INTERNATIONAL JOURNAL OF
COASTAL & OFFSHORE ENGINEERING
IJCOE Vol.4/ No. 3/Autumn 2019 (17-31)

Available online at: www. Ijcoe.org

A Systems Engineering Approach to Physical Security of Oil & Gas Installations

Sirous F. Yasseri

Brunel University London; Sirous.Yasseri@Brunel.ac.uk

ARTICLE INFO

Article History:
Received: 25 Mar. 2020
Accepted: 06 May. 2020

Keywords:
Physical Security
Security Assurance
Systems Engineering
Defence in depth
Security threats

ABSTRACT

A fundamental challenge facing security professionals is preventing loss; be that asset, production, or third-party losses. This is not dissimilar to what safety professionals have to face. Techniques and methodologies used by the safety professionals could potentially benefit the security experts. Physical security is about taking physical measures to protect personnel and prevent unauthorized access to installations, material, and documents, which also include protection against sabotage, willful damage, and theft. The characteristics of physical security controls include measures for deterrence, detection, delay, and responses aimed at risk mitigation and enhanced operational effectiveness.

This paper outlines a systems engineering framework for implementing security goals, which are suitable for meeting the challenge of providing physical security for complex systems, which includes oil and gas facilities. The proposed framework builds security requirements into system requirements and moves it in parallel with the system development for the entire system's life cycle; particularly during the concept and design phases. This is a top-down process for use by a multidisciplinary team of security, operations, and industry experts to identify and prevent the system from entering into vulnerable states which could lead to losses. This framework shifts the focus of the security analysis away from threats, being the immediate cause of losses, and focuses instead on the barriers, i.e. safeguards that prevent systems from entering into vulnerable states, which would allow an unfolding event to disrupt the system leading to loses.

The need for such a method comes from the recent experience of the securing complex systems that combine a large amount of hardware, software hazardous materials, and control elements. The method takes advantage of systems engineering and encourages the use of goal-based security requirements instead of using a strict prescriptive approach that is common among security professionals. Using this framework helps both to identify threats associated with the system, as well as weak points within the system. This framework also encourages communication between the security professional, safety engineers, and system designers. This paper draws from the existing literature as listed in the references.

1. Introduction

Physical security is concerned with constructing systems that remain operational despite intentional (willful, malicious) or unintentional (human error, equipment failure,) events [44, 46, and 50]. The objective is to design and build complete systems that proactively and reactively limit vulnerabilities and survive undesirable events; so that the system's mission is assured.

Physical security is an integral part of security engineering. The ISO/IEC 21827 standard [23] identifies the following list of sub-disciplines:

- Operations security
- Information security
- Network security
- Physical security
- Personnel security
- Administrative security
- Communications security
- Emanation security
- Computer security

This paper's focus is on physical security.

The US Department of Defence (DODI5200.44 [12]) defines the term System Security Engineering (SSE) as: "*an element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities*". A comprehensive survey of the issues and a detailed reference list is provided by Baldwin [6] and Baldwin et al. [7]. DODI5200.44 [12] defines two perspectives

for systems security engineering. First, it explains how criticality analysis and security engineering are integral to the technical and systems engineering management as per ISO/IEC 15288 [24] Another perspective of the guide is the overlay of security throughout the life-cycle. It is critical to address security requirements [16] while the largest possible ease of reconfiguration of the system exists, and also to ensure the technical maturity of the security solution throughout the vendor selection, acquisition and construction phases. This understanding should also help with setting and enforcing measures for security.

Security system designers have presented physical security as a tactics problem in the past [53], focusing only on how best to defend assets against threats. While tactics are necessary, this viewpoint misses the primary objective which is the systems' ability to function after an attack, i.e. what is at risk. Defending an asset is not a goal in itself; rather it is a means of safeguarding services and missions against disruptions oe outage. Reframing the problem into one of strategy [53] would produce better outcomes. Such reframing requires to shift most (but not all) of the security analysis away from guarding against attacks (which is tactics) and focus on the broader socio-technical vulnerabilities of a system that allows disruptions to propagate throughout and disable the system (which is strategy) [53]. In other words, rather than primarily focusing the majority of the security efforts on threats from adversary actions, which are beyond the control of the security professionals, focus should be on limiting system's vulnerabilities that are under the designers' control, especially at early phases of a project.

2. The State of the Practice

Security engineering involves several inter-disciplinary requirements, such as stronger physical structures, computer security, tamper-resistant & error-tolerant hardware, psychology, supply chain management, and law [4 and 47]. Security requirements differ greatly from system to system and will primarily depend on the socio-economic and geopolitics of the system environment [50]. System security [40] often has many layers to control entry, authentication of people accessing it, deter & delay, accountability chain, vulnerability, deception, secrecy, and damage tolerance. The challenges are protecting the right items and in the right way [29 and 35]. This paper builds on the idea that the primary objective of System Security Engineering (SSE) should be to minimize, or contain, system vulnerabilities to known or postulated security threats, and to ensure that systems during their entire life cycle are protected against these threats [13 and 27].

The principle idea revolves around the belief that an initial investment in mitigating security vulnerabilities, and the ability to take countermeasures, is cost-effective in the long term. Further, SSE provides a means to ensure adequate consideration of security requirements is made, and those specific security-related requirements are incorporated into the project requirements; not bolted on at a later stage. Security requirements should be identified early in the project (where they can be adequately addressed), implemented, and verified in the course of the system development.

The System Security Engineering Management Plan (SSEMP) is a key document to develop for SSE [27]. The SSEMP focusses on the planning of security tasks for a system, the organizations, and the installation's security. The goals of the SSEMP are to ensure that pertinent security issues are raised at the appropriate points in the project's life cycle, to ensure adequate precautions are taken during the design, implementation, testing, and operation; as well as to ensure that only a tolerable level of risk would be incurred due any introsion during the system life cycle. The SSEMP details the primary tasks required for certification & qualification, preparation of documents, evaluation of the system [15], and detailed engineering. It also identifies the responsible and accountable organizations for each task and presents a schedule for the completion of those tasks.

The SSEMP explains the initial planning of the proposed SSE work scope; detailed descriptions of SSE activities performed throughout the system development life cycle; the operating conditions of the system; the security requirements; the initial SSE risk assessment (including risks due to known system vulnerabilities and their potential impact on continuous operation); and, the verification& validation aproach and results.

An initial system security Concept of Operations (CONOPS) may also be developed [22]. This document explains how system security should operate.

The last step before handing over the system to the client's operations team is the system validation and assurance [14]. NATO AEP-67 [33] defines system assurance as:

"…the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle... This confidence is achieved by system assurance activities, which include a planned, systematic set of multi-disciplinary activities to achieve the acceptable measures of system assurance and manage the risk of exploitable vulnerabilities."

Since most modern systems rely on software for some of their functionality [24 and 26]; software assurance becomes a primary consideration in system assurance

[3]. The software assurance is a "*level of confidence that software is free from vulnerabilities, either intentionally built into it or accidentally inserted sometime during its lifecycle, and that the software functions as intended*" [11].

This paper draws from the existing literature to build a systems engineering based framework for the physical security of petroleum installations.

Two approaches are commonly used for improving security during the project development and assurance phases before handover to the client, which are prescriptive and goal-based (or performance-based) approaches [1 and 2]. In the first approach all security requirements, analyses and assessments are aimed at ensuring that hazards associated with the system are controlled, removed, or at least mitigated by using predefined scenarios - this is a threat-based approach that is well reflected in the military standards. The second approach focuses on the goals of security, namely what, how, and why we are doing something. As such the focus is on early security requirements [9 & 47] at the conceptual phase of the project. Later, during project development, the system requires verification and validation to prove that it complies with the security requirements; allowing some modifications if needed. With this approach, security goals are set at the select phase and verified during the define phase [51]. This goal-based approach is gradually replacing the prescriptive approach as it becomes more and more irrelevant to modern complex systems.

Security professionals draw heavily on language, metaphors, and models from long standing military approaches. There is a distinction in military doctrine between tactics and strategy. Strategy can be considered as the art of gaining and maintaining a lasting advantage. In contrast, tactics are a prudent means of achieving a specific objective. Tactics are focused on threats, while strategies are focused on outcomes [53]. Means of achieving an objective is tactics, in contrast, the overall campaign plan is termed strategy, which could involve operational plans, actions, and decision-making that shapes the tactical execution. Strategy and tactics are complementary and thus have an intertwined existence. In military terms, tactics are the use of armed forces in engagements, while strategy is the use of engagements to achieve the overall goals. Strategy and tactics are both needed to achieve target goals and objectives. The strategy is the path or bridge for going from where we are today to the destination. It's our general resource allocation plan [53].

Most current security policies generally follow tactics models, namely security analysts will identify some immediate causes that will provide a reason to establish a barrier along the path of a probable event [8]. This type of approach is often described as the "defence-in-depth" concept [21] and is commonly used in security literature as a framework for conceptualizing the goal of security practices. This is a necessary part of securing a system, but it misses other elements of controlling the security risks.

Exploiting vulnerabilities by attackers cause the loss (i.e. a threat); tactics consider threat as the cause of the loss [20]. According to this line of thinking, the loss is when a threat successfully disables several barriers to reach its target [44]. Loss prevention, then, is dependent on how accurately security analysts can identify potential attackers, their motives, capabilities, and strengths. Keeping this point in mind, security analysts will analyse their systems to determine the most likely path that attackers may take to reach their target. Resources can then be allocated to place barriers along that path to prevent losses. This is a causal chain-of-events model which is also used in safety engineering, where the attempt to avoid accidents is focused on breaking the chain, by either preventing individual failure events or erecting barriers to prevent propagation [49].

This threat-based approach [20] is useful for identifying and countering security threats against a single, well-defined, and well-understood attacker or asset. Once an adversary's course of action is identified, the security analyst can provide advice on how best to allocate limited resources to prevent the attack and break the chain. The idea is based on a chain of events, which believes that if one link is broken then the event can't take place. In other words, a high level of threat-understanding enables security analysts to predict not only where an adversary will attack, but also the logical and physical infrastructures required to thwart the attack, which heavily depends on the experts' opinion. Systems designed only based on experts' opinions often lead to unmaintainable, unreliable, and non-rigorous systems. Many methodologies and procedures were developed to counter this viewpoint. Issues addressing this approach are discussed by Plant [38].

The Principle of Defence in Depth [48] for physical protection [11] is built on the idea of building several layers and protection methods (structural or technical, personnel, and organizational), that have to be overcome or circumvented by an intruder to achieve his objectives. The protection of the nuclear power plant is based on the concept of Design Basis Threat (DBT) [20] for the physical protection of a Nuclear Power Plant (NPP), which is protecting a facility against the objectives of an adversary. The physical protection of an NPP is based on many different protection measures, structural and other technical, personnel, and organizational measures, installed and organized in different areas of the facility. The protection measures depend on the consequences for the facility as well as the type of attack. The DBT is based on the maximum

credible threat which an organization is expected to control. Beyond that requires government intervention.

3. Defence-in-Depth

The concept of defense-in-depth follows the *Swiss cheese model* for an accident [17]. Each slice of cheese represents a barrier or a control measure which is assumed to be imperfect (i.e. with holes), where each hole represents some bypass (circumvention) or evasion. Employing the Defense-in-Depth concept results in the stacking of barriers, such that each additional stack reduces the exposure and thus reduces the overall risk, Figure 1.

These overlapping layers of protection have been a fruitful approach since it ensures that a "core" set of scenarios is always studied and that the "core" is continually updated by input from the teams studying new emerging threats. The risk of overlooking a potential threat is thus minimized. Success depends on correctly identifying all threats and having barriers in place to impede them all.

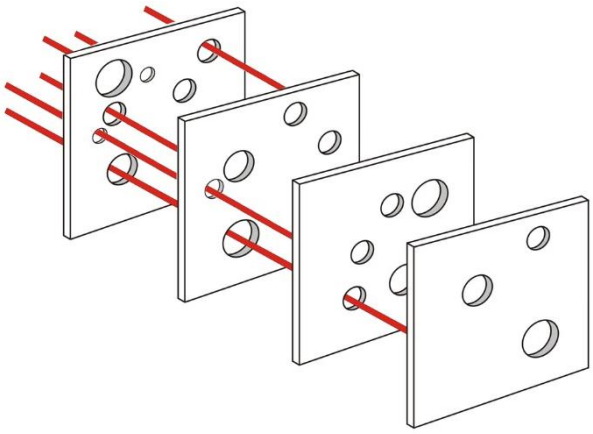

Figure 1. The concept of defense in depth; showing possible flaws in each layer.

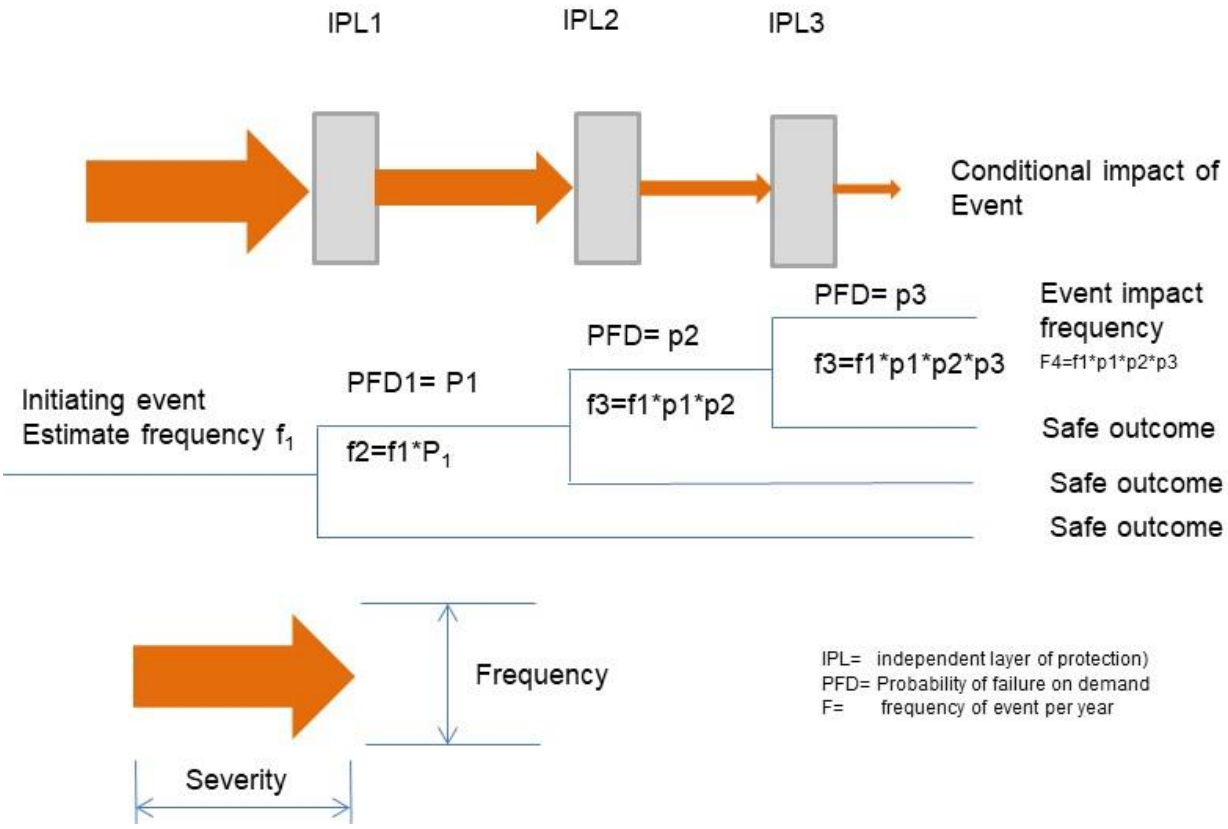

Figure 2. Reduction of severity and frequency of damage using multiple lines of defense (or layers f protection)

When scenarios are compiled, the attack event is coupled with a description of what could happen if an attacker proceeds to the inner domain without being challenged. Each scenario can contain several "attack-consequence" pairs and may have multiple paths to the target. The consequence may be then assessed for severity and frequency. The "bow-tie" [8, 36 & 37] is a suitable method for representation which details the initiating event and the safety barriers which may be present. The "bow-tie" operates as a fault/event tree, taking into account the "ANDs" (events or conditions which must both be true for a hazard to develop) and "ORs" (events or conditions, either of which, if true will allow a hazard to develop) [8].

Lines of defense (or layers of protection) analysis operate as shown in Figure 2. When addressing barriers, it must be assured that its rules are robust enough, and their independence must be guaranteed before they can be considered acceptable. Care needs to be taken when a single consequence can be caused by several different initiating events, or a single event may have multiple paths, thus affecting the cumulative risk. Whilst this might prove to be difficult to reconcile, most practitioners take a very conservative view of threat frequencies and Probability of Failure on Demand (PFD) [17] for independent layers of protection or barriers, which ensures that overall risks are tolerable.

In the example shown in figure 2, the impact event frequency is the product of the original initiating failure event frequency and the PFDs of the 3 lines of defense. As each layer is called upon to function, the failure frequency of the entire system becomes progressively smaller.

4. Security Risk

Risk assessment combines risk analysis and risk management, using a systematic process for hazard identification and determining their consequences, as well as how to cope with these risks. Numerous methodologies were devised for the risk assessment, focussing on different types of risks or different areas of concern. For example HAZard and Operability study (HazOp); Fault Tree Analysis (FTA); Failure Mode and Effect Criticality Analysis (FMECA); Markov analysis (Markov); etc. These methods are to a great extent complementary. They cover all phases in the system development and maintenance process. In general, qualitative methodologies for analyzing risk are effective in identifying risks, but they cannot account for the dependencies between events. Tree-based techniques, however, take into consideration the dependencies between events.

The security risk is defined as:

$$Risk\ (R) = [Threat(T) \times Vulnerability\ (V)] \times Consequence(C)$$

Terms in this equation are defined:

• Threat: a measure of the likelihood that a specific accident or attack will occur.

• Vulnerability: a measure of the likelihood that various types of safeguards fail.

• Consequence: the magnitude of negative effects in case of an accident or successful attack.

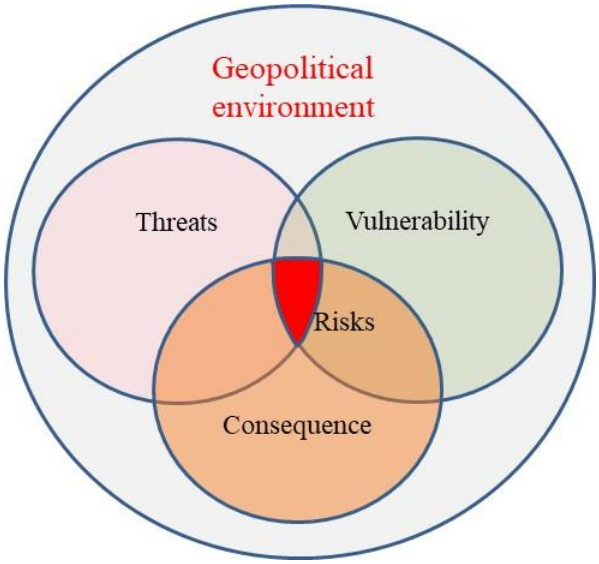

Figure 3. Risk definition as the intersection of threats, vulnerability, and consequences. All three elements may be used to make all risks as low as reasonably practicable (ALARP).

The threat, vulnerability, and consequence analysis [8] is an interactive approach to identify areas subject to high threat levels, extreme vulnerabilities, and high consequences overall, namely the intersection of these causes security concerns (Figure 3). These three elements should be considered in the geopolitics of the facility's location. What should be looked at are summarised below

Threat:

• Understand where terrorists target their activities.

• Typically based on intelligence information.

• Security responses are dependent on available information.

Vulnerability:

• Assessment for critical assets.

• Identify weaknesses/gaps for each attack scenario.

• Identify potential mitigation measures.

Consequences:

• Different types of consequences, i.e. health, environment, economy, and social aspects.

• Short and long-term consequences.

• Economic dimension, e.g. loss of productive capacity and availability

• Political dimension, e.g. stability, geopolitical issues.

The Security Assurance [30, 32, 51, and 52]requires that security measures must be implemented with the intent of providing long-term, continuous protection. New risks and vulnerabilities are introduced at an alarming rate with new technologies being developed and implemented just as fast. The skill, sophistication, and motivation of intruders seem to be increased proportionally. The critical challenge is to keep

security configurations current with continual updating. The protection is accomplished by establishing multiple defensive layers (or control measures) around the critical perimeter.

An example of hazards faced by oil & gas[5] facilities is listed in Table 1. The rest of this paper describes how to manage a facility's security concerns during the development phase.

Table 1: Examples of hazards threatening oil & gas facilities [5]

Technological	Natural	Willful (malicious) acts
✓ **Internal** o Aging & corrosion o Fire & explosion o Material failure o Corrosion o Inadequate design o Operator error o Excursion beyond design parameters ✓ **External** o Domino effect for nearby o third party groundwork	Flood Hurricane Earthquake Landslide Ground movemen	Hostile governments Terrorist attack Criminal acts e.g cybercrime of sabotage

5. Systems Engineering V-Model

Systems engineering [31] is an interdisciplinary process that assures the customer's requirements are satisfied. The lifecycle of an oil & gas facility has seven phases: (1) appraise, (2) concept development & selection, (3) front-end engineering, or defining, (4) detailing, fabricating and installing, (5) system integration and testing, commissioning (6) operation, maintenance and modification, and (7) disposal or replacement. The system life cycle may vary from operator to operator, but it would look like the upper section of Figure 4. Whatever form the life cycle takes, requirement analysis is the first step in this process. Concept development, which takes place in the select phase, is the high-level process of determining, understanding, and shaping customer needs.

The V- model describes the activities and results that must be produced during development (Figure 4). The left-hand of the V represents the system specification stream, where the system requirements and the system and subsystem or component designs are specified. The designed components are then fabricated and installed at the bottom of V. Component fabrication is followed by the testing stream in the right-hand of the V, where the gradually evolving and growing system is verified against the specifications defined in the right-hand of the V.

The V-model separates the disciplines of systems and design engineering. This way, top-down and bottom-up development approaches are integrated into the V-model. That is, the system is specified top-down and then the subsystems are integrated bottom-up. Working closely with client engineers, the requirements are elicited, analysed, validated, and documented. At the same time, the security needs of the system must be identified and added to the client's technical needs [34].

Technical, economic, and political feasibility, as well as security issues, are assessed at the appraise phase (Figure 4). In the next phase, known as the select phase, alternative concepts that meet the project's purposes and needs are explored, and the best concept is selected and justified. At this phase, security must be part of decision criteria. The project stakeholders reach a shared understanding of the system to be developed and how it will be operated, maintained, and protected [34 & 52].

Requirement analysis [16] (both technical and security) provides a framework for understanding the purpose of a system, the contexts in which it will be used, and how to keep it secure and safe. In seeking to describe the security requirement of a system, it is necessary to look beyond the system itself, and into the activities that it will support as well as the socio-economic and geopolitics of its environment.

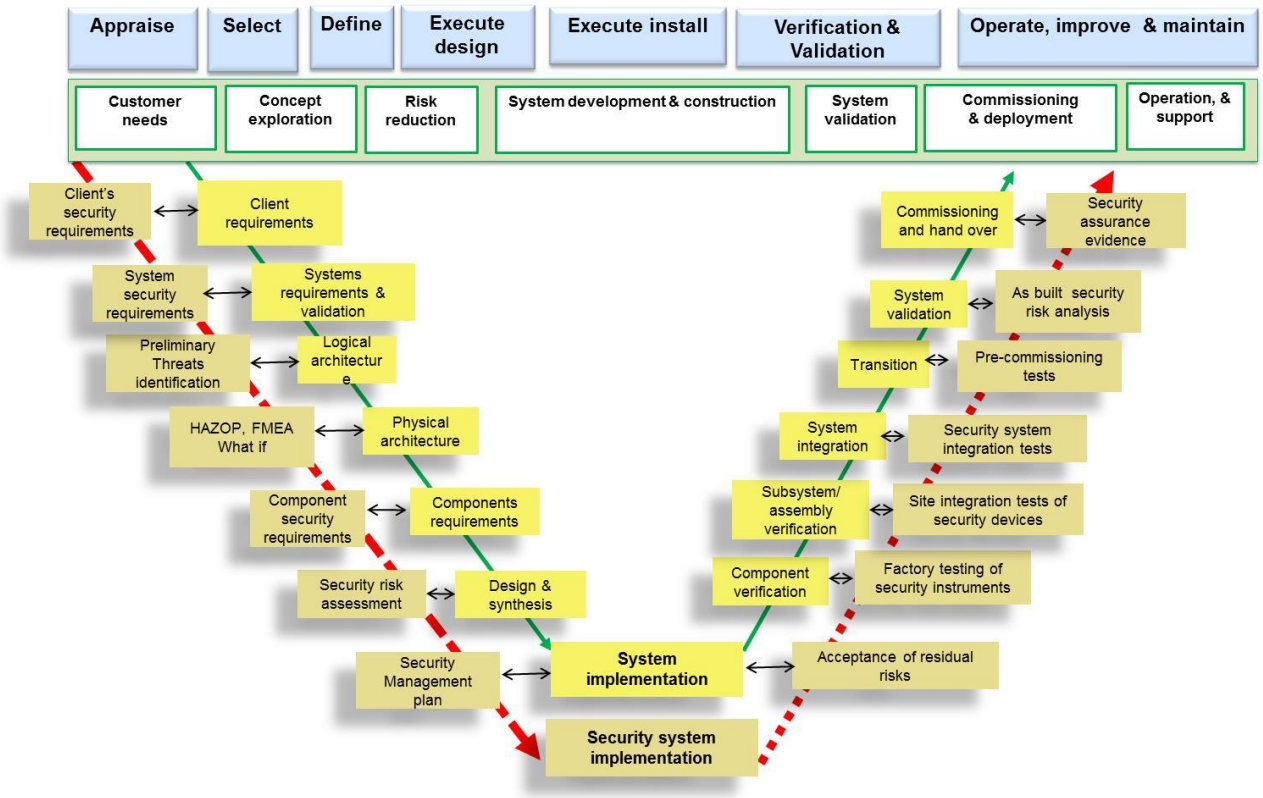

Figure 4. The V-model for the life cycle of an oil & gas project.

Requirements engineering refers to eliciting, specifying, analysing, accepting, validating, and managing the project requirements while considering the user, technical, economic, political, security, and business needs. Ideally, each requirement from the highest to the lowest level of the project must link to a parent

The client's security needs are used to set the initial security requirements. Initial security validation is done to ensure the selected requirements are sufficient and necessary for the protection of the installation. In addition to performance analysis of the security system using risk analysis, such as FMEA, Fault Tree Analyses, and Probabilistic Risk Analyses, to ensure the design will be robust and resilient.

Every security requirement must be traced to the means of its implementation, and every security system must be traced back to one or more of its security requirements. This mapping of security requirements to its implementation may be one to one or one to many [25], which is the traceability analysis.

6. Systems Engineering for Security

The design of safeguards for system protection requires a more formal methodology to support the achievement of objectives and traceability [25]. A systems engineering process can provide a framework within which different technologies can be implemented to design and evaluate the effectiveness of the security systems. Implementing such a process early in the development can save costs and prevent using less effective bolt-on security systems.

The elements of the systems engineering process envisioned for a design for security are shown in Figure 5. The initial step is to determine the security objectives (or security requirements), which includes the client's requirements, regulatory requirements, characterization of the facility, threats analysis, and identifying the targets including system vulnerabilities. The next step is the design of the security system, which includes identifying system elements to perform the detection, delay, and response functions [41]. The final step is to analyse and evaluate the design for all threats. Based on risk analysis results, the system design is modified, by including barriers (or control measures) until a desirable (optimised) compromise is obtained. The following sections describe each step in more detail [27].

Identify Security Objectives: Designing a protection system for a project begins with identifying security requirements, namely what has to be done, why, and how to do it? The security requirements are in addition to the client's operational requirements for the project. The primary focus of a protective system is to detect malicious intention and identify the perpetrators before any harm is done. This step may be complicated due to regulatory requirements and the continually changing nature of the threat. The step addresses four primary areas: regulatory requirements, facility characterization, threat definition, and target identification:

- In addition to the specific client's security requirements, the project must also comply with the regulatory requirements regarding project safety & security [39], public security, and environmental concerns.
- Facility Characteristics i.e. its purpose and general layout are needed to provide the context for more detailed protective system analysis. Characteristics such as schedule and procedures for operations, and the use of employees, among other factors, should be considered.
- The threat definition may be one of the most difficult parts of the design as many different threats exist, and adversary capabilities are constantly evolving. The adversary could be a state or non-state actor(s). Motivations, knowledge, equipment, training, and the number of adversaries are all factors to consider. Threat definition for safeguards should include sabotage.
- Target identification (vulnerable areas or critical equipment) would involve generating a list of items, flow streams, or process areas to be protected (vital zones). This list includes the location, size, and characteristics of the stored material. In principle, this is collectively referred to as the system vulnerabilities

Protective System Elements: The primary function of the protective systems is blocking, delaying, and response. The need exists to develop performance testing and validation of the types of equipment that could be part of an overall protective system. Primary protection measures are:

- Surveillance, detection, and alarm. Detection which centres on surveillance also includes alarms and communication and increasingly surveillance.
- Delay, impede & block paths to the target. Blocking is restricting access of non-authorised people reaching a vulnerable area

Verification and Validation (V&V): The final step is verifying each element of the security system by testing, as well as verification of the integrated system. When the entire system is verified, which ensures that the system is built according to the plan, then it must be validated, i.e. if the as-built security system is the right one for the facility. This is done using scenarios and case studies. Proper engineering design does not rely completely on analytical or numerical models but rather uses people to make sure the design meets the desired objectives.

The V&V strategy consists of sets of actions, each one of which is a kind of trial, test, or inspection. There may be several actions defined against each requirement.

Each action should consider the following aspects:

• The kind of action that would be appropriate for the requirement;

- Response plan (rules of engagement): Means of responding to threats and their state of readiness
- Control of hazardous materials and the type of harm it can inflict.

The following issues are also addressed:

- Operation monitoring, which also provides data regarding material accountability. Loss of material is reported to the security management
- Alarm testing and assessment. Alarm assessment may include lower limits of detection and the detectability of diversion scenarios by attackers. If an alarm is triggered, a method must be in place to recognize false alarms. The possibility of disabling the alarm system by saboteurs must be considered.
- Alarm display and communication – The final part of detection is that the alarm must be reported or communicated to the party of interest.
- Exit Delay – Safeguards are only concerned with exit delay. The plant can be designed to make it difficult or time-consuming to get in and out (except via the designated routes) to give enough time to respond if an event is detected.

Barrier Analysis: There must be at least one barrier or control measure for each threat, physical (e.g. wall) or instrumented, e.g. automatic shutdown. Generally, more than one barrier is needed to reduce the risk to a tolerable [17] level (Figure 5). In this analysis, risk should also be shown to be ALARP, namely as low as practicable, [28 & 36]

Risk Analysis: The purpose of risk analysis is to determine the level of the residual risk and if it is tolerable, as well as the effectiveness of the security system. If unacceptable then go back and rethink

• The stage at which each action could take place – the earlier the better;

• Any special equipment that would be needed for the action;

• What would constitute a successful outcome?

If it proves not to be fit for purpose, then the system designer must go back to make changes as needed until the desired performance objectives are met.

Diversion Path Analysis: An infinite number of diversion scenarios are possible [14], but only a small number may be probable. Diversion path analysis is a difficult step because it depends somewhat on the imagination of those involved in the design. Part of this analysis includes the probability of occurrence and response of the systems.

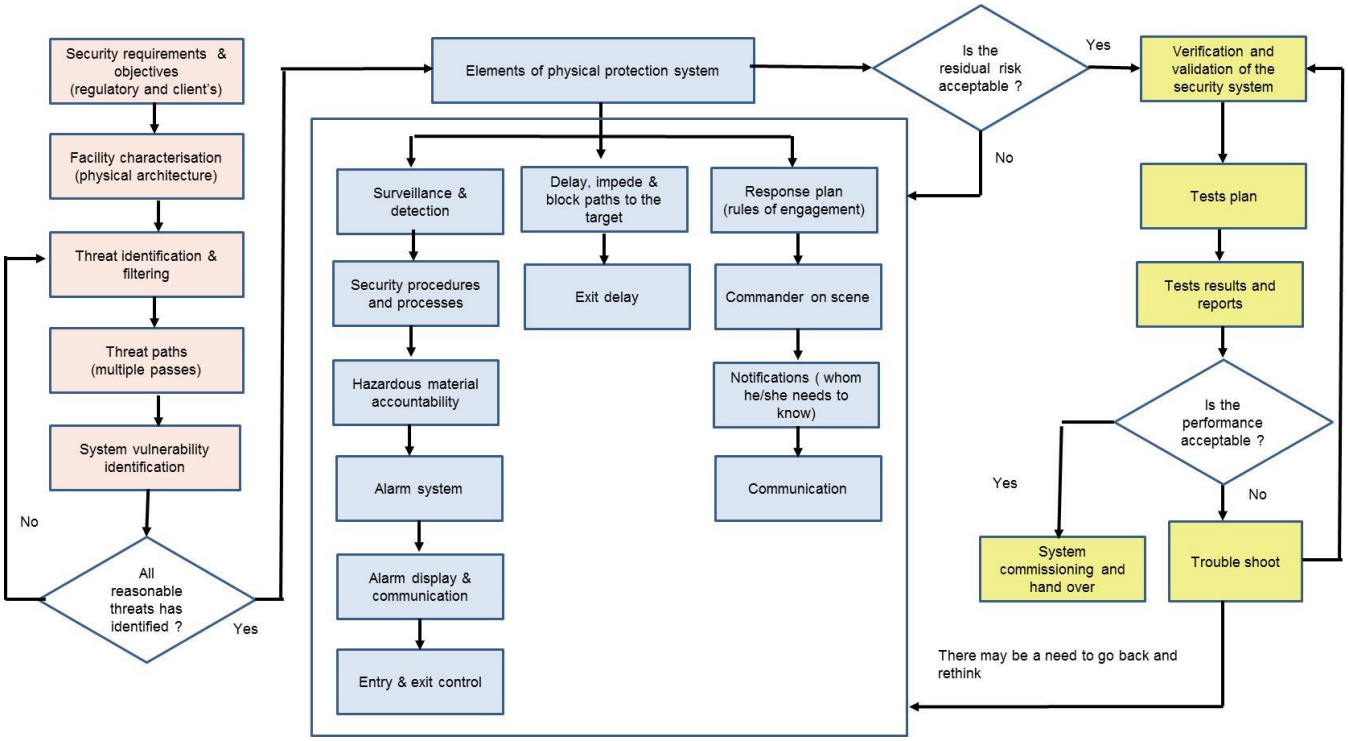

Figure 5. Elements of the systems engineering process envisioned for security design

7. Scenario Selection

There are several methods for selecting scenarios or threats. Hazard and Operability Study (HAZOP), Failure Mode and Effect Analysis (FMEA), and "What if" are just three examples. Some companies have been able to set up libraries of standard scenarios for their studies. This is particularly common where a company uses a similar installation in several different establishments.

FMEA [5 and 42] is based on the concept of the cause-effect chain. Every failure mode is related to a failure cause, and conversely, the effect of each failure is related to a failure mode which causes such effect. A failure effect leads to an unintended situation. The severity defines the importance of the scenario. The frequency relates to failure cause (threat) and effect, and it describes the likelihood of the event (threat).

The Failure Mode and Effect Analysis (FMEA) is a structured technique that is used to investigate security threats and their effects. The aim is to identify potential weaknesses of a system and find means and ways of improving the protection. A system is decomposed to its basic subsystems (or components), and their protection requirements are identified using failure modes to examine their causes and effects [42].

Effective security processes require constant updates to combat the rapid evolution of malicious technology and the ever-expanding range of threats. FMEA originally designed by NASA, and popularized by the automotive industry, has played a key role in helping manufacturers to achieve extremely low fault rates. To achieve similar results in system protection, one should think of security functions as processes, and apply FMEA to prioritize resources towards protecting vulnerable areas whose failure would lead to the worst consequences if damaged.

The advantage of FMEA is the ability in helping to think about all potential failures inherent to the processes or system. FMEA enables leaders methodically to:

•Brainstorm potential failures.

•Evaluate the severity and likelihood of failures.

•Determine the effectiveness of corrective actions in detecting failures.

•Identify appropriate measures to mitigate and prevent failure mode effect severity, as related to the defined boundaries of the system under consideration.

The basic approach (Figure 6) to carry out an FMEA is described in IEC 60812 [19].

Definitions according to IEC 60812 [19]:

•Failure cause: why did the item fail?

•Failure mode: the way that an item fails.

•Failure effect: the consequence of a failure of an item, affecting the operation, function, or state of the item.

•Failure severity: Intensity of the failure effect on item operation, on its surroundings, or the operator.

•Failure criticality: a combination of the severity of an effect and the frequency of its occurrence, or other attributes of a failure such as a measure of the need for addressing and mitigation.

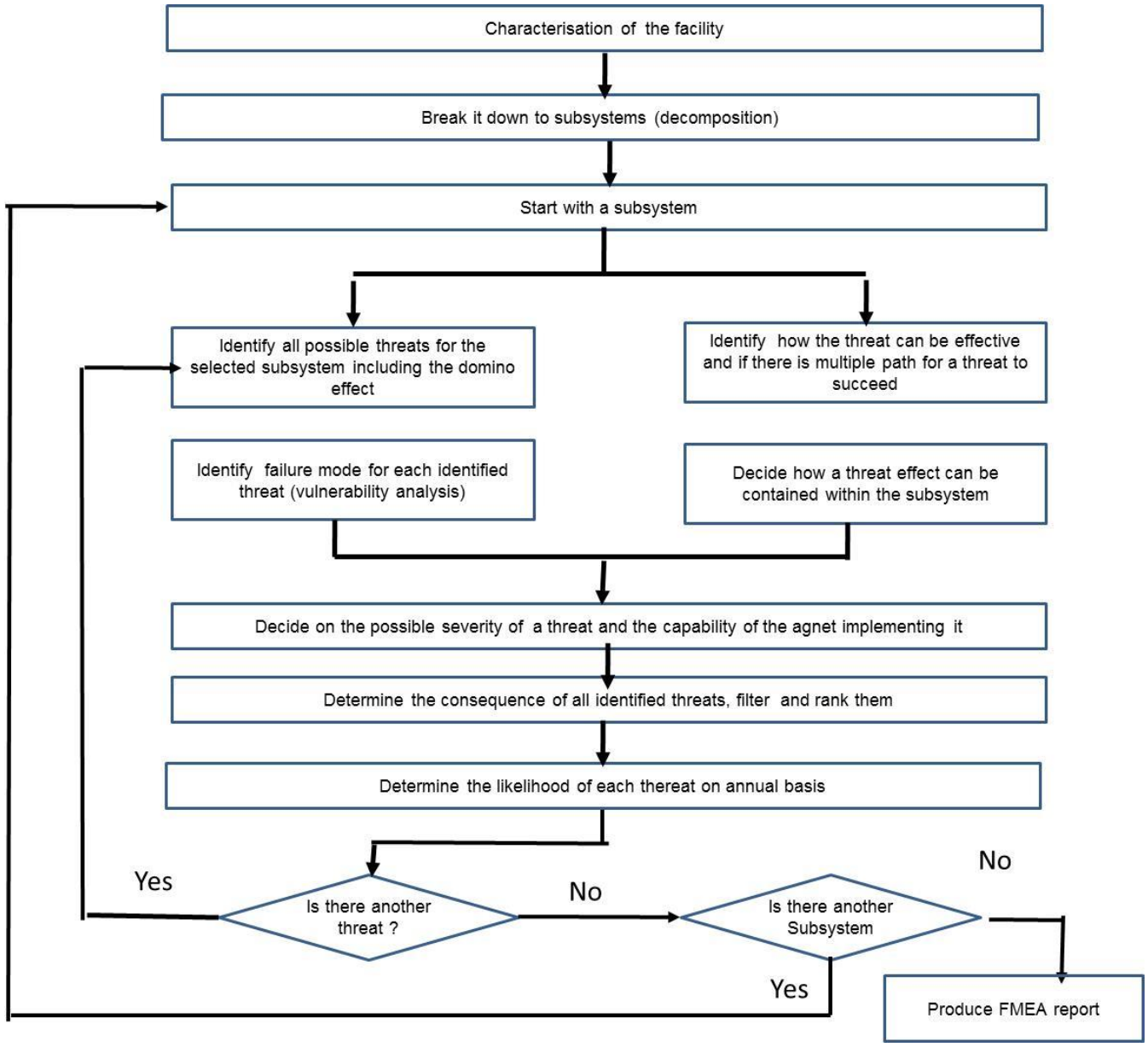

Figure 6. The basic approach to carry out an FMEA as described in IEC 60812 [19].

A similar cause-effect chain is necessary for the inclusion of security, using similar steps for security-critical events. The following elements for security cause-effect chain are a suitable starting point:

- Vulnerabilities
- Threat Agent
- Mode of threat
- Effect of threat
- Attack Probability

Vulnerabilities: The essential precondition for a security breach to succeed is a weak point or vulnerability in the system in which attackers can exploit without impediment. The vulnerability may be considered as a failure cause and should be the starting point of the security analysis. Thus, vulnerability is a weakness that can be exploited by an attacker.

If an attacker (i.e. threat agent) can exploit the vulnerability, then, the system's security is at risk. If there is no threat agent, vulnerabilities on their own do not lead to an effect. For a cause-effect chain, a threat agent is necessary.

While an FMECA usually is very effective when applied to a system, where system failures are most likely the result of single component failures, then Fault Tree Analysis may be a better alternative, especially for systems with a fair degree of redundancy. Qualification of a security system should follow the flowchart shown in Figure 7

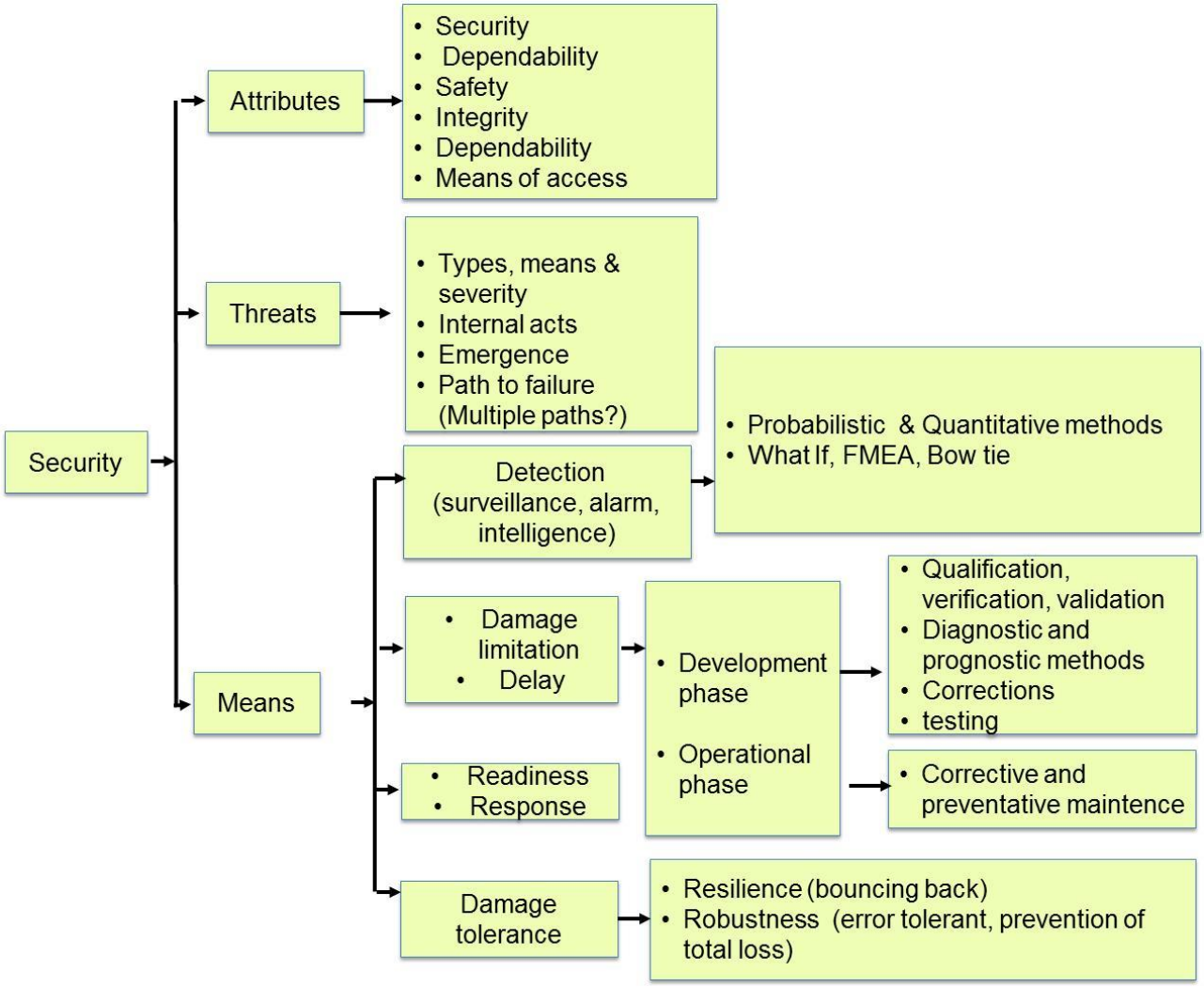

Figure 7. Components of security analysis

8. Barrier Analysis

There are several methods for describing how an incident evolves, and means of blocking (or stopping) its progress. The intention is that the threat should be prevented reaching its target by blocking its path using barriers (physical barrier or by instruments), namely controlling measures [4]

The barrier (which is a control measure in place), is an obstruction, or a hindrance that may either prevent an event from taking place or impede or lessen its consequences (protect the target). The attack succeeds either because the barriers did not serve their purposes or because they were missing. Different barriers will be needed at different stages in the escalation of a hazardous event or malicious act. In recent years, the concept of having several barriers in line has been institutionalised as defence-in-depth or layers of protection.

For the barrier analysis the following elements must be analysed:

Attacker: Attackers or threat agents are elements that are trying to exploit the system's vulnerabilities. For example hacker, terrorists, industrial espionage, or insiders may be such attackers [10].

Threat Mode: Threat mode classifies how vulnerabilities are exploited. There are many ways to exploit vulnerabilities, with different consequences. Potential types of threat (or modes of attack) will

depend on system weaknesses, as well as on the capabilities of the attackers.

Threat Effect: "The effect of a threat is described in terms of the consequence on the system's functionality or its operational condition. The threat mode describes the violated security attribute, but the threat effect characterises the violated system quality attribute" [13]. All dependability attributes may be affected by an attack. Which attribute is violated depends on the system, its environment, and the system's operational state.

Attack Probability: To assess the criticality of a security attack, the consequence and probability of the attack must be evaluated. The consequence can be assessed by analysis with assistance from experts. However, the probability of safety and security is determined differently.

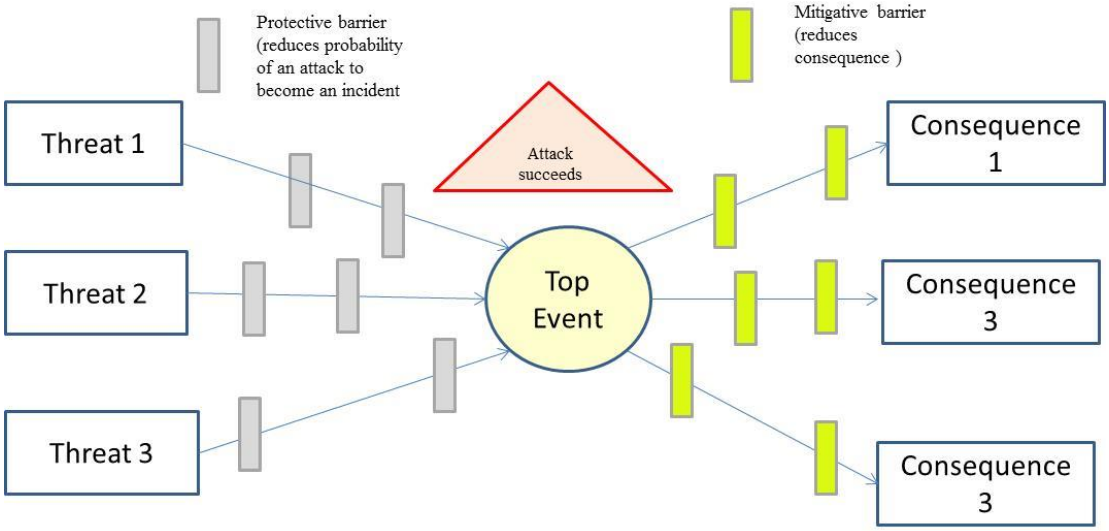

Figure 8. Bow-tie diagram

The concept of defence in depth can be explained with James Reason's "The Swiss Cheese Model", Figure 1 [17].

The holes can arise from active or latent failures. The active failures can be described as errors and violations that have an immediate adverse effect. The latent failures, on the other hand, are the decisions or actions that lie inactive but cause great damage and severe consequences when triggered. A bowtie diagram is a popular approach to describe and analyse the scenarios and to define the critical safety and security elements, Figure 8. A bowtie diagram visualises the barriers that are used to prevent an incident from happening, as well as the barriers that are used to protect vulnerable targets if the incident occurs.

Four types of barriers are defined [18], these are physical or material barriers, functional barriers, symbolic barriers, and incorporeal barriers. The physical or material barriers are barriers that physically prevent something from happening, or protect a target from an incident by blocking or mitigating the effects, e.g. a perimeter wall. Physical barriers are passive and do not need action from an agent. The functional barriers are instruments, e.g. an alarm system or a surveillance system, which have certain pre-conditions that need to be met before the barrier is activated. This activation can be done manually or automatically. The symbolic barrier, on the other hand, needs an intelligent agent who understands how the barrier works for it to achieve its purpose, e.g. a warning sign on the facility's control panel. Finally, the incorporeal barriers are barriers that do not have a material form or substance. Instead, it relies on knowledge by the user to be able to achieve [36 and 37].

9. Discussion

Physical security is defined as the ability of a system to operate in a damaged state, while working under constraints, to best achieve the system's mission. In an oil and gas [45] installations, the goal is to carry on with production while preventing harmful release to the environment, loss of life, and financial loss. The reason for not operating as desired, or for loss of property or life or releasing harmful material may be due to accidental or malicious causes, but the high-level goal of preventing these events is the same.

Applying systems engineering to security requires initially focusing on the security needs as a high-level policy i.e. as a strategy rather than a tactical problem. Certainly, malicious action is a critical consideration in addressing security, but, focusing only on adversaries,

diverts attention away from reducing system vulnerability by making it inherently secure and damage-proof. The security goal is not only to guard the physical asset and prevent intrusions, which is threat-focused but also to build a system that is tolerant of all sorts of disruption. The objective is to ensure that critical safety functions and services are maintained if disruptions do take place. Viewing the problem from a strategic vantage rather than tactics, security analysts and defenders can concentrate on the system's vulnerabilities, rather than just continually reacting to evolving disruptions [53].

Resilience must be built into a system to reduce its vulnerability. In a resilient system potential damage to one part of a system is less likely to spread far and wide. Resilience can also be the ability to bounce back from an adverse situation, which is a broad concept with many definitions, but most include the following elements:

- Withstand shock in a time of crisis.
- Quickly recover the functionality of the situation after a disaster or a sudden shock.
- The system should remain functional even if parts of the system have failed/damaged. The objective is to mitigate the severity and/or duration of disruptive events.

The resilience of a system is governed by five elements which are Robustness, Redundancy, Resourcefulness, Responsiveness, and Recovery. The first two are system based properties, and the last three are properties of the organisation running the facility. These elements should be designed into a system to provide inherent resilience capabilities [39].

1-Robustness: Robustness incorporates the concept of reliability and encompasses the ability to absorb and withstand disturbances and errors. That is:

1) If something in the system fails it moves to a safe state, and barriers are added to the system to contain damage escalation.
2) Decision-making chains of command must be responsive to changing circumstances and threats,
3) Designed to prevent unexpected shocks in one part of a system from spreading to other parts of a system, i.e. to localize and contain their impact, - no domino effect (the modular design is a good policy).
4) Damage tolerant.

2-Redundancy: Redundancy involves having excess capacity and back-up systems, which enables the repair of core functionality in the event of disturbances. This element assumes that a system will be less likely to experience a collapse in the wake of stresses or failures of some of its infrastructure if the design of that system incorporates diversity and overlapping alternatives.

3-Resourcefulness: Resourcefulness means the ability of the operators to adapt to crises, respond flexibly, and – when possible – contain the damage spread, protect people both inside and outside of the system boundaries.

4-Responsiveness: Responsiveness means the ability to mobilize quickly and act in the face of crises. This component of resilience assesses whether an organization has good methods for gathering relevant information and communicating the relevant data and information to others, as well as the ability for decision-makers to recognize and resolve emerging issues quickly and act fast.

5- Recovery: Recovery means the ability to regain a degree of normality after a crisis or event, including the ability of the operators to be flexible and adaptable in dealing with the new or changed circumstances after a threat is materialised. This component of resilience assesses the organization's capacities and strategies for feeding information throughout the organization, and the ability for decision-makers to take action to adapt to changing circumstances.

10. Conclusion

A systems engineering framework for the design and evaluation of effective physical security is outlined. This paper argues that in contrast to a bottom-up tactics-based approach, a top-down strategic approach is better. The top-down approach starts with identifying the system losses that are unacceptable, and against which the system must be protected. This will lead to a small and more manageable set of potential losses stated at a high-level of abstraction. A tactics approach starts with how best to protect a facility against disruption, in contrast, a strategic approach concentrates on essential services and functions which must be protected against disruptions and what is considered to be an unacceptable loss.

A chain of events may lead attackers successfully breaching several layers of protection, such as the perimeter walls and the surveillance systems, etc. In almost all such cases, security analysts will identify some barriers that should have served as the last layer of protection (or line of defence) and believe that if only that barrier would have been in the path of attackers, then the attack would have not succeeded. The author believes this is not a correct argument, since the vulnebale element is assumed to have passive role. A tactics-based approach, although necessary, is not sufficient.

A security analyst focussing on tactics would model the threat as the cause of the loss, but it is the vulnerability that leads to the loss event. Based on this concept, then preventing losses, is heavily dependent on the degree to which security analysts can correctly identify the

potential attacker and their motives, capabilities, and objectives. With this understanding, security professionals can determine the most likely route (or causal chain) attackers may take to achieve their goal. Then, loss prevention resources is directed to provide "defence-in-depth". However, threat prioritization is challenging given the sheer volume of threats and ever-increasing sophistication and complexity of attackers. If the focuses of the defenders are on the wrong threat, then probably the barriers are not effective. An unstated assumption is that if defence against the more severe and sophisticated threats is implemented, then less sophisticated cases would be covered, which is not necessarily true. Simple requirement errors or operational procedures may allow even unsophisticated attackers from previously ignored or less important adversaries to succeed.

The primar emphasis of this apper isto indetfiy the system's vulnerability first, and then look for the ways and means of protecting against malicious acts.

Acknowledgment

He author wishes to express his gratitude to Mr. Chris Millyard and Dr Jeff Banks for reviewing this paper.

11. REFERENCES

1. American Petroleum Institute, (2005). *Security Guidelines for the Petroleum Industry*, pp58.
2. American Petroleum Institute and National Petrochemical & Refiners Association, (2018), *Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries*, pp 168.
3. Idaho National Engineering and Environmental Laboratory, (2004), *A Comparison of Oil and Gas Segment Cyber Security Standards, Prepared for the U.S. Department of Homeland Security Under DOE Idaho Operations Office Contract DE-AC07-99ID13727*.
4. Anderson, R.J. (2008), *Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Ed*, New York, NY, USA: John Wiley & Sons.
5. Asllani, A., Lari, A. and Lari., N (2018), *Strengthening information technology security through the failure modes and effects analysis approach*, International Journal of Quality Innovation (2018) 4:5, pp 14.
6. Baldwin, D.A., 1997, *The concept of security*, Journal Review of International Studies, 23, 5-26, British International Studies Association
7. Baldwin, K., J. Miller, P. Popick, and J. Goodnight (2012). *The United States Department of Defence Revitalization of system security engineering through Program Protection*. Proceedings of the 2012 IEEE Systems Conference, pp19-22, Vancouver, BC, Canada.
8. Centre for chemical process safety, 2002, *Guidelines for Managing and Analysing the Security Vulnerabilities of Fixed Chemical Sites*, published by American Institute of Chemical Engineers (AIChE) Centre for Chemical Process Safety (CCPS)
9. Coole, M., Corkill, J. & Woodward, A. (2012). *Defence in depth, protection in depth and security in depth: a comparative analysis towards a common usage language*, The Proceedings of the 5th Australian Security and Intelligence Conference, 27-35, Perth, Western Australia.
10. Cordner, L., 2013 *Offshore Oil, and Gas Safety and Security in the Asia Pacific- The Need for Regional Approaches to Managing Risks RSIS Monograph*, No. 26, S. Rajaratnam School of International Studies, pp 104.
11. DAU. 2012. "*Defence Acquisition Guidebook (DAG): Chapter 13 -- Program Protection*" Ft. Belvoir, VA, USA: Defence Acquisition University (DAU)/U.S. Department of Defence (DoD). November 8, 2012.
12. DODI5200.44, *United States Department of Defence, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*, Department of Defence Instruction Number 5200.44, November 2012.
13. DHS. 2010. *Build Security In. Washington, DC, USA*: US Department of Homeland Security (DHS).
14. Dzida W, Freitag R (1998) *Making Use of Scenarios for Validating Analysis and Design*. IEEE Transactions on Software Engineering 24(12):1182–1196.
15. Garcia, M. L., 2008. *The Design and Evaluation of Physical Protection Systems*, Second Edition, Boston: Butterworth-Heinemann.
16. Federal Aviation Administration. *Requirements Engineering Management Handbook* DOT/FAA/AR-08/32, 2008, last accessed 23/12/2017.
17. Hauge, S. and Øien, K., 2016, *Guidance for barrier management in the petroleum industry*, SINTEF report A27623, SINTEF Technology and Society
18. Hollnagel, E., (2004), *Barriers and Accident Prevention*, Ashgate
19. International standard 2006, IEC 60812, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)* pp95
20. IAEA, 1999. "*The Physical Protection of Nuclear Materials and Nuclear Facilities*" IAEAINFCIRC/225/Rev. 4 (Corrected), International Atomic Energy Agency, Vienna.
21. IAEA, 2005, *Assessment of Defence in Depth for Nuclear Power Plants*, Safety report series N. 46. INTERNATIONAL ATOMIC ENERGY AGENCY VIENNA, pp 130.
22. INCOSE 2015. *Systems Engineering Handbook – A Guide for System Life Cycle Processes and Activities*, version 4.0. Hoboken, NJ, USA: John Wiley and Sons, Inc., ISBN: 978-1-118-99940-0.
23. ISO/IEC 21827, ISO and IEC (International Organisation for Standardisation and International

Electrotechnical Commission, (2008) *Information technology–systems security engineering–capability maturity model*.
24. ISO/IEC 15288: *Systems and software engineering – System life cycle processes*.
25. Königs, S.F., Beier, G., Figge, A., and Stark, R. (2012). "*Traceability in Systems Engineering – Review of industrial practices, state-of-the-art technologies and new research solutions*," Elsevier Advanced Engineering Informatics, 26(4), pp 924-94
26. ISO/IEC 27001, (2005). Information security management, BSI Group. Retrieved 02 March 2020.
27. Kissel, R., K. Stine, M. Scholl, H. Rossman, J. Fahlsing, J. Gulick. 2008. "*Security Considerations in the System Development Life Cycle*," Revision 2. Gaithersburg, MD. National Institute of Standard and Technology (NIST), NIST 800-64 Revision 2:2008.
28. Kiszelewska, A., and Coole, M, (2013), *Physical Security Barrier Selection: A Decision Support Analysis*, Proceedings of the 6th Australian Security and Intelligence Conference, Edith Cowan University, Perth, Western Australia, 2nd-4th December 2013, pp 13.
29. Merge-Safety & Security 2016, *Project no.10011, Recommendations for security and safety co-engineerin*g, release No. 3, pp 166
30. MITRE. 2012. "*Systems Engineering for Mission Assurance*." In Systems Engineering Guide.
31. NASA, (2007). *Systems Engineering Handbook. NASA Technical Report NASA/SP-2007-6105 Rev1*, ISBN 978-0-16-079747-7, Washington, DC, USA.
32. National Defence Industrial Association (NDIA) System Assurance Committee. 2008. *Engineering for system assurance*. Arlington, VA: NDIA.
33. NATO. 2010. *Engineering for System Assurance in NATO programs*. Washington, DC, USA: NATO Standardization Agency. DoD 5220.22M-NISPOM-NATO-AEP-67.
34. NIST SP 800-160. *Systems Security Engineering - An Integrated Approach to Building Trustworthy Resilient Systems*. National Institute of Standards and Technology, U.S. Department of Commerce, Special Publication 800-160.
35. Nityanand, K., 2015, *Standards for physical security management in industry: A research paper on behalf of National police academy*, Hyderabad pp240.
36. Norwegian Petroleum Safety Authority-PSA, (2013), *Principles for barrier management in the petroleum industry*, pp 34
37. OGP 2016, report 544 *Standardization of barrier definitions*, Supplement to Report 415, International Association of Oil &gas Producer
38. Plant R, Gamble R (2003) *Methodologies for the Development of Knowledge-based Systems*.
39. Ross, R., J.C. Oren, M. McEvilley. 2014. "*Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*." Gaithersburg, MD.
40. RON Ross, R., McEvilley, M., Carrier, J., (2014), *Systems Security Engineering Considerations for Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, NIST Special Publication 800-160, Vol. 1
41. Royal Canadian Mounted Police (2004) *Protection, detection and response, Physical security guide*, Technical Security Branch, 1-20
42. Schmittner C., Gruber T., Puschner P., Schoitsch E. (2014) *Security Application of Failure Mode and Effect Analysis (FMEA)*. In: Bondavalli Snell, M.K., Jaeger, C.D., Jordan, S. E., Scharmer, C., Tanuma, K., Ochiai, K., and Iida, T. 2013.
43. SANDIA Security-by-Design Handbook, *REPORT SAND2013-0038*, Prepared by Sandia National lab Laboratories, Albuquerque, New Mexico, USA, pp 141.
44. Sklet, S., (2006)Safety barriers: *Definition, classification, and performance*. Journal of Loss Prevention in the Process Industries, 2006. 19(5): p. 494-506. The
45. US Department of energy, 1996 *hazard and barrier analysis guidance* EH-33 office of operating
46. Transportation Security Administration of the united states, 2018, *Pipeline Security Guidelines*, March, pp 30.
47. The US homeland security, 2003, *The national strategy for The Physical Protection of Critical Infrastructures and Key Assets*, pp 96.
48. Unites Nations' office of counter-terrorism and united nation security council, 2008, *the protection of critical infrastructures against terrorist attacks: a compendium of good practices*, pp 170.
49. Vanderhaegen, F. (2018) *Human-error-based design of barriers and analysis of their uses*. Cogn Tech Work 12, 133–142 (2010).
50. Yasseri S., (2014). "*Physical Security for Petroleum Facilities*," Journal of petroleum safety, PP 4.
51. Yasseri S. Bahai, H. and Yasseri, R., (2018). "*A Systems Engineering Framework for Delivering Reliable Subsea Equipment*, 2018-TPC-.
52. Yasseri, S. Bahai, H, Yasseri, R, 2018, *Reliability Assurance of Subsea Production Systems: A Systems Engineering Framework*, International Journal of Coastal & Offshore Engineering, Vol.2, No. 1, pp 1-19.
53. Young, W. and Leveson, N., (2013) *Systems thinking for safety and security*, In Proceeding ACSAC '13 Proceedings of the 29th Annual Computer Security Applications Conference Pages 1-8 New Orleans, Louisiana, USA — December 09 - 13, 2013 ACM New York, NY, USA .