporate security, and in the modern society, the operation and security of the plant’s computers and data are protected by a special function within the information technology department. But, plant security needs a place at the “table” whenever the plant is expanded or when there are major changes to the process equipment to insure that the process is secure from outside intrusion.

Risk assessment of technological processes (chemical, petroleum, power plants, and electromechanical systems) is a complex process that requires enumeration of all possible failure modes, their probability of occurrence, and their consequences. This risk is managed through thorough analysis and technical review and playing “what if” analyses. This type of analysis is also known as HAZOPS.
RISK MANAGEMENT PLANS

We are going to march through some of the theory around risk management and develop a scenario or two and then present risk management analysis. In the following, we will not get into Monte Carlo simulation, which is often the preferred way of performing the risk analysis, but some statistics are inevitable. A good risk management plan has to cover a lot of variables and examine a lot of options. But it starts with an assessment of assets.

The first step is to start with a replacement cost assessment of the facility and its assets. This should include a valuation of the replacement cost for all equipment and might even include the cost of obtaining new or replacement permits for equipment, including such items as air pollution studies, water pollution evaluations, etc. This by itself is going to be a major effort. The risk management department of the company or the insurance provider can provide some guidance and a lot of help.

**Step 1 is to obtain or develop a cost estimate for replacement of the facility.**

The cost estimate should be as recent as possible, but even if it is a few years old, a fairly accurate adjustment can be made from various cost estimating handbooks, and such sources as RS Means, cost estimation, and McGraw-Hill/Engineering News Record's construction cost index. The cost estimate generally should not be any closer than two or three significant figures. Any other level of accuracy is unwarranted. The cost estimate should be broken into as many different significant production units as existing within the plant and should also include the value of associated assets and inventory. The inventory should be broken out separately, because the value of that inventory can change more rapidly than inflation.

*For example:*

It is the total replacement cost for the facility that will serve as the baseline for our assets in the estimation of the risk (Tables 1.1 and 1.2). Oftentimes, the asset analysis for Unit A might look like the following if we assume that Unit A is an ammonia production facility:

> Remember that **Risk = Vulnerability × Assets × Threat**

**TABLE 1.1  Cost analysis for replacement of a chemical plant**

<table>
<thead>
<tr>
<th>Item no.</th>
<th>Description</th>
<th>Original cost (millions)</th>
<th>Replacement cost (2012) (millions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unit A</td>
<td>11.2</td>
<td>22.4</td>
</tr>
<tr>
<td>2</td>
<td>Unit B</td>
<td>3.7</td>
<td>4.1</td>
</tr>
<tr>
<td>3</td>
<td>Raw materials inventory A (current $)</td>
<td>1.1</td>
<td>1.1</td>
</tr>
<tr>
<td>4</td>
<td>Raw materials inventory B (current $)</td>
<td>0.3</td>
<td>0.3</td>
</tr>
<tr>
<td>5</td>
<td>Finished inventory current values A and B</td>
<td>5.4</td>
<td>5.4</td>
</tr>
<tr>
<td>6</td>
<td>Associated buildings and support</td>
<td>3.9</td>
<td>12.0</td>
</tr>
<tr>
<td></td>
<td><strong>Total replacement costs</strong></td>
<td></td>
<td><strong>44.3</strong></td>
</tr>
</tbody>
</table>
The next step is to consider the vulnerability. The vulnerability is dependent upon scenarios, which to some extent depend upon the threats, but the threat matrix needs to be set aside for a little while to develop the vulnerability analysis (Table 1.3).

This type of analysis gives us a baseline for vulnerabilities. Are the numbers rough? Sure. What are other scenarios you would use to develop these loss estimates and methods? The specific vulnerabilities can become quite extensive, and when one considers improvements to the process, the installation of control systems, firefighting equipment, etc. may significantly reduce the vulnerabilities to the plant, and the decision to include existing safety and equipment improvements in the baseline case is valid.

There are a number of vulnerabilities that can lead to subunits of the plant being destroyed or damaged. These are as a part of the whole and will total up to the replacement cost of the plant. These vulnerabilities need to be paired with individual threat pairs to determine the basis for the risk.

**THREAT SCENARIOS**

The scenarios for development of threats are subject to a wide range of occurrences and are often highly subjective. For example, the threats might be earthquake, hurricane, lightning strike, tornado, and terrorism. Some of the threats can be ruled out or assessed as highly improbable because they are statistically insignificant. For example, the threat of a hurricane in Kansas is nil, but tornadoes and lightning strikes and perhaps even earthquakes may be statistically significant.
In the threat analysis, there are a number of significant unknowns, and we do not know what we do not know, and we have to deal with that. It is the unknown that keeps risk managers up at night worrying about the level of threat and how it will be implemented against the assets.

At the end of this chapter, we are presenting a description of a chemical plant and some ideas for improvements that need to be made to eliminate or reduce potential or existing threats. In the scenario at the end of this chapter, the plant is over 40 years old, and a couple of possible threat scenarios are utilized here as examples of the types of incidents that might be used to evaluate specific threats to a plant. The following scenarios should be used with extreme caution as they are specific to an industry and only examples of the types of incidents that might occur. In our scenario, the total list of all things that need to be done is very expensive, but that is not your problem yet. Develop and prioritize the responses from the list and add new ones of your own.

A recent lecture by Kip Hawley, on the Center for Homeland Defense and Security’s website (www.chds.us) pointed to an alternative model for threat analysis—Inside Out Analysis. The scenarios were based on the analysis of the Underwear Bomber who concealed explosives in his underwear and attempted to destroy himself and the plane he was flying in on December 25, 2009. That led to an reexamination of risk thinking to consider Worst Case Scenarios (or How bad could it possibly be or get?), and then plan layers of prevention toward setting up barriers against that possibility. That type of analysis is certainly appropriate in the examples and should be considered as the ultimate for response scenarios.

For example, what would happen if due to a series of catastrophic internal failures, the plant disappeared in a massive internally caused explosion which not only resulted in the deaths of critical employees but caused secondary explosions and fires and spills which led to community contamination and evacuations? Are these scenarios likely, maybe not, or even possibly not, but then that was the type of thinking which led to Buncefield, Bophal, Chernobyl, Sevesto, and the BP Texas City Disasters. The impossible is not necessarily impossible, only highly improbable. We need to consider that type of planning in our analyses.

STATISTICS AND MATHEMATICS

An aside is pertinent here. The statistics for prediction of the frequency of certain events involve fractal mathematics, and they can get somewhat involved, as the frequency follows a power curve. The events are scalable but the actual frequency of occurrence is difficult to predict. Few, if any, incidents give a warning that they are going to occur. The exception to this is hurricanes and cyclones, where the science of forecasting has enabled reasonably accurate prediction. Tsunami forecasting may provide only a few hours of warning. Earthquakes, plant accidents, and terrorist attacks cannot be predicted with any precision. Self-organized criticality is its own problem within a plant.

Dr. Ted G. Lewis, director of the Naval School of Homeland Security, has written an excellent paper on the probable loss and the frequency of occurrence. In “Cause-and-Effect or Fooled by Randomness,” he discusses self-organized criticality and relates the possibility of a successful terrorist incident to a power law
function that has an expression of Probability of Exceedence $= x^{-q}$ where $x$ is the relative severity of the incident and $q$ is an experimentally determined exponent. Figure 1.3 is a reconstruction of some of his data from his paper. Unfortunately, the paper only has data on deaths from a terrorist incident and not financial losses.

An example calculation is that in an earthquake the probability of exceeding five deaths is approximately 50%, while the probability of exceeding five deaths from a terrorist incident or an airline accident is less than 10%.

**PAIRING VULNERABILITY AND THREAT DATA**

Vulnerability and threat data must be paired. There are several methods of doing that, which will be discussed in the following. The best approach for setting priorities and determining threats and vulnerability is similar to the “what if” process used by
OSHA in preparing HAZOPS. This vulnerability and threat assessment team takes a good look at the community and the surroundings and the facility. Law enforcement and perhaps military should be included in the team, along with the engineering, accounting, and security personnel from the plant. The working framework will be a group output that will identify the assets (as we have done previously), combined with an analysis of the specific vulnerabilities and the methods of attack. (Note that we are differentiating “attacks” from “incidents” because attacks are external, but incidents can include natural events and combinations of internal foul-ups, violation of safety procedures, etc.)

For an analysis of an attack scenario, one must put themselves inside the mind of a terrorist or a disgruntled employee. The attacker will not necessarily be aware of the value or criticality of the various processes in the plant but the employee will be. The intent of either of them is to cause harm or damage. The terrorist may have military-grade weapons or explosives at his/her disposal, but if plant security is reasonably good, he/she will not know where to place them for the greatest damage. The disgruntled employee will probably not have military-grade weapons or explosives at his/her disposal, but his/her knowledge of the plant is much more detailed, and he/she knows, especially within his/her department, what is most critical to the plant’s operation, what is easiest to damage, and thus where his/her sabotage will do the most damage.

The questions that should be asked during an analysis of attack scenarios include such things as:

- What are the most critical operations in the plant?
- Where are bottlenecks where equipment failure or sabotage or damage could shut down production?
- If I were an insider with intent on sabotage, how would I disable or destroy this operation?
- How easy is that to accomplish?
- If I am an outsider with limited knowledge of the plant, what is most visible?
- What appears to be most valuable?
- How would I destroy that aspect of the plant?
- What tools or weapons am I likely to have? How would I deploy or use them?
- If I have a limited knowledge of the plant, perhaps a plant aerial photo or a plant map, how would that change any of the answers to the questions above?

It is important to include the possibility of cyber attacks in the consideration of an attack scenario. The questions are slightly different and should include some of the following:

- What type of data transmission do we use?
- How it is encrypted and how secure is that encryption?
- When we use sensors or controls or SCADA systems, are they open or encrypted?
- Is there cross-checking for control systems and sensors to insure that the readings are accurate and that valves and controls are operating as indicated?
- How easily could these systems be sabotaged or intercepted?
• What happens if we get a message from one of our remote sites (such as pipeline pumping station)? How quickly can we respond? What is the impact of an incident on overall production?
• Do we have dedicated systems for operator consoles that are not open to the Internet?
• Do the operators have access to the Internet and e-mail from outside sources while at their work stations?
• Do we have systems where anyone, including operators, can enter or extract operating data to portable electronic media? (Do the computer systems have USB ports or CD/DVD reading/writing systems in the computer?)

If these questions do not give the plant security task force nightmares, the plant is either very secure, or the task force is asleep and uninvolved and does not realize the potential for internal or external attack. The purpose of the questions is to lead the task force to prioritize and expand a risk table similar to the one shown in the following.

SETTING PRIORITIES

The challenge of setting priorities is inexorably linked with the determination of the likelihood of the events or attacks, and the entire process is influenced by the cost of the attacks and the cost of control or mitigation measures designed to prevent the attacks or minimize the damages. There are a number of methods of setting the priorities and determining the likely annual and other costs. There are also a number of very good software packages that will assist with this effort. First, we will discuss the basic methodology and then one example of good software for helping determine priorities.

The basic risk analysis matrix is usually expressed as a table using stripes, dots, and white space, for easy identification of the levels of risk and the costs to some agreed-upon basis. The key words are “agreed-upon basis.” Where there is no agreement or definition, the determination of risk is just opinion (Table 1.4).

This is a risk table, and in one form or another, it is used and modified to perform risk analysis in facilities. By adding rows and columns and performing advanced analysis on the table elements and by carefully defining vulnerability, we can develop

<table>
<thead>
<tr>
<th>Item descriptions</th>
<th>Vulnerability rating</th>
<th>Cost very high</th>
<th>Cost high</th>
<th>Cost moderate</th>
<th>Cost low</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Very high</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The risk analysis matrix is usually in color. Red indicates high risk, yellow indicates moderate risk, and green indicates lower levels of risk, but we have chosen to use stripes, dots, and white spaces to highlight the risk levels, respectively.
a reasonably accurate estimate of the risk and the cost to reduce it. There are a few important points to remember about this type of analysis: (i) one cannot foresee everything, (ii) much of the data are subjective and may be accurate only to orders of magnitude, (iii) performing this type of risk analysis can be a lot of work, (iv) the likelihood of an attack or the frequency of an event will probably be the most difficult element to estimate, (v) put political considerations and internal disputes aside because what is done is for the health and survivability of the entire plant, and (vi) garbage in, garbage out (GIGO)! When you calculate the numbers, get serious about it or do not perform it.

OTHER DEFINITIONS OF RISK ASSESSMENT

“Traditional” risk assessment programs exist to identify hazards arising from work activities to ensure suitable risk control measures are in place. However, incidents continue to happen, either as a result of inadequate risk assessments or failures in the necessary risk control measures.

Risk management involves preparing action plans, implementing, and measuring performance. This can be proactive, based on risk assessments; active, based on safety audits and site inspection; and reactive, based on incident investigation and analysis.

Risk assessment of technological processes (chemical and power plants, electromechanical systems) is a complex process that requires enumeration of all possible failure modes, their probability of occurrence, and their consequences.

Security risk analysis, otherwise known as risk assessment, is fundamental to the security of any organization. It is essential in ensuring that controls and expenditure are fully commensurate with the risks to which the organization is exposed. However, many conventional methods for performing security risk analysis are becoming more and more untenable in terms of usability, flexibility, and critically—in terms of what they produce for the user.

The basic elements of risk must be explored, and a security risk assessment methodology and tools must be introduced to help ensure compliance with security policies, external standards (such as ISO 17799), and legislation (such as data protection legislation).

BUSINESS DEFINITION FOR RISK ASSESSMENT

Determining the level of risk in a particular course of action is important. Risk assessments are an important tool in areas such as health and safety management and environmental management. Results of a risk assessment can be used, for example, to identify areas in which safety can be improved. Risk assessment can also be used to determine more intangible forms of risk, including economic and social risk, and can inform the scenario planning process. The amount of risk involved in a particular course of action is compared to its expected benefits to provide evidence for decision making.
BROAD DEFINITION FOR RISK ASSESSMENT

Risk assessment is the overall process of identifying all the risks to and from an activity and assessing the potential impact of each risk. The impact is measured by combining assessed and costed risk, the likelihood of an incident, and the impact of the incident. These elements are then combined to produce a single cost figure.17

QUANTITATIVE RISK ASSESSMENT

This approach employs two fundamental elements: the probability of an event occurring and the likely loss should it occur. Quantitative risk analysis makes use of a single figure produced from these elements. This is called the “annual loss expectancy (ALE)” or the “estimated annual cost (EAC).” This is calculated for an event by simply multiplying the potential loss by the probability. As previously discussed, it is theoretically possible to rank events in order of risk (ALE) and to make decisions based on it accordingly. The problems with this type of risk analysis are usually associated with the unreliability and inaccuracy of the data. Probability can rarely be precise and can, in some cases, promote complacency. Controls and countermeasures often tackle a number of potential events, and the events themselves are frequently interrelated, and the cost of improvements cannot be clearly calculated or assigned.

Notwithstanding the drawbacks, a number of organizations have successfully adopted quantitative risk analysis.

QUALITATIVE RISK ASSESSMENT

This is by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. If we are cynical and not willing to perform the work required to make our risk assessment quantitative, we would call this informed opinion. It is easier to perform but harder to justify, especially to the financial types in the plant environment. Most qualitative risk analysis methodologies make use of a number of interrelated elements.

Threats

These are things that can go wrong or that can “attack” the system. Examples might include fire or fraud. Threats are ever present for every system. We discussed a number of these earlier.

Vulnerabilities

These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, a vulnerability would be the presence of inflammable materials (e.g., paper or stored hydrocarbon liquids or even flammable gasses). Again, it is often difficult to express a quantitative or qualitative
percentage of the operations that would increase the vulnerability. The easiest way of expressing the vulnerabilities is through group consensus, which leads to an agreed-upon percentage for damage.

COUNTERMEASURES FOR VULNERABILITIES

There are four types of controls that are critical countermeasures for vulnerabilities:

1. **Deterrent controls**—Deterrent controls reduce the likelihood of a deliberate attack. If one cannot see or locate the target, it cannot be attacked. Similarly, if the site or perimeter is so intimidating, the likelihood of attack is reduced. (Think of trying to attack a castle high on a steep and rocky hill; see photo in the following.)

2. **Preventative controls**—Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact. Preventive controls would consist of things like fireproof construction, double-walled piping, and SCADA systems with shutdown and alarm systems in the event of a system upset. Equipment such as safety flares, vents, and pressure relief vents would also fall into this category.

3. **Corrective controls**—Corrective controls reduce the effect of an attack. Fire sprinklers, fire brigade, blast walls, spill control diking, and relocation of certain facilities to give greater separation from hazards would all fall into this category.

4. **Detective controls**—Detective controls discover attacks and trigger preventative or corrective controls. This is the area for inspections and preventive maintenance, sensor systems, radar, television cameras, computer monitoring, and facial recognition services.

These controls are outlined in Figure 1.4: it illustrates the manner in which these controls work.

The D’s of security systems

There are “three D’s” of security: “denial,” “detection,” and “deterrence.”

Another set of “D’s” is as follows: “detect,” “delay,” “defend,” and “devalue.”

Detection is the easiest to explain. It involves identifying the attack prior to its inception. Surveillance, fencing sensors, remote detection devices, community intelligence, cooperation with the local police and military authorities, development of a local community network of informants and contacts, monitoring of the employees and their families all could contribute to the detection phase.

Denial generally involves design and construction that prevent the facility from being attacked. In this sense, a fence or barrier contributes to the denial, just as a locked door does. So does a concrete barrier system and/or bollards. In the design of denial systems such as traffic controls, it is often wise to consider the potential impact of car or truck bombs and barrier systems that will reduce or minimize the potential effects of blasts.

Deterrence is related to the presence and visibility of a force or a force projection that says to the potential attacker, “Don’t even think of trying to attack this facility.” It is a projection of the visible symbols and facilities of the security and
defense of the plant. For example, on the way into one of the large Aramco facilities in Saudi Arabia, the approach road is lined with Jersey barriers to direct traffic, visible security checks, and a highly visible security presence, and after the security checkpoints, there are armed defensive positions with automatic weapons that are rapidly accessible from the security positions. The guard force is also equipped with two-way radios, side arms, and the aura of an armed presence that could repel an attacker. This can be a strong deterrent to an attack.

When it comes to the terms “detect,” “delay,” “defend,” and “devalue,” the “delay” and “devalue” terms may need a bit of clarification. Most conventional fencing is looked at as a delaying presence. However, most chain link fencing will only delay a determined intruder by less than a minute, and a locked door may only provide slightly more than a minute of delay.

A recent incident related to me by someone in the oil industry in the Middle East indicated that a major oil facility had triple layers of fencing, fairly widely separated with separate zones of influence, and military response for the middle zone. Each line of fencing was separated by several tens of meters.

Two terrorist suicide bombers in separate trucks coordinated their attack on the facility. The first one made it past the outer perimeter, but could not penetrate into the middle perimeter. He started ramming his truck laden with explosives against the fence in an effort to batter it down. The terrorist was so focused on his own activities and failures that, in frustration, he detonated his truck bomb just as the second terrorist drove up to the fence. The resulting explosion took out both trucks, but aside from a hole in the ground where the fence was and some flying debris, the facility was undamaged. In this instance, the value of delay was important both for response and for outcome.

The concept of “devalue” is akin to the concept of disguise or camouflage. What an attacker can see and if highly visible may be a target. He may know that a
pipeline exists, but if it is underground and not visible, it may not really be a target worthwhile for his consideration—similar to buildings under cover or screen, fencing that uses screening, and barriers that restrict or prevent observation. Consider that even the most dedicated of attackers using standoff weapons will want to see some of his aiming point and/or have the satisfaction of knowing that he has created some damage. It is almost like saying, “Out of sight, out of mind” (Fig. 1.5).

First, consider a logical expression for security vulnerability, which is usually expressed in terms of the probability of adversary success given attempt:

- \( \Pr(S) = 1 - \Pr(\text{detect}) \cdot \Pr(\text{engage}) \cdot \Pr(\text{neutralize}) \)

- In words, this equation states that adversary nonsuccess (defender success) requires that the defender detect, engage (which consists of delay and response), and then neutralize the adversary (in sequence)—failure to do any one of these will result in adversary success (barring any random things outside the protector’s control that might thwart the adversary’s attempt).

**SAMPLE THREAT SCENARIO NO. 1 (FIG. 1.6)**

**Background**

**The process** You are the chief security officer for a large chemical complex that manufactures ammonia, urea, ammonium nitrate, and urea-formaldehyde products (based on an actual chemical plant). The plant is about 40 years old and uses natural gas as a feedstock in a Haber–Bosch gas shift reactor. Natural gas is partially burned to produce CO and \( \text{H}_2 \) and purified. Then the \( \text{H}_2 \) is reacted with the leftover \( \text{N}_2 \) from
the partial combustion and recombined in a recirculating loop to produce ammonia (gas). The ammonia gas is reacted with CO to make urea, and the ammonia is then burned to produce NO and reacted stepwise with oxygen to produce $\text{N}_2\text{O}_4$ and then with water to produce nitric acid or $\text{HNO}_3$. The nitric acid is then reacted with more ammonia to form $\text{NH}_3\text{NO}_3$ or ammonium nitrate. Ammonium nitrate is a liquid that is pumped through a shot tower where it passes through a fine screened tray to form droplets that are then dropped against a rising column of air to form spherical solids or prills. The prills are hydroscopic and will adsorb moisture from the air and melt together, so they are coated with a fine coating of wax to prevent their melting together.

**The plant** The plant is a sprawling conglomeration of several separate individual manufacturing operations. The plant units are well separated by several hundred meters, and they are essentially stand-alone units. The plant has a large rail facility (10 separate spur lines from the main line) adjacent to its manufacturing and equally large
storage areas (warehouses) for shipping and receiving. The plant footprint is approximately 700 acres (300 ha) and is protected by a 2 m chain link fence on three sides, and one side is along a major river, where there is a commercial boat dock for water shipments. The plant also has major storage areas for diesel oil and a major gas holder for the natural gas supply. About 1/2 of the plant area is devoted to the shipping/rail yard. Process units are separated by about 100 m. The plant uses coal as a basic source of energy and receives it by rail. Most of the shipments into and from the plant are by rail. The rail yard is separated from the main plant by an internal chain link fence, and the plant has two of its own locomotives (mules) to move the rail cars around inside the plant.

The area surrounding the plant consists of a four-lane divided highway (moderate traffic) and a two-lane access road. On two other sides of the plant, there are commercial developments and small residential developments. The plant shipping areas (tank farm) have 6–500,000 gallon insulated tanks (two for liquid ammonia, two for other chemicals, and one for diesel fuel) all diked with earthen dikes and an 80 ft diameter high-pressure ammonia storage tank. The plant dikes do not have good drainage, and manual valves are used to drain rainwater, and as a consequence, many valves are left open.

The plant computer facilities are at least 10 years old, and many of the orders arrive by fax, and confirmation is often sent out by wire and by antiquated teletype and printer systems. The plant control systems are reasonably modern, but they have an open system with distributed control systems and wireline controls for various processes.

Plant surveillance is at a minimum. There are some TV cameras but they are primarily at the plant office and the main gate. The guard force is 20 people, and most of the time, the guards are involved in the traffic management in and out of the plant. There are three guards on night shift, and the guard force office is right by the front gate where all the communications is located, including the plant switchboard and plant radio.

The plant is union and has approximately 2700 employees in a 24/7 operation. About 300 of the personnel are office workers and are on a 5-day per week schedule. It has its own fire department (small) and there is a community fire department (one truck + volunteers) in the adjacent community. There are two sizeable cities across the river, plus other emergency services including two hospitals and other commercial services available, but they are 0.5 hour away by car.

The rail yard is poorly illuminated, but given the nature of the facility, it is not considered much of a risk (no TV cameras). Most of the plant is of open (unprotected) construction, with piping and process areas open to the weather, except for control houses in each facility, and compressor and electrical areas and a break room. The plant is maintained in a reasonable manner, but there is always a persistent and strong (eye-watering) level of ammonia fumes in the compressor buildings and in the process areas. Operators must wear respirators and goggles when working in the compressor areas, and goggles are mandatory in all parts of the plant. Hard hats and long sleeve clothing are also mandatory.

In the event that an employee becomes contaminated by ammonia, the standing instructions are to head to the showers and begin undressing while in the shower. (The safety showers are heated and weather protected.) Activating the safety shower will summon the rescue personnel, and the standing instructions are to completely undress, including shoes and all clothing in the event of contamination. Safety
personnel will wrap the person in protective blankets and will provide medical treatment as appropriate on the way to the infirmary.

**The threat** There is general unrest and vandalism against the plant. The plant union is threatening a strike, and you have specific community individuals who are stirring up anger against the plant and trying to get the communities organized to ask the plant to shut down or move. There is additionally some threat against the idea that the plant is manufacturing “high explosives” (ammonium nitrate), and that is viewed as a potential threat to the community as a whole.

**Your challenge** You are a new head of security. Given that the plant is in relatively poor shape, you have been tasked to come up with a plan to improve security. A rash of thefts and vandalism has alerted the plant management, and you have the authority and significant budget to upgrade physical security at the plant. What are your priorities?

**Note:** this is a composite of an older plant fabricated from work memory of five different chemical plant locations each at least 40 years old. You will also want to look up some of the chemical properties of ammonia, ammonium nitrate, and CO and familiarize yourself with the overall process before attempting to provide answers or prioritizing some of the more complex responses involving the community.

Ammonia has some toxic and irritating properties in its various forms. A quick look at a material safety data sheet (MSDS) will help clarify some of the issues. Ammonia can be both smelly and irritating to mucous membranes, including the lungs and the eyes. Given high concentrations of ammonia, inhalation can be fatal, but that happens only after eye irritation and lung irritation. In a community setting, it can be extremely annoying.

Nitric acid generates a pungent and irritating vapor. Again, look up the MSDS for data on the compound. While nitric acid is not generally a substance released to the environment either accidentally or deliberately, it is a corrosive liquid. It is not generally a fence line issue for the plant.

Ammonium nitrate is unique because it is both a fuel and an oxidizer. Ammonium nitrate is a fertilizer and a primary high explosive, and when mixed with fuel oil, it becomes ammonium nitrate fuel oil, the explosive which was detonated in the destruction of the Murrah Building in Oklahoma City, OK, on April 19, 1995. This was a “home-grown” terrorist act. For reference of the power of ammonium nitrate by itself, look up the Texas City disaster of April 16, 1947, which was the largest nonnuclear explosion in the United States (see Wikipedia on the issue for detailed description), and the West Fertilizer fire in West, Texas, on April 17, 2013. The West Fertilizer fire may be more directly applicable to the local residents’ concerns about the liability from having the plant in their neighborhood, which may need reassurances that the plant safety and security is performing adequately.

**A list of possible priorities** There are a huge number of problems in this scenario. Poor management and lack of attention to maintenance and community have led to vandalism, which may be internal or external to the workforce. There are problems with the community, with the regulatory community, with the work force, and with lots of other areas. The guard force is minimal given the size of the plant.

Here are some solutions and recommendations that will help improve things. We have deliberately not prioritized the order of the improvements because perusing
the list will cause you to consider what you might do first. Go through the list and put some numbers on the list to focus on the things you think are important:

- Add new guards.
- Rotate shifts, and add a standby reserve.
- Dramatically and visibly increase security presence in the vicinity of the ammonium nitrate plant and its storage areas.
- Improve communications with the local police and fire and emergency services.
- New guard stations with keys for verification of guard surveillance.
- Greatly increase video surveillance.
- Duplicate communication/surveillance system at a secure location inside the plant.
- New encoded plant radios.
- Patch holes in plant fence.
- Replace dike drain valves with rising stem valves to increase visibility of closure.
- Better lighting/video surveillance in rail yard.
- Improve diking/spill control in loading areas.
- Badge all workers and install gate controls.
- All workers must wear badges at all times.
- Color-code hard hats and equipment for better visibility and identification.
- Biometric controls in sensitive areas of plant.
- Set up community contact committee for better local relations.
- Better training/retraining for guard force.
- Plant-wide meetings to explain new security and management procedures.
- New color video surveillance equipment.
- Better plant perimeter lighting.
- Institute safety and security drills with multiple events.
- Provide occasional plant lunches to various departments when safety/security goals have been met.
- Install a guard station at the point that the railroad enters the plant.
- Lock the railroad gate, install video cameras, and inspect station/shelter at the gate location.
- Coordinate the movement of rail cars with the warehouse/shipping departments and their supervisors.
- Install security on distributed control systems.
- Upgrade plant-wide internal and external communications with secure and buried fiber-optic lines and backup radio links.
- Light pathways and work areas to provide bright walkways and operator areas for night operations to increase worker inspections.
• Examine fence lighting to provide patrols with dark spaces, but illuminate and perform video surveillance of the fence line.
• Insure that foliage on the outside of the outside of the fence has been cleared to at least 20 ft from fence line.
• Install new lighting and video surveillance in the warehouse areas.
• Install fire and emergency alarms throughout the plant areas.
• Install a weather station with recording gas detectors on the fence line near the communities.
• List your other actions here:
  • 1
  • 2
  • 3
  • 4
  • 5
  • 6
  • 7
  • 8
  • 9
  • 10
  • 11

**SAMPLE THREAT SCENARIO NO. 2**

Figure 1.7 is an aerial view of a large chlorine–caustic soda chemical plant. For security purposes, the location has not been identified, and the photo is approximately 40 years old. The plant is adjacent to a city in the northeastern United States, and parts of the plant are over 100 years old.

**Background**

The plant produces chlorine (gas—Cl₂) and caustic soda (NaOH) through an electrolysis process. When saltwater is disassociated, it produces chlorine gas, sodium hydroxide, and hydrogen. Sodium hydroxide is a highly corrosive base, and chlorine gas is highly toxic and very corrosive as well. Chlorine gas was used in WW I as a chemical warfare agent, and it is being used by the Syrian regime against the rebels in the 2014 conflicts. The gas is dense and has a sharp odor and is yellow green in color. You are referred to the MSDS on both products for information on the toxic properties.

**The plant** The plant is old and has been around since the early 1900s. Consequently, there is asbestos in almost all parts of the plant, so construction or improvements need to be carefully managed. The plant uses coal as a primary source for its steam,
and recently, the plant has constructed a new recycling facility that will generate energy from residential and commercial garbage. The energy from waste (EFW) facility accepts truckloads of garbage and industrial wastes and sorts and classifies it to gain energy. The EFW plant has had significant startup problems including air problems, odor problems, and significant material handling problems, which resulted in poor performance, several fires, and other operating problems even though the EFW plant is highly automated.

As part of the company safety plans, the plant has a resident doctor and the infirmary is active 24 hours per day. Workers in the plant must wear proper safety
equipment at all times, including a hard hat, boots or work shoes, goggles, and an escape canister. If there is a chlorine release, the escape canister reduces the concentration of gas in the area to breathable levels, giving the employees the opportunity to run away from the gas plume. There is also a gas leak alarm at the plant, and everyone is accustomed to hearing it and knowing that they are to run away from gas clouds. As shown previously, there are residential areas on two sides of the plant and associated heavy industry on a third side. The plant is bounded by a highway on the south and bisected by another and also by the railroad spur. The northern portion of the plant is used by the EFW facility. The plant has a 2 m chain link fence with three strand barbed wire on top. At night, several of the principal operating areas associated with the chlorine plant are brightly lit, but the rail yard and nonprocess areas are poorly lit to unlit.

**The threat** The plant has a strong and militant union that has gone out on strike frequently. The plant employs about 280 persons in a 24/7 operation. The management and the union are often at odds, and in a recent strike, there were a number of minor acts of vandalism, sabotage, and pranks. There is a major waterway near the plant, but given the nature of the waterway, most of the chemicals are shipped out via rail through highly populated areas. The rail line separates the two halves of the plant, and there is a growing community awareness that the chemicals manufactured and their derivatives are toxic, harmful, and potentially life threatening. There is no current way of determining who is in the plant at any one time. There is also the issue of an occasional chlorine release into the community, sometimes strong enough to cause the paint on the adjacent houses to need repainting.

The local community is near or at a boiling point because of the plant, the waste problems, and other issues related to the long-term disposal of chlorinated chemicals in a local landfill. Cars of employees have been vandalized, some of the buildings have been tagged with spray paint, and plant intrusions have been recorded. So far, every incident is relatively minor. There have been threats of bombs and derailing shipments and sabotage by militant environmentalists and others opposed to the plant’s presence.

The security is divided because part of the staff, approximately half, is relegated to the north gate to control traffic and security for the EFW facility (north of the tracks). There are two guard stations, but the north gate and south gate stations operate independently and do not really communicate. Trucks entering the plant are directed to the warehouse. The dispatch and inspection stations are located right on top of the plant gates.

**Your challenge** You have just been made of head of security and have about 20 people on your staff. Your new position is as a result of your boss being fired for an incident involving diversion of funds in conjunction with activities in the warehouse. You are now reporting directly to the vice president of operations. He called you in with your new appointment and told you to quiet the community around the plant and improve security at the plant. Your challenge is to come up with your own list of actions and improvements to make the plant better liked in the community. Develop a list of at least 10 action items, but do not worry about the budget.
1 See the writings of Dr. Ted G. Lewis of the Naval Postgraduate School for Homeland Defense and Security. He has an extensive model simulation of self-organized criticality on the website https://www.chds.us/?media/resources&collection=53&type=SIMULATION.

2 As an example of self-organized criticality that leads to failure, one frequently has to look no further than any one of many government assistance programs or regulatory programs. In the years that they have been in existence, the bureaucracy has taken over the mission, and now, services are being delayed or denied because of a paperwork blizzard, deliberate cover-ups that point to political agendas, and sheer incompetence. One of those agencies in the United States is the military veteran’s hospital system where care is being denied to needy veterans and the paperwork has been shuffled around to make the system appear better than it is. Similar charges have been leveled against the Internal Revenue Service, the Department of Homeland Security, the Department of Interior, most of the Department of Health and Human Services, and the Environmental Protection Agency where blind adherence to rules has often trumped common sense.

3 One of the methods to reduce internal risk is HAZOPS, a critical review of plant operations and processes with a focus on analysis of potential methods of failures. For detailed requirements of HAZOPS, see the website www.OSHA.gov and search for process safety management and HAZOPS, or see http://www.osha.gov/Publications/osha3133.html.

4 Sabotage can be very serious or just annoying. In plants with strong unions, it can be a factor during a strike. Based upon personal experience, one union member boiler house worker ran a hose into the inspection port of the hopper in the coal-fired boiler cyclones immediately prior to the strike. The water interacted with the fly ash and made cleaning the collection hopper very difficult. The hoppers had to be cleaned continually in order for the cyclones to remove the fly ash. Sabotage? Sure, but more of an annoyance rather than a damage.

5 A good case in point is illustrated by the BP refinery disaster in Texas City on March 23, 2005. In that incident, as Wikipedia described, “A number of plant workers were killed when a vent stack flooded and spewed volatile chemicals in the vicinity of the plant. Hydrocarbon flow to the blow down drum and stack overwhelmed it, resulting in liquids carrying over out of the top of the stack, flowing down the stack, accumulating on the ground, and causing a vapor cloud, which was ignited by a contractor’s pickup truck as the engine was left running. The report identified numerous failings in equipment, risk management, staff management, working culture at the site, maintenance and inspection, and general health and safety assessments.” One of the CSB findings was that a trailer that was occupied only a small fraction of the year was located too close to the stack (source of the explosion). The trailer was occupied at the time of the explosion, resulting in over a dozen fatalities.

6 Any competent meteorologist or hydrologist will tell you that the probability of an extreme weather event is highly unpredictable and the frequency of the event is cited with respect to an anticipated average frequency. The problem is that the database from which that frequency data was developed is often less than 100 years.

7 A recent visit to a petroleum refinery in the Middle East illustrates this statement. Plant maintenance removed a pump from a bottom fed line on a large crude oil storage tank. Nobody told the operators that the pump had been removed. The tank valve was not locked out nor de-energized. “According to the plant operator, ‘the valve came open by itself.’” The resulting spill was 55,000 barrels of crude oil. Only 50,000 barrels of crude was recovered due to poor design of the impoundment. The other 5000 barrels are floating above the saline groundwater and are gradually making their way toward the ocean. These types of accidents generally happen through multiple failures to follow procedures, and the after
incident report almost always indicated that the accident was preventable if procedures were followed.


9 Physical and historical assessment methods may involve such items as building cost data adjusted by historical inflation and building costs indices such as the Engineering News Record (magazine) index and such estimating guides as RS Means guides on building and equipment cost reconstruction. The DOE also has a guide on cost estimating, as do many of the other agencies, including the DOD and the GAO. Some of these guides are quite specific. McGraw-Hill Publishing Company has a software program for equipment costs as part of the Plant Design and Economics for Chemical Engineers, 5th ed., and there are a number of other equipment cost estimating guides on the Internet. Also, many of the large engineering and design-build construction companies also have very good equipment estimating divisions.

The accuracy of a good estimate increases with the amount of detail and the cost of preparing that estimate. The cost of a good estimate accurate is within about 10% of the actual construction cost.

The American Association of Cost Estimators has defined five categories of accuracy for cost estimates. Their most accurate estimate category is a Class 1 estimate, which has a range of −3 to +15% of construction cost, and the estimates are made from a detailed takeoff of bid and process documents, but these cost estimates are expensive and can run to 10% or more of the construction cost of the project.

10 CERCLA, the acronym for Comprehensive Environmental Response, Compensation, and Liability Act, authorizes EPA to respond to releases, or threatened releases, of hazardous substances that may endanger public health, welfare, or the environment. CERCLA also enables EPA to force parties responsible for environmental contamination to clean it up or to reimburse the Superfund for response or remediation costs incurred by EPA. The Superfund Amendments and Reauthorization Act (SARA) of 1986 revised various sections of CERCLA, extended the taxing authority for the Superfund, and created a free-standing law, SARA Title III, also known as the Emergency Planning and Community Right-to-Know Act (EPCRA).

11 One of the most notorious incidents is the Bhopal, India, incident where, in 1984, an alleged incident of sabotage killed over 3787 and injured 558,125 persons through a gas release of methyl isocyanate. The cause is under debate with the Indian Government claiming the cause was negligence and sloppy management, while Union Carbide (now Dow Chemical) claims that the cause was an act of deliberate sabotage.

12 Under tort law, which is often largely unwritten, many major suits for equitable relief have been brought against companies for permitting or releasing contamination into the environment and causing property damage and personal injury to residents of areas where the company has operations, either in or out of the United States. US cases of note include the Love Canal, a case about a leaking landfill; the Hinkley, CA, hexavalent chromium-contaminated groundwater incident against Pacific Gas and Electric brought to notice by the film Erin Brockovich; the Times Beach incident involving polychlorinated biphenyls; and the Woburn, MA, groundwater contamination (chlorinated solvents) incident, which was described in the movie A Civil Action. There are many, many others.

13 Two significant refinery fires and explosions that lead to fatalities include Buncefield Oil Storage Depot, Hertfordshire, United Kingdom, in December 2005, and the Gulf Oil refinery fire, Philadelphia, on August 17, 1975 (see Wikipedia for descriptions of each incident). There was also a significant refinery fire that resulted in fatalities of the firefighters in 1975. The drainage system was insufficient to remove the oil from a tank fire, and the firefighters were working in a pool of water that had oil on it. When the
fire fighting foam blanketing a pool of water with oil standing on it developed an opening, vapors were released and ignited, and eight firefighters were killed or died as a result of burns (see the article on the fire in Wikipedia).

14 A discussion with a prominent Middle East security force for a major petroleum producer indicated that right after the World Trade Center attack on September 11, 2001, the security force went into a crash priority program of reorganization because they realized that a number of the perpetrators were of Arabic nationality and might be coming after their facilities next. Prior to that, they were focused primarily inward until they realized that they had an external threat as well.


16 In a recent training course at a large chemical company in the Middle East, some elemental network analysis indicated that the location of the security command center was right next to the front gate. Any terrorist incident involving a bomb would have taken out that command center, leaving emergency services coordination in a difficult situation. The solution to that problem is to provide a backup command center with full duplicated access to everything that the primary command center has in the way of information. The information sources, however, cannot be routed through the primary center, but must be fully independent in order to be reliable.


18 A Jersey barrier looks like an inverted letter Y. It is about 0.7 m tall, 10–15 cm at the top and about 0.5 m at the base. Effective ones are made from concrete.