Security risk assessment and protection in the chemical and process industry

Authors: Genserik Reniers[1,2], Paul Van Lerberghe[3], Coen Van Gulijk[2]

[1]Centre for Economics and Corporate Sustainability (CEDON), Faculty of Economics and Management, HUB, KULeuven, Stormstraat 2, 1000 Brussels, Belgium, e-mail: genserik.reniers@kuleuven.be

[2]Safety Science Group, Faculty Technology, Policy and Management, TU Delft, Jaffalaan 5, 2628 BX Delft, The Netherlands

[3]Director Engineering Optimit, Gerechtstraat 10, 2800 Mechelen, Belgium

Abstract

This chapter describes a security risk assessment and protection methodology that was developed for use in the chemical- and process industry in Belgium. The approach of the method follows a risk-based approach that follows desing principles for chemical safety. That approach is beneficial for workers in the chemical industry because they recognize the steps in this model from familiar safety models .The model combines the rings-of-protection approach with generic security practices including: management and procedures, security technology (e.g. CCTV, fences, and access control), and human interactions (pro-active as well as re-active). The method is illustrated in a case-study where a practical protection plan was developed for an existing chemical company. This chapter demonstrates that the method is useful for similar chemical- and process industrial activities far beyond the Belgian borders, as well as for cross-industrial security protection. This chapter offers an insight into how the chemical sector protects itself on the one hand, and an insight into how security risk management can be practiced on the other hand.

Keywords: *chemical industry, security risk assessment, protection, intentional acts, rings-of-protection concept*

1. Introduction

Security focuses on intentional harm. That is to say, the damage to a chemical- or process plant was intended by a party within or outside the operating company and therefore malignant. Protecting organisations against this kind of threat is fundamentally different from the protection needed against accidents in the safety domain. Safety goes hand in hand with an accidental, non-deliberately caused, event. It requires a different approach from security. Nevertheless, some well-developed tools from the safety domain can be used effectively when we design a security system for a chemical plant. This chapter demonstrates that concept. Safety management and risk analysis take centre-stage in this

chapter. In that sense, this chapter follows different approach to the design of a security system than the more traditional security management design approaches as described by Garcia (2008) or Gill (2006). This approach is justified by the fact that workers in the chemical- and process industries are already very familiar with safety and risk models that are extremely important when operating a plant. The design methods, even if they are based on similar principles for the protection of human life and property, have developed differently than security methods. An overview of safety design in the process industries is given by Mannan (2005) and Cameron and Raman (2005). Since these works are quite exotic in relation to the security management domain, much of this work hinges on SRMbok by Talbot & Jakeman where many design models are used that are recognized by security managers and process safety workers alike.

Starting from Talbot & Jakeman (2009), security can be defined as the condition of being protected against danger or loss that follows from the intentional and unwarranted actions of others. This definition looks at security as an end-product. Another way of looking at security is as a process leading towards a situation where something is 'to be secured'. Security can thus also be defined as the process involved in taking preventive measures to avoid harmful incidents caused by (internal or external) people as well as controlling such incidents and their adverse effects (Reniers, 2011). Both definitions are useful to understand the requirements for assuring adequate security risk assessments and protection. The motives for causing damage can vary from mundane (e.g. small financial gain through theft) to potentially highly damaging terrorist actions. The latter case is of particular interest for a chemical company since it typically holds mind-boggling amounts of hazardous materials that are toxic, flammable and sometimes both which potentially makes them a vulnerable target.

Similar with regards to providing safety at a chemical plant, risk assessments are carried out for security of such plants; they are called 'security risk assessments' or 'threat assessments' (API Recommended Practice 780, 2012). The starting point for any security risk assessment is risk identification. Identifying the security risks and determining the necessary measures to counter those security risks, is fundamentally different from safety risks. Security risk assessments focus on 'qualitative likelihood' (in terms of 'low', 'medium', 'high'), consequences, vulnerabilities, threats and target attractiveness. It is typically a qualitative exercise that often focuses on the identification of scenarios (for example: blowing up installations X and Y in plant Z; burglary of item A in building B, etc.). With safety assessments the 'quantitative likelihood' (in terms of probabilities and frequencies) and 'consequences' often take centre-stage where the quantitative or semi-quantitative exercises are performed (Cameron & Raman, 2005).

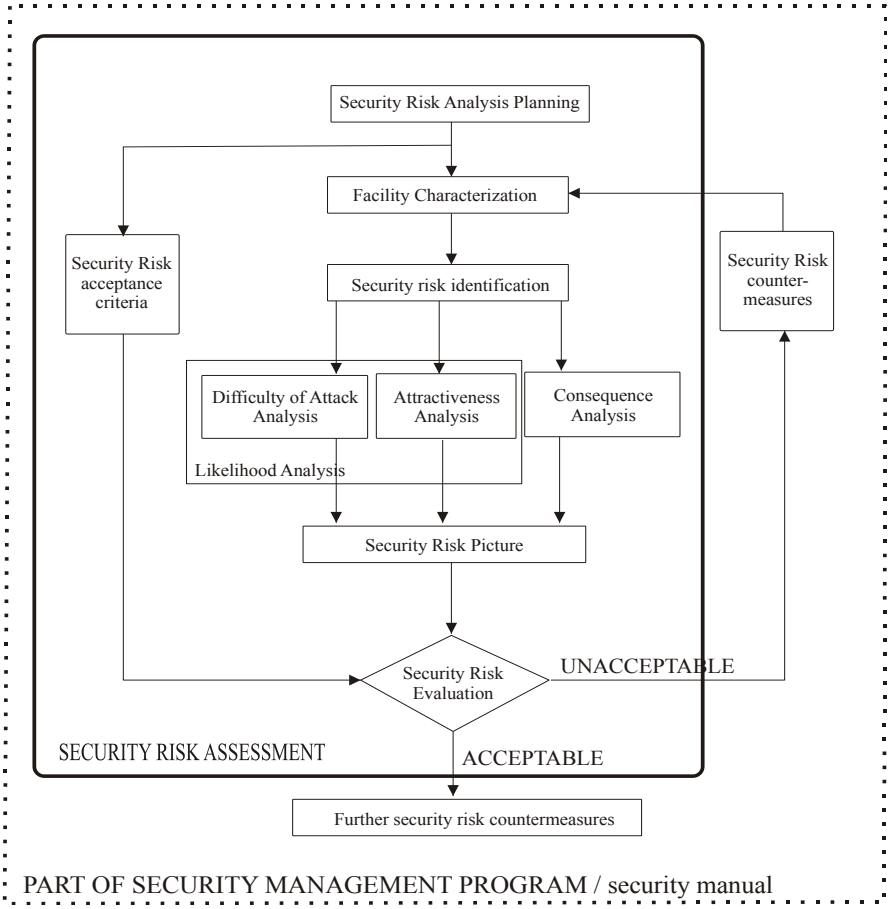
Like safety assessments, security assessments are focussed on proactive action and consequence controls. It is these similarities in safety and security that prompts experts to indicate that, for

achieving an optimal result, an integrated approach is required (Fontaine et al., 2007; Holtrop and Kretz, 2008). This topic is explored in section 2. The basic theoretical concepts that form the basis of such an integrated approach are dealt with in section 3. The translation to practical cases is explained in section 4, which is based on an existing chemical plant.

2. Security risk assessment approach

Security risk assessment in the chemical and process industry is characterised by a systematic approach to organizing information concerning the assets that need to be protected, the threats that may be posed against those assets, and the likelihood and consequences of attacks against those assets. Assets are usually grouped into the following categories: know-how, people, property and infrastructure (e.g. chemical installations), reputation and information. Hence, security risk assessment serves to improve a chemical company's understanding of the threats and possible responses to those threats. As such, it forms the basis for establishing a cost-effective security risk management program suitable to reduce the potential adverse effects of intentionally induced losses upon the company. Security risk assessment at a generic level is presented in Figure 1.

Figure 1. Iterative process of security risk assessment as part of security management (based on Reniers, 2010)



Before the security risk identification process can take place it is important to undertake a so-called *geographical overview* of the company in the Facility Characterization phase. In this phase, neighbouring companies and their industrial activities that may be a target for adversaries should be identified, as they may be developing, using, or storing chemical product(s) or process(es) that have the potential to interact with the product(s) of the company under consideration with extreme results. Furthermore, the possible access roads from where the adversary may intrude the company's premises without being noticed, should be determined. Another important issue to deal with, is how to escape from the premises in case of a major event.

The security risk identification process should identify all company security risks. For more information on security risk identification in a chemical industrial surrounding, see Reniers *et al.* (2013). This process should be carried out by using desk-top research as well as historical data. Desk-top research is derived from rather fundamental and theoretical perspectives generating ideas on what could or might happen and can be found in the professional and academic literature (CCPS, 2003; Landoll, 2006). Historical data comes from crime incident/management databases, containing, for example, details of attack histories and experiences at other chemical plants. This information is very useful for both carrying out security risk identification and for understanding the specificities of risks and their consequences. It is important that relevant stakeholders (be they internal or external) should

be involved in the security risk identification process. This process might typically include the company, government officials, policing organizations and even representatives from relevant intelligence networks.

Once the company's security risks have been identified, every security risk should be analysed. Also, the level of every risk, or combination of risks, should be assessed. Once this exercise has been carried out, individual security risks can be compared and evaluated. As part of the evaluation process, the companies' security risk appetite has to be set and agreed upon with the relevant stakeholders. The outcome of the risk analysis is then compared with the security risk appetite of the company. Typically, it is the responsibility of the security manager, together with the organization's board, to conclude whether the risk is acceptable, tolerable (eventually with countermeasures), or unacceptable and therefore needs to be mitigated in some way. Every step in the process has to be rigorous and transparent so that changes over time can be captured as well.

3. General design principles for building up a protection strategy inside a chemical plant

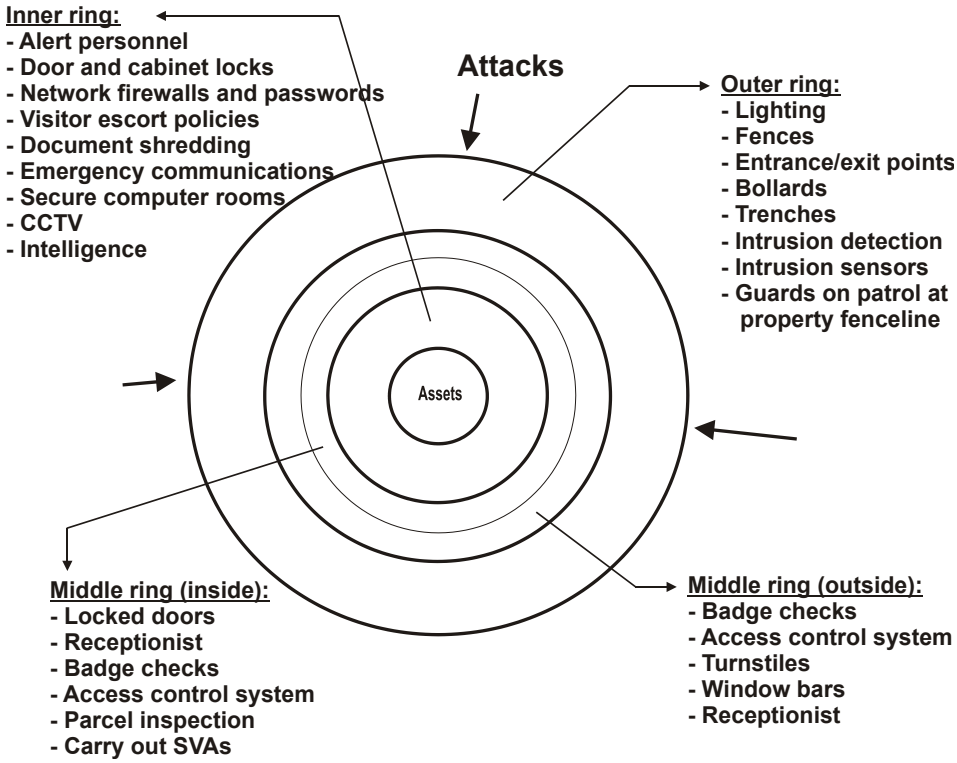
3.1. The rings-of-protection concept

So-called Layers of Protection are specifically used by safety managers in the chemical industry (see for example CCPS, 1996; Dowell, 1999; Meyer and Reniers, 2013). Detailed process design provides the first layer of protection. The second Layer of Protection concerns the automatic regulation of the process heat and material flows and ensuring that sufficient data is available for operator supervision. In the chemical industry this layer is also called the 'Basic Process Control Systems' (BPCS). A further layer of protection is provided by a high-priority alarm system and instrumentation that facilitates operator-initiated corrective actions. A Safety Instrumented Function (SIF), sometimes also called the emergency shutdown system, may be provided as the fourth protective layer. The SIFs are protective systems which are only needed on those rare occasions when normal process controls are inadequate to keep the process within acceptable bounds. Any SIF will qualify as one independent layer of protection. Physical protection may be incorporated as the next layer of protection by using venting devices to prevent equipment failure from overpressure. Should these different layers of protection fail to function, walls or soil embankments may be present to contain liquid spills. Plant and community emergency response plans further address the hazardous event.

The fundamental basis of security management can be expressed in a similar way to the Layers of Protection used in modern chemical process plants for addressing (safety-related) accidental events. In

the similar security-related concept of concentric so-called "rings-of-protection" or layered protection (CCPS, 2003; Fennelly, 2004; Ellis & Hertig, 2010), the spatial relationship between the location of the target asset and the location of the physical countermeasures is used as a guiding principle. Rings-of-protection, also known as the layered defences, are based on the 'Defence in Depth' principle (IAEA, 1996; Ellis & Hertig, 2010; ASIS, 2012). An effective countermeasure deploys multiple defence mechanisms between the adversary and the target. Each of these mechanisms should present an independent obstacle to the adversary. Figure 2 (based on Reniers, 2010) illustrates the rings-of-protection concept and its component countermeasures (listed non-exhaustively).

Figure 2. Rings-of-protection concept found in modern chemical plants (based on Reniers, 2010)



When the security management team has decided which security risks require protection measures, a company security concept can be designed. In this regard, a complete view of the chemical plant and its surroundings, geographical as well as socio-technical, is the starting point.

The rings-of-protection concept illustrated in Figure 2, and based on the Defence in Depth approach, is the backbone for security systems (IAEA, 1996; CCPS, 2003; Fennelly, 2004; Talbot & Jakeman, 2009; Ellis & Hertig, 2010; Reniers, 2010; ASIS, 2012). Most commonly, the terminology of 'perimeters' and 'zones' is used.

Every ring from Figure 2 is defined and constructed according to the risk sensitivity of the objects inside that zone (e.g. storage of flammable liquids; a reactor that is prone to explode during process disturbances, etc.). This occupancy will be important for building the rings-of-protection for the chemical plant. The barriers that protect a specific ring are designed with a certain 'resistance against intrusion'. The target in the centre is the asset that is deemed most attractive for a potential adversary and therefore requires the most protection. The resistance of a barrier and the time it takes an adversary to get to the target are important factors in the probability of interruption when setting up a path analysis.

An adversary will choose a specific path (usually one of several options), also called 'adversary path' (Arata, 2006; Garcia, 2006 & 2008; Norman, 2010) to get to a target. The path can be seen as an ordered series of actions taken against a facility, which, if/when completed, results in a successful attack. As an example, to destroy a water pump, the series of subsequent actions may be: penetrate fence, walk to outside door O of building B, penetrate outside door O of building B, walk to inner door D of target room R, penetrate inner door D of room R, destroy water pump. Remark that several series of actions may be possible to destroy the water pump, and only one of them is exemplified. The 'critical path' is that path (out of a number of possible paths) requiring least time to complete the ordered series of actions. To adequately protect the target, it is essential that the time needed for the critical path is higher than the interception time. To this end, for every of the actions composing the path, there should be a delay element (e.g., a steel fence) and a detection element (e.g., a thermal camera with VCA). Several possible calculation models are available to carry out a path analysis, for example the EASI model (Garcia, 2006 & 2008).

A ring-of-protection translates into a number of physical measures, as it is a combination of physical security equipment, people and procedures. Elements of all these types are typically needed together in order to guarantee adequate asset protection against different threats be they theft, sabotage, terrorism, or other malevolent human or technical attacks from outsiders as well as insiders.

3.2. The intrusion process

Before commencing the design of the protection barriers (that is, the rings-of-protection), the different steps corresponding to an adversary's intrusion should be understood. These steps will help the security manager in generating security specifications. A description of an intrusion can be presented via the acronym "PICER":

- ***P**reparation stage:* this is where the adversary will start gathering information about the site and the target. He or she may visit the chemical plant several times and possibly participate in seminars, site visits, and engage in social engineering (name dropping to enter the site) or even contract work; the adversary path will be determined by the adversary in this stage.
- ***I**ntrusion stage:* this is when he or she will enter the site. The time taken to reach the target was calculated by him/her (while determining the path in the previous stage) so that in event of an alarm activation there will still be time to escape. Different methods can be used for calculating the amount of required time to reach the target. Most commonly used is the critical path method (as explained before);
- ***C**ollecting stage:* at this stage the adversary collects goods or commits the unwanted action;
- ***E**xit stage:* this is when the adversary will leave the chemical plant;
- ***R**ewarding stage:* this stage or process is more relevant to law enforcement than the security manager since it involves trading stolen goods for money. This can take place immediately or some time later.

The principle of 'PICER' is mentioned in a handbook that is published by the Belgian Institute of Security (Institute of Security Belgium, 2013). The handbook is used in training sessions as required by Belgian Law (Belgian Official Gazette, 1990) but is regretfully not publicly available. The PICER principle indicates that the design of the protective rings should be focused on the first perimeter, or at least as early as possible in the protection process. The first, second, etc. perimeters should be able to react as soon as possible, even (and preferably, if possible) during the preparation stage. Camera surveillance may for example help to identify people loitering around the first perimeter or it might detect people trying to collect information about the strength of the fence. Indeed, when a CCTV system is installed on a large site, then it will not only return information about an intrusion itself, but it can also be used in a preventive stage by guards on patrol (receiving information from a distance), who are able to manually inspect the condition of the fence: intact, broken, cut).

At the moment an attack starts, a detection indicator should be executed. The later the detection takes place, the greater the difficulty of interception becomes. If an intrusion is detected, there must be a way of engaging a response.

As already noted, physical protection in itself will not prevent an attack. It is typically a combination of different security measures that need to be employed, a principle which is defined as "OPER". Similar to PICER, the 'OPER' principle is mentioned in the training handbook of the Belgian Institute of Security (Institute of Security Belgium, 2013), which is mandatory by Belgian Law for private security officers to be examined about to be allowed to carry out their profession (Belgian Official Gazette, 1990). The OPER acronym stands for:

- **O**rganizational – about security awareness, management requirements for security, and other procedures to prevent intrusion
- **P**hysical – security equipment such as barriers, fences, etc.
- **E**lectronics – security equipment such as access controls, burglar alarms, cameras, etc.
- **R**eporting –transmission of an alert to an external dispatch service

The design process of the rings-of-protection will be based upon this OPER principle. Each perimeter (equal to a certain ring of protection) will consist of a fence with gates or barriers. The access to these rings will be equipped with the right access control system and (depending on the organization) often in combination with intrusion detection and CCTV. In the event of an adversary attempting to gain access the activation of the systems will generate a response.

3.3. Organizational requirements

Adequate security starts with the genuine commitment of organization top management. In the safety domain, top management commitment has been identified as an essential contributing factor for adequate safety performance (see e.g. Wu et al. (2008), Kapp (2012)). Due to the similarity between operational safety and security management, it can be assumed that the same conclusion on management commitment holds for security. However, in the security field, there are only few scholarly publications that prove this claim. As an example, qualitative research by Reniers (2011) indicates that success will depend to a large extent on senior management showing meaningful support for security.

Security within a chemical plant, as also in other industrial sectors, needs to be clearly defined and set up according to the security risks present, and considering the balance between the threats and the risk appetite (see before). If the approach to security is not written down in a security manual, there is a danger that ad-hoc decisions will be made in dealing with threats, possibly leading to inadequate responses. We recommend that the development of a credible security manual is based on the following domains of consideration (see also Talbot and Jakeman, 2009):

- a security policy
- security procedures
- An employees' screening process
- a security awareness programme

- security training
- an emergency response facility
- incident reporting

The process needs to be accompanied by a security audit to assess the security 'maturity' of the chemical plant, the results of which can feed into a gap analysis between the existing situation and the desired situation, to identify areas needing improvements. We recommend, based on more than 20 years of practitioner's experience, that the audit be performed on 12 security domains: Risk Assessment Strategy, Human Aspects, Physical Security, Access, Intrusion, CCTV, Fire, Integration, Guarding, Information Security and Security Audit. Literature supports this taxonomy, e.g., Talbot & Jakeman (2009) developed a model in which most of the domains, which they call 'categories', can be retrieved. To our best knowledge, the sum of these domains encompass all security items that need to be considered in a chemical organization, and the possible integration of security with safety is also taken into account.

The design of a physical protection model for chemical plants is explained more in depth in the next sections. The explanation is based upon the case study of a real chemical plant and the way security was setup in this plant (for further reading on the development of an integrated security process, see Talbot & Jakeman, 2009).

While in this section, we explained the general design principles for building up a protection strategy inside a chemical plant, the next section elaborates a very practical approach to illustrate how these design principles can be translated into an industrial case.

4. Security measures and protection; Practice in the chemical industry

4.1. Physical security

In a previous section, the concept of the rings-of-protection (that is, defences in depth or plant perimeters of protection), was explained. Since the rings will be the basis of the complete security plan, there will be security breaches if they are not well researched.

Prior to determining the rings-of-protection, an inventory of each part of the plant (building, building level, department and other 'clusters' of the plant) needs to be prepared. The plant's so-called "vital points", especially deserve attention. Vital points (physical assets) mainly include: water-inlet, water-outlet, storage rooms for waste, electrical generator rooms, and storage locations of highly dangerous

goods. The inventories of every location situated within the premises of the plant serve to identify the targets.

The subsequent site visit should shed light on the flows of materials (including raw materials, produced materials and waste), cars, people (own employees, maintenance personnel, contractors, visitors, and others), information, and ICT. These flows will help determine the most appropriate locales for access points and also for other security measures. Once a complete inventory has been finalised, the protection level of zones and perimeters may be determined. In Figure 3, a generic setup of a chemical plant, using the rings-of-protection concept, is shown.

Figure 3. Generic setup of a chemical plant

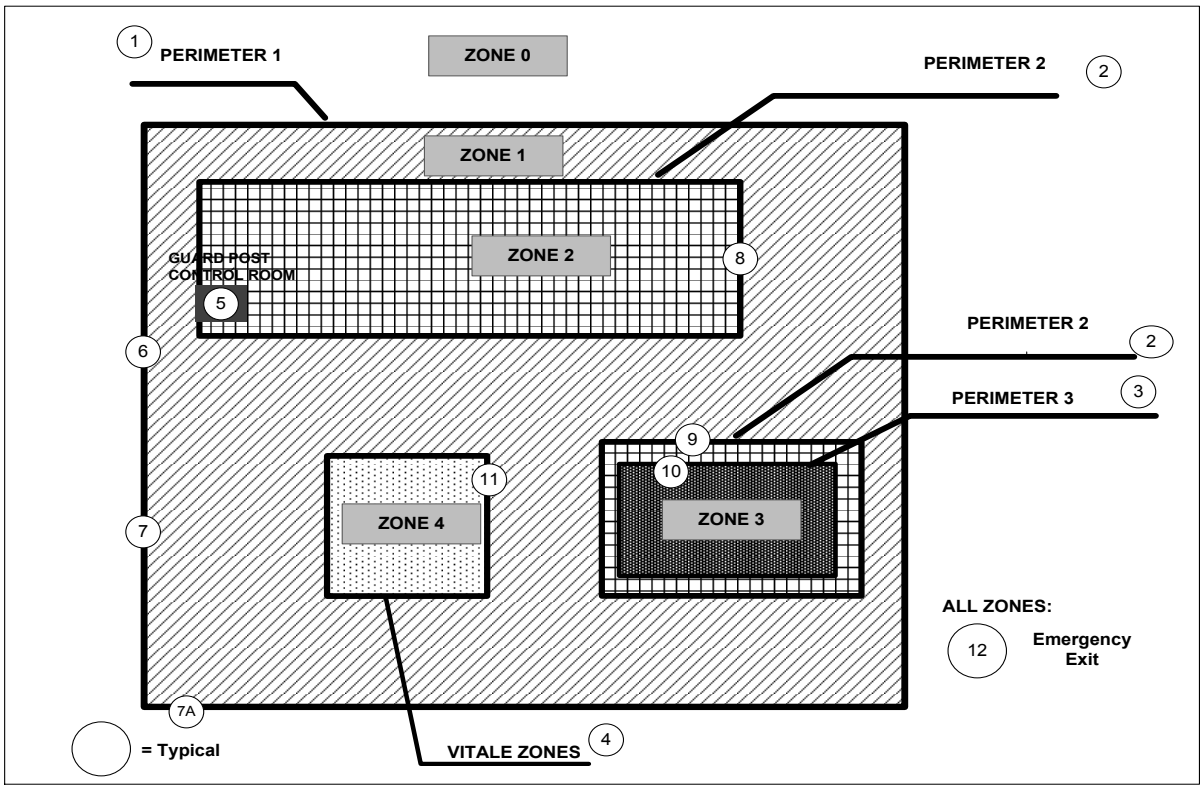


Figure 3 schematically shows zones and perimeters for areas with different risk profiles. So-called "Typicals" are also indicated on this drawing. A *Typical* is as a summation of technological items composing a security barrier, and thus describes the specific detailed technical characteristics of a security measure installed at a plant or at a part thereof. For example a Typical for car access will indicate all security elements of which this access point consists: a barrier, a badge-reader to enter the site, and a vehicle loop to leave the site. These Typicals will be used to describe physical security needs for the perimeters as well as the requirements for accessing the different zones. The PICER principle will be used to determine the needed protection within the perimeters and zones. Note also

that the security needs are met by the OPER principle: the measures are built up from organizational, physical, electronic and reporting elements.

For example, '(6)' indicated in Figure 3, is the Typical that represents the access for pedestrians and cars to ZONE 1, whereas '(7)' is an indication of the access for the entrance of trucks, and (7A) indicates the access for the entrance of railway carriages.

During this setup, the zone outside the plant borders, called zone '0', should not be neglected. Although this zone may seem unimportant, it is potentially the starting point of the intrusion. This zone actually becomes crucial if several chemical installations, not being located at the same premises, form part of one larger chemical plant. If such is the case, there may be public domain between the different installations of the plant, and zone '0' may become an important zone where people and/or materials are transported between the installations. Some secured goods or people will be traveling from one secured plant to another secured plant. This means that they will be remaining for a defined, or non-defined, time in a 'non'-secured zone. In such case, measures need to be set up for securing this zone or for securing the zones where travel and/or transportation is possible in between.

The first protection ring will in most cases be the boundary of the plant site. Other zones will be:

- 2 = administrative offices for exploitation of the site
- 3 = buildings, essential administrative offices as well as storage rooms, and production clusters
- 4 = vital zones (see earlier), the operational centre and the central security room
- 5 = high-security areas

To better identify the security countermeasures required, a specific methodology can be used. The methodology we suggest, uses definitions called URB and URS. URB stands for "User Requirements Basic" and URS is an acronym of "User Requirements Specific". This method is based on practitioner's experience within security, and is based on a multidisciplinary approach integrating security and safety needs, and taking financial considerations into account. This object-oriented approach represents concepts as "objects" that have data fields (attributes that describe the object) and associated procedures known as methods. It is a well-known programming method and programming languages such as C++, C#, and Java can be given as examples of such approach. Gabbar and Suzuki (2004) describe the design of a safety management system using an object-oriented approach. In our application of the approach to the field of security, the URB explain the generic needs of a specific element of the perimeter and the throughput in a zone. The URS define the specific rollout of the

physical protection system. The URB as well as the URS are a combination of all possible security requirements (people, procedures and technical issues).

The way an URB is written down, is given in the procedure displayed in Figure 4. This URB reporting structure is actually based on the OPER principle.

Figure 4. Scheme of an URB

URB – <indicate the name of the URB>

/* *<Start of the rules>*

#D *<Description part>*

#O *<The organisational measures to be taken into account>*

#P *<The specific physical security measures, including resistance time and the norms>*

#E *<The specific electronic security measures, with an indication of the probability of detection ($D_{etection}$) expressed in % (value between 0 and 100%) wanted>*

#R *<Indication of the way this alarm will be transmitted and displayed, with an indication of the Alarm priority (A value between 1 and 5)>*

#L *<List of applicable regulations like: internal laws, SEVESO, …>*

*/ *<End of the rules>*

The generic procedure of Figure 4 gives for the first URB, the syntax as displayed in Figure 5.

Figure 5. Definition of URB for perimeter 1

URB – Perimeter 1

/*

#D <Boundary between Zone 0 and 1>

#O <Indicate the boundary of the chemical plant>

#P <Fence with a resistance time of t seconds according to following norms: N1, N2, etc., access for cars and people must be possible>

#E <Electronic Detection for non-authorised access, based up on Nx with $D_{etection}$ = y % >

#R <Alarms connected to the central Security Management Systems $A_{PRIORITY}$ = 1>

#L <applicable Regulations>

*/

Once the complete set of URBs has been defined, the URSs can be drafted. An URS describes the technical specifications of the URB. It is however neither a technical descriptive of the solution, nor is it a set of procedures. In case of an existing plant it is often common that several URSs are present but that some of them differ on one or more specific parts. As an example, for the URB 1, for example 6 URSs can be identified, namely:

URS 1 = the fence itself

URS 2 = the access-points for pedestrians and cars

URS 3 = the access-points for the trucks

URS 4 = the access-points for the trains

URS 5 = the access-points for the boats

URS 6 = the access-points to the utilities such as water and electricity

As strange as it may seem, it is worth noting that places where energy is produced or where cooling water or water needed for production is being stored, are often forgotten as targets for adversaries. However, these locations should also be protected (Arata, 2006), hence the URS6 in our list above.

On the schematic security drawing of the plant, Typicals (that is, as mentioned, the summation of technological items composing a security barrier) with a number and a letter should be mentioned. An important point, especially in chemical plants, is also to make an inventory of ATEX-zones or other zones with explosion risks, for example in Figure 3 marked as Zone 3. These zones will need specific equipment for every kind of security technology that will be installed.

To explain in detail the concept of Typicals an example is given here. To enhance the understanding of Typicals, a plan of a chemical plant with the rings of protections and the Typicals on that plan are shown in Figure 6.

Figure 6. Chemical plant and its Typicals

Figure 7 gives a schematic drawing of one illustrative Typical, that is, the security equipment needed for a standard emergency exit. The emergency exit may only be used to access a building in case of evacuation. As often seen, this door is also used for shortcuts or for smoking outside the building. To prevent the opening of this door by means of the panic bar, a magnetic contact will additionally be added in combination with a loud sounder and a camera. In case of an opening the sounder will indicate the opening of the door, and the camera will start recording the person(s) leaving the building.

Figure 7. Typical 12: “Emergency exit”

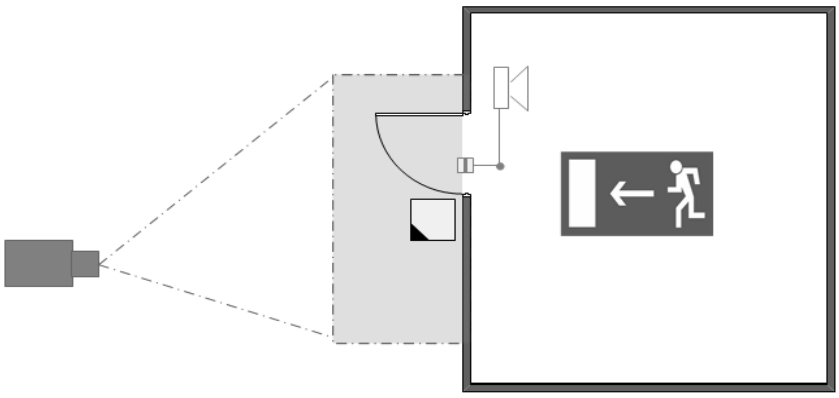
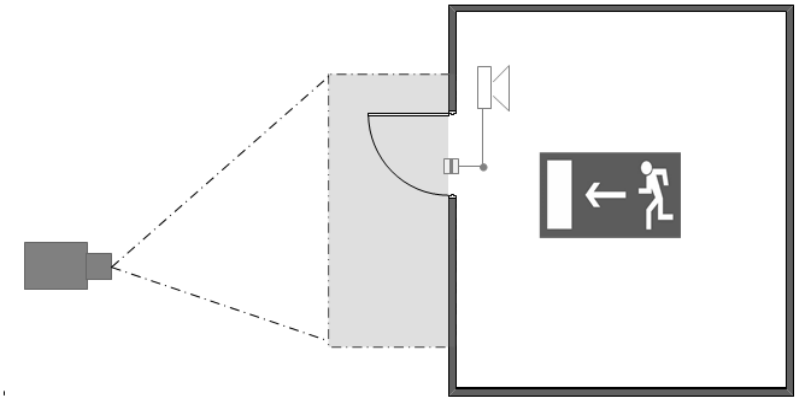


Figure 8 shows the same Emergency Exit as is shown in Figure 7, but now this door also needs to be used as an access point to the building. As its main function is to be an Emergency Exit, the number of the Typical is kept but a capital “A” is added. This door has the same functionality as the one from

figure 7, but with a specific operating instruction, namely the use of the door as an entrance with a badge reader.

Figure 8. Typical 12A: “Emergency exit with access-IN”



This emergency exit can be described by using the technical sheet as given in Figure 9.

Figure 9. Technical sheet for the Typical 12A from figure 8.

TECHNICAL SHEET	TYPICAL 12A	Reference	TF.XX.0022
	BPC400	Edition /Date	V008-26/03/2013
PROJECT:	Emergency Exit with access-IN		
Organisational measurements			
Yearly maintenance of all equipments Guards have to execute a guard tour every day to look for open doors.			
Physical measurements			
Access persons	Emergency door must be in accordance with the most restrictive standards of the zone, from whereat the emergency exit takes place.		
	Emergency door must be in accordance with the guidelines of the law		
Electronic measurements			
CCTV	When using this door there will be a trigger given to the CCTV to start recording all images during the time of the buzzer. (in this way one can find out who has used the emergency exit's)		
	At activation of an alarm the cameras will register the alarm so that a verification is possible and the recorded images can be analysed afterwards.		
Access control	At unauthorized exit activates an internal buzzer and report it to the person that the use is not allowed. A message is given to the monitoring team.		
	When a person wants to enter the building than he has to use a card reader. This reader will overrule the standard alarm functions of this door. The buzzer can be reset only by intervention of the monitoring.		
Intrusion detection	Emergency door is connected to the central system which is located in the control room.		
	Every move to this door will be reported as an alarm, the alarm message only in the event of evacuation will not come through. (overruling)		
	When you open the door to leave the secure zone is activated the siren		
	There is a sabotage sensitive magnetic contact present at the door		
Reporting measurements			
Monitoring will start the service reset and alarm handling.			

For calculating the budget of such equipment, an inventory of all items has to be made. In Table 1 all equipment for such an installation of a Typical 12A is summed.

Table 1. Required equipment for the Typical from Figure 8

TYPICAL 12A - Emergency Exit with access-IN	
Card reader	*1*
Magnetic contact anti-sabotage	*1*
Internal sirene with build in flash	*1*
PLC for logic of door	*1*
Camera external in housing (heated/ventilated) on support	*1*
Controller Access	*1*

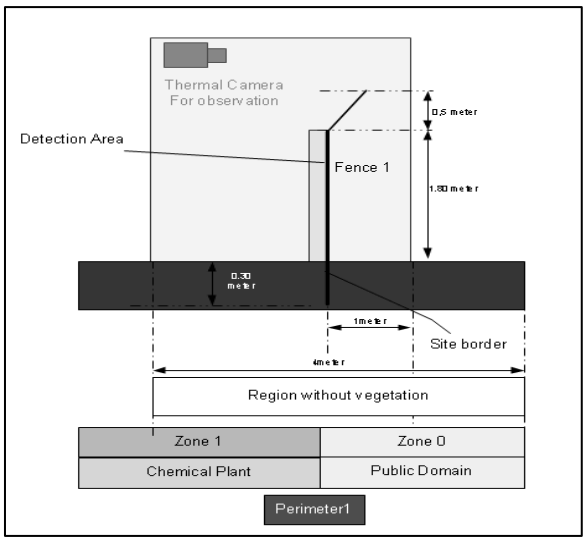
4.2. Perimeter Protection

Every ring of protection is made up of a perimeter and the corresponding zones (enter- and exit zones). The perimeter will have a specific resistance based upon the results of the so-called critical path method (see also earlier in this chapter). The critical path method is a step-by-step technique for security intrusion that defines the path an intruder could use to reach his or her goal. To define the critical path, an asset/attack matrix must be made up, and the path with the lowest detection and delay probability needs to be determined (Garcia, 2006 & 2008; Norman, 2010). To set up such a critical path analysis, the targets must first be defined. A target is defined as the location the adversary would like to enter and where he or she would like to commit an undesired act. The method further defines the time an intruder will need, considering the obstacles and the tools, to reach his or her target. This time will then be used to calculate the maximal intervention time for guards or police force to be on location. The way this resistance needs to be built up and the way the possible risks can be mitigated will be defined by the security manager of the plant.

The first perimeter, usually being the property boundary of the plant, is mostly a simple wired fence. The fence is a physical OPER measure. It is usually used to prevent trespassing attempts and for keeping out unwanted visitors. If it should also act as a perimeter with a certain protection against adversaries (such as burglars, terrorists, etc.), then a more appropriate fence type can be chosen. If it also has to prevent attacks from vehicles then it may be extended with an anti-ramming device like a barrier of concrete. However, preventing or mitigating attempted illegal entry should not be regarded as sufficient protection. Evidence of a potential trespasser should be available as promptly as possible. To this end, an appropriate perimeter detection system (see for example Figure 10) may be installed.

This introduces an electronic OPER measure. For chemical plants, the use of thermal cameras with VCA (Video Content Analysis) is suggested. As the premises of chemical plants are usually rather large, and often with trees and other vegetation present, tests indicated that thermal camera systems have the lowest rate of falls alarms when used as perimeter detection. Even in case of over-climbing and cutting of the fence this seems to be the best solution. Tests have revealed that well-organized intruders can overcome some of the other security countermeasures such as leaking coax or seismic pressure systems in several seconds without giving any alarm (also electronic OPER measures). A schematic drawing of such a perimeter protection is illustrated in Figure 10.

Figure 10. Schematic drawing of Typical perimeter 1 for a chemical plant

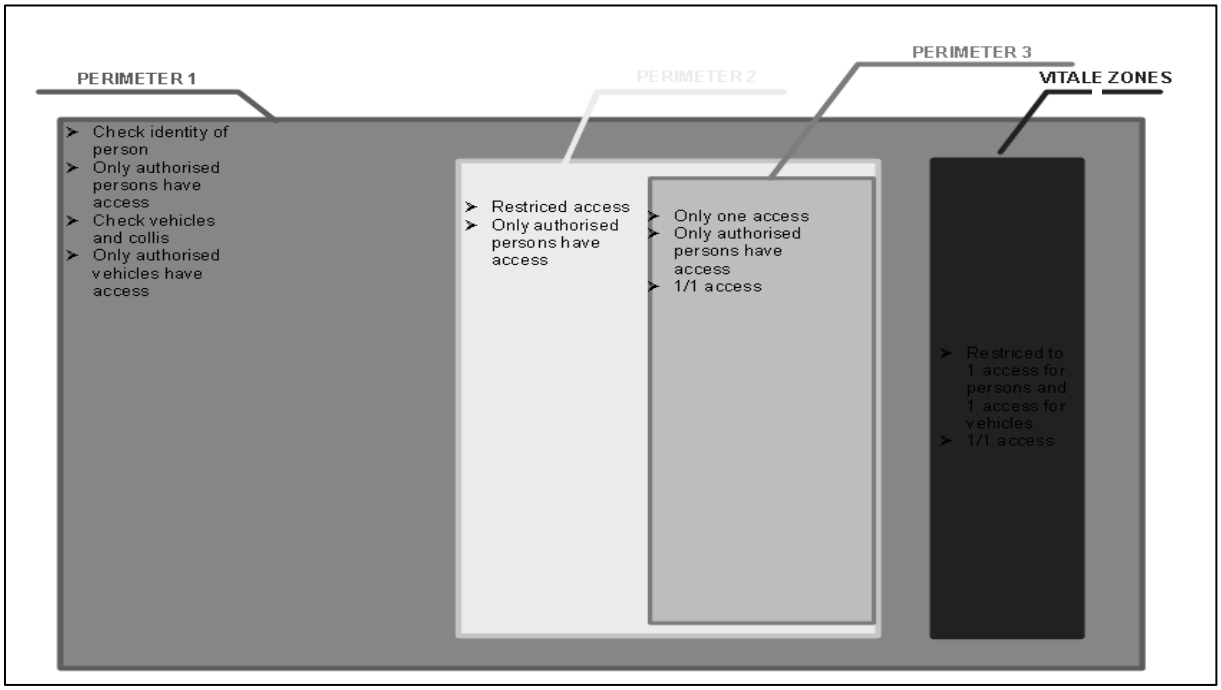


4.3. Access Control

Access control methods like these combine physical and electronic OPER measures in a single security system. The company security manual needs to guide the choice of an appropriate access system. It will indicate if a one-by-one access (that is, an access only allowing one person entering or leaving at one time) is required on a perimeter or just a protection to unauthorised access. Otherwise it will indicate if people have to identify themselves by means of a second verification system. Maybe there is also a need for installing an ‘anti-pass back’ (that is, a way to prevent people of accessing a site twice without leaving the site, e.g. handing over of badges to other people). This can be the case for example if the number of people in a certain location has to be counted, or if a person cannot access the plant if he does not possess the right certification, or if a person is not authorised to enter this specific zone.

All these parameters must be carefully defined before decisions can be made about a type of cards, doors, and what have you. These parameters will indicate if employees need to access the site by means of a man-height turnstile or a simple gate-door or no barrier. The number of users and the timeframe will indicate the type of the door as well as the number of access points. If a one-by-one access for every employee at the perimeter 1 is needed (e.g., having 500 people entering between 8am and 8:15am), then several turnstiles to let these people correctly in during this timeframe are required. This can be visualised as displayed in Figure 11.

Figure 11. Definition of access authorization for a chemical plant



Access control will help to define the access levels and the behaviour of the access. In a chemical plant it is important to foresee up-scaling of the access levels. Due to the possibility of this up-scaling, the behaviour of the access system can be changed in a few seconds. Usually, 3 levels are defined: level 1= normal operations; level 2= degraded operations; level 3= alarm. This will for example reflect in level 1 as an operational level where everybody has a common or standard access, when authorized. For level 2 for example there will be a limited access only for persons needed in this operational level. So this could mean that a person having an access for 24/7 in normal circumstances, no longer is allowed on the plant in special circumstances, or that the numbers of doors are restricted and that he or she cannot enter the 'usual' buildings.

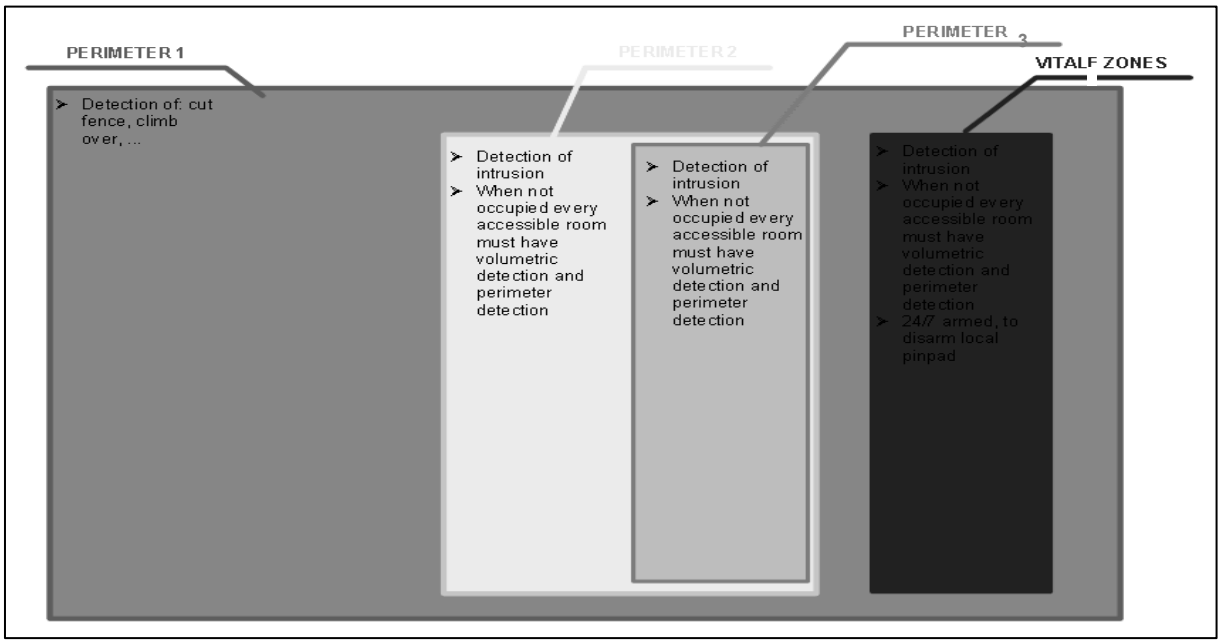
Another important issue in the part of access control is the possibility to use mustering points. These points must be equipped with 'readers', who have no access capabilities but who build up the list of all persons present on this location. Such an inventory of present people can be very useful for rescue workers searching people in the reactive and curative phase of an incident. The lists will be used to verify whether there are still persons missing. However, usually a one-by-one access is not possible as too many people have to enter a plant site at the same time. Therefore a "time and attendance" system coupled to the wages of the employees, may be a solution.

Access control is not only based upon the readers and the authorisation of having an access. It uses also doors. These doors must be of the same protection level as the fence. Obviously, it makes no sense placing a wooden door in a steel fence or placing a reinforced door in a Gyproc constructed wall.

4.4. Intrusion Detection

For intrusion detection systems are electronic measures in OPER. We will use the same setup as for the access control measurements. Figure 12 provides an overview of the described needs for this security measurement.

Figure 12. Definition of intrusion detection for a chemical plant



Most of the chemical plants work on a 24/7 regime. Intrusion systems will therefore be installed on the perimeter and/or in administrative buildings or those buildings who do not have a 24/7 regime (for example vital zones).

As the size of a chemical plant can be very large, the first point of detection should be installed on the first perimeter. However, intrusion can also start from the inside. The probability of each type of intrusion scenario must be defined in the security risk assessment process. Most often, a burglar alarm is installed in the buildings, whereas a perimeter detection system is established on the perimeter.
These systems should be connected to a central guarding room. Only this way the guards can react promptly after an intrusion. The faster there is the correct response after an alarm, the lower the probability of an adversary to be successful.

4.5. Camera Surveillance

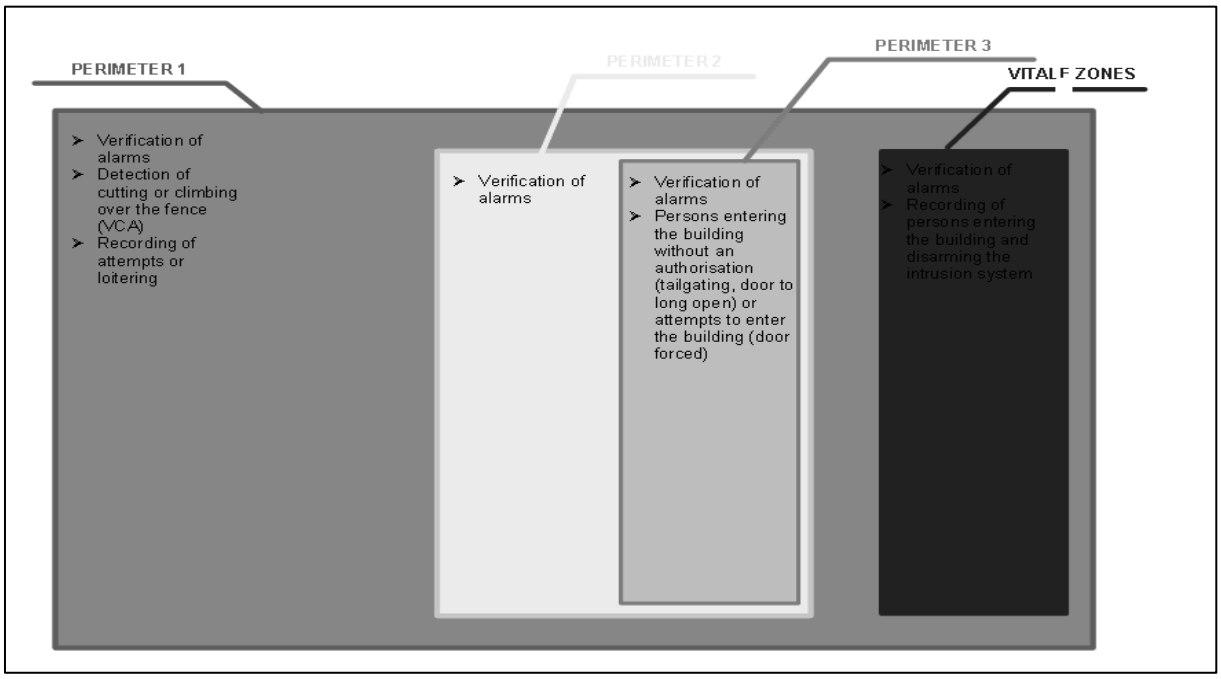
It is often not possible to put a guard at every door or at every location susceptible of an attack. This cost would be very high for any company, also for a chemical company. Other solutions to detect possible intrusions are thus required. Electronic systems for detection of intrusion are adequate but unfortunately not always relevant. For example a fence-wire has to cope with calibration and compensation problems due to environmental and product behaviour in outdoor installations. As these problems still generate a lot of 'unwanted' alarms, guards are needed for verification of these alarms. As guards are mostly not present on the location of the intrusion, an additional system must be put in place to aid them to prevent neglecting these alarms. Therefore it is important to install cameras who will be the eyes at the location of the guards. Camera's count as electronic measures in the OPER system.
Cameras can only visualise what they see. A correct description of the means and scope of the camera surveillance system is therefore important. The following should be defined in advance to overcome unusable images for the purpose of the camera surveillance:

- what must be viewed
- which part is important in the picture and which part not
- what definition is required (overview, detection, recognition, identification, …)
- who is viewing the images and on what basis (reactive, proactive, …)
- what can prevent the camera of viewing the correct images (plants, construction site, changes on the perimeter …)

Cameras are part of the overall security measures and by themselves they will of course not prevent the security incidents of happening. In Figure 13 some definitions of camera surveillance for a chemical plant are presented. Nevertheless every chemical plant has its own peculiarities and therefore definitions must be fitted to the result of the chemical plant's security assessment and security manual.
As can be seen in Figure 13, the camera surveillance system will mostly be used as a verification of the act. A camera will not prevent an incident of happening or catch the intruder during the act. It will,

in the best case scenario, deter an adversary committing an unwanted act. The integration of cameras with other security technologies is thus needed, especially in chemical plants where premises can be large and not always well illuminated at all locations. The absence of light can be indeed a problem for camera surveillance and it must be resolved using the correct techniques.

Figure 13. Definition of camera surveillance for a chemical plant



The visualisation of the images and the contents of these images can have a better performance by using intelligent VCA-techniques (Video Content Analysis). If combined with thermal cameras instead of standard cameras, even day/night, a better result is obtained in chemical plants.

Intrusion can be detected quickly, even sometimes before the actual intrusion takes place, when combined with the newest 4D/3D techniques called 'video image understanding'. Video image understanding is a technique that uses sensors and telemetry in 2D-images together with human behaviour analysis. It is even so that the combination of thermal cameras and VCA can be used for fire detection or gas detection. In this case thermal cameras will have a double effect and a reduced cost as they have a double functionality, especially in the chemical and process industry. Moreover, such thermal cameras are a nice example of an integration of safety and security needs in a chemical industrial area.

4.6. System integration

The necessity of integration of procedures, people and systems was already mentioned as the OPER principle. All the previous sections follow this principle. But there is also a need for integration between systems. Not only between two security systems, such as camera surveillance and access control, but between all security systems installed and used within a chemical plant, and between security and safety needs.

Most often the security manager will use integration for an interaction between fire detection and access control. It is obliged that some doors, in case of a fire, need to be unlocked or locked, to prevent the fire to expand or to enable people to escape to fire-free areas. This can be opposed to access control being a purely security-based solution. Access control is setup to prevent 'unauthorised' people to enter the plant, whereas fire detection is setup to leave the plant in case of a fire. Hence access control demands fail-secure locks where fire detection demands fail-safe locks. In this case the appropriate lock and access point must be installed so that everyone, in case of fire, has a free exit, but that the entrance is still secured and only available for those who have access.

This is of course only one part of the integration, even when it still is a very difficult one. For example, it was observed that after a flash fire alarm an intrusion was seen but was not detected due to the integration of the two systems not being setup properly. In most cases, the fire alarm will cause the power to be cut off from the access points and doors will be left unsecured. Hence, integration is more than setting up some hardware links: it is also about the interaction between systems that sometimes are not regulated. For example the use of thermal cameras for gas detection or the help of camera surveillance for an overview of the location of a fire and the additional escape routes. In a chemical plant it is very important that security people as well as firemen have a complete overview of the fire, its location, its extension region, the escape routes for people and also the possible routes for the fire brigade. For chemical plants it is important that part of the integration includes the activity inside the control rooms, not only between systems but also between people.

5. Discussion

This chapter describes a systematic development for a practical security system in the chemical and process industry. A specific contribution is the detailed description and analysis of risk-sensitive areas and so-called Typicals that function as security barriers. The detailed description aids the tracking of security measures and facilitates and even enables careful thinking about risks and then appropriate processes and other mitigation measures. We suggest that chemical companies wishing to assess their security situation, initially perform a gap analysis between the actual state of the plant and the ideal security situation as described above.

When the URS is defined, an inventory of the actual (existing) situation of the plant can be made. The plant's URS can be used while defining the correct definitions of the Typicals. A difference between the conceptual URS and the physical URS will be observed. For example there may be several types of gates in the fence to enable an entrance to a certain zone. At one time the gate may be a sliding gate, at another time it may be a bi-fold gate. The functionality of the gate will be the same, that is, a truck entering the site. But the technical specification will be different. Detection of the open/closed state of a sliding gate will be differently than for a bi-fold gate. This will define the difference between the USR and the Typicals. It will also impact upon the budget estimation for the proposed security systems. What is an appropriate budget allocation will vary with circumstance and in any event will depend on the findings from the gap analysis.

Once all Typicals are defined for the plant, the budget estimation can be commenced. For each Typical the technical equipment needs to be defined. This equipment typically combines several OPER measures and will then be used to fix a complete price for the Typical. Inventory of the site will provide a perspective on the situation as it is; the gap between this state and the to-be state. It also indicates the number of Typicals.

The combination of the number of Typicals and the 'to-be installed equipment' provides for a calculation of the amount of investment that is needed for the installation of the security system. These Typicals can be of help later, when changing the site or constructing a new building on this site.

6. Conclusions

To build an effective security design in the chemical- and process industries, it is essential to start from a structured security risk assessment that is recognized by people working in that industry. This will help in choosing the right concept for the needed security solutions and protection. Designing a correct security plan is based on this concept.

The design of so-called Typicals is suggested, and an approach where risk, behaviour and standards will interact on the roll-out of these Typicals, is proposed for drafting the security plan. For chemical plants, specific information will be needed, as these kinds of sites are often very large and several types of production processes take place on the same site, often using large amounts of various hazardous chemicals. The detailed description of risk-zones, PICER scenario's and Typicals based on the OPER system helps to keep track of security measures in the plant but also force analysts to think carefully whether their security plan provides full coverage of the risks. Whenever possible, it is

recommended to look for double functionalities of the technological equipment, as to optimize the security countermeasures' costs, and as to integrate security needs with safety requirements.

Recommended readings

The our knowledge, a security system that is specifically dedicated to bridge the gap between security and chemical- and process risks is absent outside the references made in this paper. Therefore, we cannot recommend further reading in that direction, however, we can point out some of the work that helps the reader understand the approach that is common in the chemical- and process industry that is followed in this paper. In Lee's handbook of process safety (Mannan, 2005) chapter 1 (§2.1 – 2.3) describe the background of the problem for process dangers but more relevant for this work: chapter 6 shows the design of risk-control systems in the process industries. Cameron and Raman (2005) show the preoccupation with numbers and risk but also show a specific concern in the design of management systems in chapters 3 and 11. The preoccupation with graphical information and maps, that is also present in this paper, follows from risk analyses in the process industries that use geographical risk contours (as shown in chapter 9 in Cameron and Raman, 2005). The layers-of-protection method that is used in process industries is fundamentally different than for security though lessons about the validity of barriers and the structured analysis of risk reduction can be useful in the security domain (Dowell, 2001).

References

API Recommended Practice 780 (2012) Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries, Document Draft, Washington: American Petroleum Institute.

Arata, M.J.Jr. (2006) Perimeter Security, San Francisco: McGraw-Hill.

ASIS (2012) Protection of Assets. Physical Security, Alexandria, VA: ASIS International.

Belgian Official Gazette (1990) Wet tot regeling van de private en bijzondere veiligheid (in Dutch), p. 10963.

Cameron, I.T. & Raman, R. (2005) Process systems risk management, Amsterdam: Elsevier academic press.

CCPS, Center for Chemical Process Safety (1996) Inherently Safer Chemical Processes. A Life Cycle Approach. New York: American Institute for Chemical Engineers.

CCPS, Center for Chemical Process Safety (2000) Guidelines for Chemical Process Quantitative Risk Analysis, 2nd edn. New York: American Institute for Chemical Engineers.

CCPS, Center for Chemical Process Safety (2003) Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. New York: American Institute for Chemical Engineers.

Dowell AM (1999) Layer of protection analysis and inherently safer processes, Process safety progress 18(4), 214-220.

Dowell AM (2001) Layers of protection analysis, New York: AICHE press.

Ellis J & Hertig CA (2010) The Professional Protection Officer. Burlington: Butterworth-Heinemann.

Fennelly LJ (2004) Handbook of Loss Prevention and Crime Prevention, 4th Ed., Burlington: Butterworth-Heinemann.

Fontaine F, Debray B, Salvi O (2007) Protection of hazardous installations and critical infrastructures – complementarity of safety and security approaches. In Linkov I. *et al.*, Managing Critical infrastructure Risks, 65-78, London: Springer.

Gabbar HA, Suzuki K (2004) The design of a practical enterprise safety management system, Dordrecht: Kluwer Academic Publishing.

Garcia, ML (2008) Vulnerability Assessment of Physical Protection Systems, Burlington: Butterworth-Heinemann.

Gill M.(2006) The handbook of security, New-York: Palgrave-Macmillian.

Holtrop D & Kretz D (2008) Onderzoek Security & Safety: een Inventarisatie van Beleid, Wet- en Regelgeving. In Dutch. The Netherlands: Arcadis.

Institute of Security Belgium (2013), Handbook "Basisopleiding bestemd voor Leidend Personeel van beveiligingsondernemingen" (in Dutch), Brussels: Ministry of Home Affairs.

IAEA (International Atomic Energy Agency) (1996) Defence in Depth in Nuclear Safety, Vienna: IAEA.

Kapp EA (2012) The influence of supervisor leadership practices and perceived group safety climate on employee safety performance Original Research Article, Safety Science 50(4), p. 1119-1124.

Landoll DJ (2006) The security risk assessment handbook. Boca Raton: Auerbach Publications.

Mannan S (2005) Lee's loss prevention in the process industries, Burlington: Elsevier Butterworth-Heinemann.

Meyer T & Reniers G (2013) Engineering Risk Management. Berlin: De Gruyter.

Norman, TL (2010) Risk Analysis and Security Countermeasure Selection, Boca Raton: CRC Press.

Reniers GLL (2010) Multi-plant Safety and Security Management in the Chemical and Process Industries. Weinheim: Wiley-VCH.

Reniers GLL (2011) Terrorism security in the chemical industry: results of a qualitative investigation. Security journal 24:1, p. 69-84.

Reniers GLL, Herdewel D, Wybo J-L (2013) A Threat Assessment Review Planning (TARP) decision flowchart for complex industrial areas. In press in: Journal of Loss Prevention in the Process Industries.

Talbot J & Jakeman M (2009) Security Risk Management body of knowledge. New York: Wiley & Sons.

Wu T, Chen C, Li C (2008) A correlation among safety leadership, safety climate and safety performance Original Research Article, Journal of Loss Prevention in the Process Industries 21(3), p. 307-318.