2010

Theory of entropic security decay: The gradual degradation in effectiveness of commissioned security systems

Michael P. Coole
Edith Cowan University

2010

Theory of entropic security decay: The gradual degradation in effectiveness of commissioned security systems

Michael P. Coole
Edith Cowan University

Edith Cowan University

Copyright Warning

The Theory of Entropic Security Decay: the gradual degradation in effectiveness of commissioned security systems.

By

Michael P. Coole

A Thesis

Submitted to the Faculty of Computing, Health and Science

Edith Cowan University

Principle Supervisor: Dr David Brooks

Submission Date: 29th November 2010

In Partial Fulfilment of the Requirements for the Degree of

Master of Science (Security Science)

DECLARATION

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university. To the best of my knowledge and belief, this thesis contains no material previously published by any other person except where due acknowledgement has been made.

Date: 29th November 2010

ABSTRACT

As a quantitative auditing tool for Physical Protection Systems (PPS) the Estimated Adversary Sequence Interruption (EASI) model has been available for many years. Nevertheless, once a systems macro-state measure has been commissioned (Pi) against its defined threat using EASI, there must be a means of articulating its continued efficacy (steady state) or its degradation over time. The purpose of this multi-phase study was to develop the concept and define the term entropic security decay. Phase one presented documentary benchmarks for security decay. This phase was broken into three stages; stage one presented General Systems Theory (GST) as a systems benchmark for the study. Stage two applied the writings from stage one to physical security, and stage three presented a benchmark for considering physical system decay. Phase two incorporated the pilot study towards validating the feasibility of undertaking the main study and refining interview instrumentation. Phase three executed the main study, extracting and presenting security experts (N=6) thoughts, feelings and experiences with the phenomenon of security decay. Phase four provided the interpretative analysis, responding to the study's research question.

The study found that within a systems approach to physical security there is a complex interrelationship between the built environment, physical controls, technology, people and management processes as they achieve the elements of Defence in Depth. Within this complex interrelationship the study indicated that decay occurs at the constituent level, and if left undetected expands to affect the sub-system in which it is located. Furthermore, based on the interrelationary aspects of Physical Protection Systems (PPS) the decay expands from its point of entry into the remainder of the system, propagating throughout the Defence in Depth system. The study suggested that security decay theory is primarily concerned with managing the natural entropic processes/pressures occurring against commissioned levels of effectiveness within PPS. In addition, the study indicated that in order to maintain PPS at their commissioned levels of effectiveness during their life cycle, they need to be managed in accordance with their commissioned designed specifications. The most effective method to manage decay in order to maintain the designed specifications within PPS is through the utilization of a performance indicator frame work, which facilitates full management of the system.

ACKNOWLEDGEMENTS

The first acknowledgement goes to Dr Dave Brooks, my principle research supervisor from Edith Cowan University. Dave provided me with this area of focus as it has been an area in which he has a strong interest. I don't believe this thesis would have been possible without Dave's direction and support provided the necessary academic advice and development, which enabled me to explore the concept of security decay outside of what had previously been considered. Thanks for your help Dave.

The second acknowledgement goes to Mr Jeff Corkill, also from Edith Cowan University. Jeff provided academic guidance, developing my critical analysis and academic writing skills both in my undergraduate degree and during my Masters of Science course work.

I would also like to acknowledge the very busy security industry practitioners who supported me in achieving this study, especially Mr Peter Zappelli. These practitioners took time out from their extremely busy schedules to participate in my research panels, providing their depth of experience from solving real world security problems to address my research enquiry.

I would like to especially thank my wife Shiarne, and children Bailey and Rachel who have endured the many hours of lost time together while I engaged in this research enquiry. Thanks, you guys are awesome.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS AND FORMULAS

PUBLICATIONS AND CONFERENCE PRESENTATIONS

There was one conference presentation that resulted from this thesis. The conference proceeding is presented, including the publication's abstract.

Publication: Coole, M., & Brooks, D. (2009). The theory of entropic security decay. Proceedings from the second Australian Security and Intelligence Conference. Perth, Western Australia. Retrieved from: http://igneous.scis.ecu.edu.au/proceedings/2009/secintel/ASICProceedings.pdf

ABSTRACT

This paper discusses the effects decay has within the systems approach utilised when implementing security strategies, specifically the theory of defence in depth. Defence in depth is implemented within a risk management framework to reduce an organisation's identified risks which could lead to undesirable and unacceptable consequences. This theory aims to link layered security elements into a system to ensure a holistic and functional security system, underpinned by the functions of: deter, detect, delay and response. For such a system to be commissioned, and maintain its commissioning effectiveness these functions must be performed in their sequential order and within a period of time, which is less than an adversary's task time. This paper argues that such a relationship between the defence in depth elements, and each elements constituents requires an orderly relationship, and that factors which impede this orderliness directly affects the security system as a whole. This paper applies the concept of entropy, referred to as the steady degradation of a system, underpinned by the characteristics of disorganisation and decay to argue that a security system can become degraded through the reduction in effectiveness of its individual components. Such degradation decays the effectiveness of the whole system. Within the risk management frame work this paper argues that as decay increases, risk reduction decreases, therefore risk exposure increases.

Key words: security, decay, entropic, defence-in-depth, risk management.

CHAPTER 1

INTRODUCTION

1.1 Introduction

The concept of risk management is well established in academic and organisational literature and to some degree, so is security risk management; however, the effectiveness of security risk management has been questioned (Brooks, 2009, p. 1). Therefore, this study discusses how security risk management may be implemented in a systems approach, using the theory of Defence in Depth whilst being cognizant of the concept of entropy. It has been proposed that defence in depth strategies can be impeded by the characteristics of disorganization and decay underpinning entropy. For an organisation to maintain a sound security profile, all Defence in Depth elements and their constituents must be maintained at their optimum level of performance. It is argued that organisational security should draw on the concept of entropy to establish the concept of security decay, which results in a reduction in overall system performance and avoidance through the active monitoring and reviewing of treatment strategies.

1.2 Background of the Study

In contemporary business, risk management is considered a significant management activity. Borgsdorf and Pliszka (1999, p. 6) define risk management as "the planning, organising, leading and controlling of an organisation's resources" to minimise the potential of negative effects on the business activity. This approach is a formal systematic process that includes identifying exposure to risk, evaluating methods to manage risk, implementing treatment strategies, ongoing performance monitoring of implemented strategies and implementing necessary adjustments to such strategies, referred to as a systems approach (Hatfield & Hipel, 2002, p. 1054). Such an approach is supported through Australian Standards in risk management (AS/NZS ISO 31000: 2009) and security risk management (Standards Australia, 2006). Security management has embraced the risk management concept for planning how organisational resources can be efficiently and effectively managed to reduce the chances of negative outcomes from breaches of security programs.

1.2.1 Physical security

For contemporary security professionals, risk arises from a combination of a threat exploiting some vulnerability such that it could cause some harm to an asset, where an asset is considered anything with value and need in protection, normally including people, information, property and reputation (Burns-Howell, Cordier & Erikson, 2003, p. 11). The risk management process includes the implementation of acceptable practices; procedures and principles which when organised into a cohesive whole have the desired effect of significantly reducing the statistical chances of undesirable events against such assets from occurring. Therefore the aim of security controls (design) is to decrease the ratio of unfavourable events to total events (Broder, 2006, p. 25). Such a planning process in security management is in general referred to as *security risk management*.

In addressing security risk concerns, Standards Australia HB167 security risk management (2006, p. 63) states "the key elements of organisational, community or individual security controls are those components which contribute to the management of risks through their ability to deter, detect, delay, respond and recover from adversary attacks", such a view is supported by Somerson (2009, p. 13) who states, "a security programs objectives in controlling for security related risks are to deter, detect, delay/deny, respond and where necessary recover from reasonably foreseeable attacks". According to Burns-Howell, Cordier and Erikson (2003, p. 11) acceptable risks can be defined as "a judgement on the unique elements of each risk, with the decision based either on the costs of protecting an asset, balanced with the costs if it is damaged or lost, or on the organisation's appetite for accepting risks. Therefore, a security risk management plan determines the level of treatment controls required based on a facility's risk rating and are implemented in accordance with the theory of defence in depth (Garcia, 2001).

The theory of defence in depth aims to link layered security elements into a system incorporating people, technology, barriers and procedures to ensure a holistic and functional security system (Smith, 2003, p. 8). This system delivers effective risk based decisions, enhanced operational effectiveness, and a reduction in overall risks and costs (Trusted Information Sharing Network, 2008, p. 2). However, it has been argued that security controls can degrade over time reducing the level of risk treatment. This argument was first considered by Underwood (1984) who referred to decaying security,

stating, “security decay is the most serious threat to a security system” and that “security decay must be expected”, “avoided”, and “countered” (Underwood, 1984, p. xi). Underwood (1984, pp. 249-250) postulated that:

> “the provision of effective security is paradoxically the first step towards decay, as an effective system will not only repel successful attacks, but also prevent the attacks being made: arguing an illusion is then created that the established security is unnecessary suggesting decay will follow until the degree of security falls to the point where an attack will succeed”.

Underwood’s (1984) writings were reviewed by McClure’s (1997) thesis “Security Decay: the erosion of effective security”, where he viewed the theory of security decay as being primarily concerned with the influence apathy has on security. McClure (1997, p. 4) defined security decay as “a concept and phenomenon when effective security indirectly causes an attitude of apathy towards the provision of security, resulting in ineffectiveness’. McClure (1997, p. 4) states:

> “apathy leads to poor compliance with security policy and procedures causing a decay of security effectiveness”.

However, it could be argued that a lack of education and awareness leads to security decay or that the two arguments are interlinked. Nevertheless, such arguments only consider minimal causal factors and do not consider holistic factors, nor describe where security decay lies within the Defence in Depth system.

Consistent with the writings of Underwood (1984) and McClure (1997) it can reasonably be argued that the concept of security decay is a significant risk to any security program. However, to date very little dedicated research has been conducted into the area. Furthermore, what has been discussed provides very limited insight. For example, according to Garcia (2001, p. 6) the theory of Defence in Depth should be implemented in security management using a systems approach. Garcia’s (2001) views are supported by many published security authors (Underwood, 1984; Fennelly, 1997; Fisher & Green, 2003). In addition, Underwood (1984, p. xi) states “It is important that security is seen as a whole, and both designed and operated as a system”. Such views indicate that security should be designed, implemented and managed as a system. In considering Underwood’s (1984, p. xi) writings, Bittel (1978, p. 652) explains that the practice of management also requires a system approach. Underwood (1984, p. xi) points out that the normal processes of management by objectives should be applied to

the establishment of the security system. In considering the systems approach to both security and management, it can be argued that nobody would deny the importance of applying systems thinking and analysis to security management.

The systems approach to both security and management is a well supported theme. As such, it is reasonable to argue that any discussion in relation to a holistic approach to security decay must consider a systems approach. This approach must include designing, implementing, and managing the security system. That is, a holistic approach to security decay must encompass both the processes in establishing the system and the ongoing management processes which aim to ensure the system reliably delivers, over time, the output for which it was commissioned. In light of such literature, the study supports the concept of security decay; however, argues that the concept of security decay must be considered, defined and applied congruous with the systems approach utilized to employ the theory of Defence in Depth.

However, to date there is a dearth of dedicated published research pertaining to security decay. This study argues previous approaches by both Underwood (1984) and McClure (1997) were viewed through a narrowly focused lens and are therefore limited in that they did not consider the systems approach to security. The systems approach to Defence in Depth interrelates the functions of detect, delay and response into an effective security system, referred to as a Physical Protection System (PPS) (Garcia, 2001, p. 5). As such, this research argues that any theory of security decay must be considered within this approach. The study postulates that decay within a security system lies within both the elements and their constituents of detect, delay and response and in their interrelationships towards achieving the desired protection goal. Whereby factors such as apathy are only contributors towards decay and do not represent the salient contributor or actual decay within the system.

In considering the concept of security decay from a systems approach, according to Hamlyn (1969, p. 16) explanations in science may be divided into two kinds. First, explanations made by reference to laws; second, explanations made by reference to theories. According to Hamlyn (1969, pp. 16-17) in making reference to laws we seek to account for deviations from expectations by reference to the law. In contrast, theories are invoked to account for laws and in doing so, seek to provide a model of some sort into which the laws may be incorporated. It is therefore argued that any consideration of

security decay within a systems approach must be discussed by either drawing on those scientific laws and/or theories which apply to systems in general.

1.3 Significance of the Study

The security industry, both government and commercial, rely on the application of security risk management. Risk management is becoming a well established discipline, with its own body of knowledge and domain practitioners. States worldwide have their own risk management standards and in many of these states, it is the company director's responsibility to ensure that appropriate risk management meets internal and external compliance requirements. Nevertheless, many of these standards and compliance requirements only consider risk management, not security risk management. However, security risk management is unique from other forms of risk management and many of the more generic risk models lack key concepts necessary for effective design, application and risk mitigation (Brooks, 2009, p. 1).

It is expected that characteristics that may make an organisation prone to entropic decay can be identified and measured. Once these characteristics are understood, this will allow the use of considered funding to stimulate and maintain the effectiveness of various security risk mitigation strategies. Therefore, this research aims to expand Underwood's (1984) and McClure's (1997) theory of security decay towards establishing the theory of entropic security decay. This theory is based on the argument that security is achieved through a systems approach and that all systems if left will degrade due to the effects of natural entropy.

1.4 Purpose of the study

The concept of entropy inevitably leads to security systems decaying over time, reducing their commissioning levels of efficiency and effectiveness. To purpose of this study is to articulate the concept and define the term entropic security decay.

1.4.1 Objectives

1. To determine if the theory of entropic security decay is supported by security experts.
2. To identify a framework for evaluating entropic security decay.
3. To formulate a definition for security decay.
4. To stimulate academic discourse into the concept of security decay.

1.4.2 Research Question

Do security experts support the theoretical validity of entropic decay theory, which argues that security decay is represented by "the gradual degradation of the microscopic quantities (constituents), and, or, the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system"?

This research question was considered by responding to the following sub-questions:

1. Do security experts support the systems approach to implementing effective security controls?

2. Do security experts support the argument that security systems can and do suffer from decay?

3. Do security experts support that security decay lies within the systems elements, constituents and their interrelationship?

1.5 Study Overview

According to Lin (1976, p. 5) "social research follows a sequence of phases", as such, the study adopted a multiple phase approach incorporating a number of sequential phases to achieve the research outcomes. Figure 1.1 presents the phased sequencing, designed to facilitate a logical step by step approach towards responding to the study's research question.

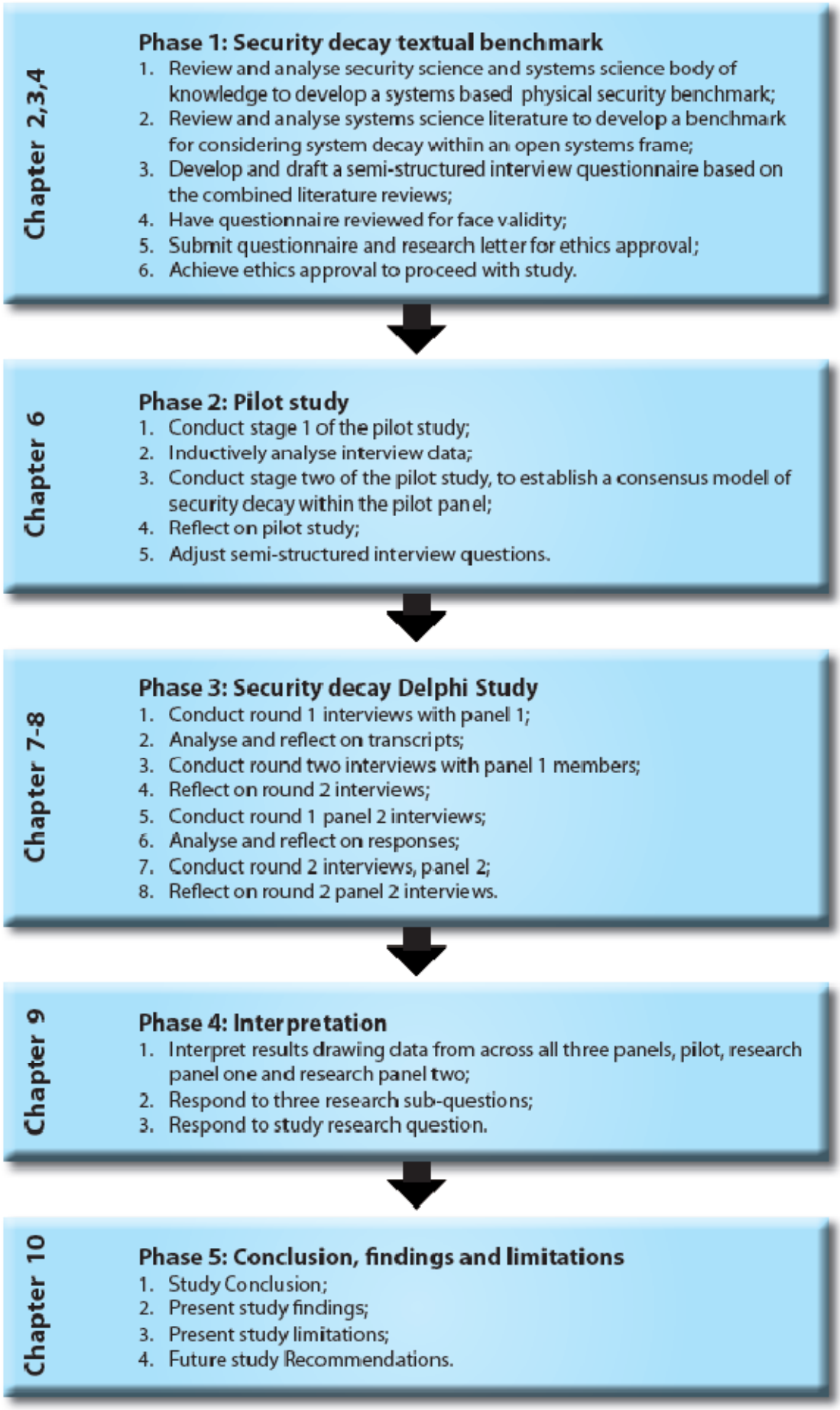


Figure 1.1 Study Phases (Adjusted from Lin, 1976, p. 6).

The study was designed to explore, define and develop deeper understandings towards the concept of security decay. Hamlyn (1969, p. 16) stated "explanations in science are/can be divided into two kinds, those which make reference to laws, and those which make reference to theories". In exploring the phenomenon of security decay from a systems approach, consistent with Hamlyn's (1969, p. 16) writings stage one of phase one of the study made reference to theories, developing a literature based benchmark for considering measured security by drawing on the theory of Defence in Depth and General Systems Theory (GST) (Chapters 2 and 3). At the completion of a security system benchmark; the study then made reference of laws towards developing a literature based benchmark for considering degradation or decay within an open systems approach to physical security (Chapter 4).

Phase two of the study aimed to consider security experts thoughts, feelings and understanding of security decay within a systems approach to implementing effective physical security through the use of a semi-structured interview questionnaire, starting with a pilot study (Chapter 6). At the completion of the pilot study, the semi-structured interview questionnaire was adjusted to increase its usability and draw out deeper data. Phase three incorporated the main study interviews using the Delphi methodology (Chapters 7-8). Phase four (Chapter 9) of the study sought to interpret the interview data in relation to the three research sub-questions and the study's research question. This phase aimed to validate the theoretical assumptions underpinning the theory of entropic security decay. The final phase, phase five (Chapter 10) presented the study's findings, limitations, its recommendations and conclusion.

1.6 Conclusion

This chapter presented the study's background and the current limitations within the area of security decay. The study was designed to reduce the current knowledge gaps through developing deeper understanding of security decay from a systems approach. In developing a deeper understanding the study sought to define the term entropic security decay. The study produced a number of beneficial outcomes. (1), a system based understanding of security decay. (2), expert validation of the theoretical underpinnings of entropic decay theory. (3), a systems framework for managing Physical Protection Systems (PPS) in a manner to maintain their commissioned effectiveness over their life cycle and (4) initial deductive definition of Security Decay.

CHAPTER 2

A SYSTEMS APPROACH TO SECURITY

2.0 Introduction

Phase one of the study requires the establishment of a systems framed security decay benchmark. This benchmark was established through a conceptual review of literature. The choice of such a literature review stems the writings of Stake (2010, pp. 109-111) who explains that some literature reviews aspire to maximise the broad and complex conceptual standing of the research question/s, encompassing a vast number of citations working across multiple disciplines, extending the understanding of a specific phenomenon related to different fields. Such literature reviews bring together writings on diverse matters towards providing an existing framework for deductively exploring phenomenon (Patton, 2002, p. 453). The conceptual review was achieved via a documentary analysis of published materials including books, journal papers, conference materials and internet web sites. Stake (2010, pp. 109-111) advocates the benefits of such a conceptual review, stating "it significantly contributes to highlighting the complexity of a professional problem".

This chapter presents the first stage of phase one of the study; establishing a systems approach to security benchmark. The chapter presents the common thread within published security literature leading to the study's theoretical foundation (underlying theory); being General Systems Theory (GST). This chapter is broken into a number of sequential sections. Section 2.1 discusses the difficulties associated with academic security research and provides an operational definition of security for the study. Section 2.2 presents the systems literature towards providing an open systems frame for considering physical security within a systems approach. Section 2.3 concludes the chapter.

2.1 Security

Security management in contemporary times concerns a wide spectrum of activities and skills. According to McCrie (2004, p. 11) conceptually, and in actuality, no contemporary organisation can survive or thrive without adequate security. However, security is a multi-disciplinary profession (Brooks, 2007, p. 1), where the concept of security can have different meanings depending on context. As a result of its diversity,

security as a profession lacks consensus in definition (Borodzicz & Gibson, 2006, p.182; Manunta, 1999, p. 58). Such definitional diversity has implications for security research. For example, in establishing an academic security frame for considering security decay, Lorenz (1963; 1968) stated "once the initial state of a system is known, then any changes in this state can be considered as its measure of error". Such a view was also presented by Pitzer (1995, p. 26) who considered that when measuring a quantity, a standard must be chosen, then find a means of comparing the measurement of an object of interest with this standard". McClure (1997, p. 59) referred to this as "benchmarking", drawing on the works of O'Leary (1995 cited in McClure 1997, p. 59) who defined benchmarking as "the process of constantly measuring and assessing products, services and practices against recognised standards". However, as McClure (1997, p. 59) wrote "the problem faced in benchmarking a security function, is recognising a standard on which to compare".

2.1.1 Security as a construct

Security as a construct, is one of ancient need (Underwood, 1984, p. x), which according to Maslow (1970, p. 39) for humans has its basis in psychological necessity. In discussing the concept of security Maslow (1970, pp. 35-46) states "the concept of security relates to humans having a hierarchy of five universal needs". These needs include:

1. Survival needs- food and shelter;
2. Safety needs- protection and security;
3. Love, affection, and a sense of belonging-the need for humans to feel part of social groups, such as families, religious groups, fraternal societies;
4. Esteem needs- the need for self satisfaction with work and group activities and social recognition from others;
5. Self-actualization-which Maslow defined as the simultaneous fulfilling of the first four (4) needs.

Within Maslow's (1970) hierarchy of needs the concept of security is one of the more basic needs and encompasses; stability, dependency, protection, freedom from fear, from anxiety and chaos, need for structure, order, law, limits and strength in the protector, which collectively are defined as "security". Based on the hierarchy of needs Maslow (1970, p. 39) considers that if security needs are not fulfilled an individuals' ability to achieve those higher order needs are impeded. In considering security within the context of social organisation, security has been connected with the notion of law and order (Manunta, 1999, p. 60), where according to Maslow (1970, p. 43) whenever a

threat to law, order, or to the authority of society occurs a regression from those other lower level needs rapidly occurs towards the safety/protection/security needs.

In discussing the diversity within the contemporary security profession Somerson (2009, p. 51) considers that the connection between safety, protection and security is drawn from humans early functional pursuit of self protection against the felonious acts of others. However, in considering the notion of safety within the concept of security Somerson (2009, p. 51) suggests this originated from mans commissioning of barriers to guard himself from "the duncery of his own negligence", where the sum of these guards provides the function of safety.

In contemporary times this diversity has lead to the concept of security being defined in many ways, for example, Craighead (2003, p. 21) defines security as "free from danger" or "safe". However, Fisher and Green (2004, p. 21) defines security as "a stable relatively predictable environment in which an individual or group may pursue its ends without disruption or harm and without fear or disturbance or injury". Such a definition is supported by O'Block, Donnermeyer and Doeren (1991, p. 7) who define security as "freedom from fear of crime and the actual danger of being the victim of crime".

In considering the various definitions of security put forward by Fisher and Green (2004) and others (O'Block, Donnermeyer and Doeren, 1991; Craighead, 2003, p. 21) it is argued that whilst they share common themes they are descriptive in nature, therefore more representative of dictionary definitions, which Runyon, Coleman and Pittenger (2000, p. 11) suggest lack observable and measurable variables. In the context of operational security such criticisms and viewpoint are supported by Manunta (1999, p. 58) who argues all encompassing descriptive definitions are inadequate, purporting security must be considered by a more functional, clearer definition. It is argued that Manunta's (1999) approach would be more congruous with Maslow's (1970) discourse on security.

In considering Manunta's (1999) standpoint, the Concise Dictionary (p. 497) defines functional as (1) involving, or containing a function or functions, regarded as the "intended purpose" (2) "practical" rather than decorative (3) capable of "working", meaning Manunta (1999) takes on a purposeful "functionalism" approach to security. For example, Manunta (1999, p. 58) defines security as "a function of the presence and

interaction of Asset (A) requiring protection from either a person, organisation or community referred to as Protector (P), a Threat (T) to the asset requiring protection in a given Situation (Si)" defining security by the formula S= f(A, P, T) Si. Manunta (1999, p. 58) argues the absence of one of the core elements (A, P, or T) voids the concept of security of its significance, as without an Asset there is nothing to protect, without a Threat there is no reason to protect, and without a Protector there is no striving for or pursuit of security.

Manunta's (1999, p. 58) functional approach towards security is supported by Cohen and Felson's (1979) Routine Activity Theory. This theory, within the context of law and order, postulates that for a crime to occur there must come together a likely offender, a suitable target and the absence of capable guardians. Such an approach towards definition is congruous with Underwood's (1984, p. x) definition of security, defining security as "confidence in the retention of belongings", "confidence in personal safety". In considering various sentiments towards defining security Manunta (1999, p. 58) argues that functional definitions have advantages over descriptive views. According to Manunta (1999, p. 58) they separate beliefs and chance approaches from managed security, distinguishing security from other attached concepts such as safety, yet being general enough to embrace all types and levels of Assets, Protectors and Threats in all possible Situations.

The separation of security from safety at the functional level is supported by Somerson (2009, p. 51) and Garcia (2001, p. 2). Somerson (2009, p. 51) highlights the sentiment that, whilst both domains address themselves directly towards augmenting overall organisational objectives, their emphasised functions remain separate. For example, security as a function has received its greatest emphasis in economic loss prevention and defence industries. A focus supported by Garcia (2001, p. 2) who refers to security as systems used to prevent or detect an attack by a malevolent human adversary. Whilst Garcia (2001) accepts there are some overlaps with safety, as a function security's salient focus is on preventing attacks by malevolent human adversaries. In contrast, according to Somerson (2009, p. 51) safety's emphasis is based in losses arising from workers compensation claims.

Such a functional approach towards security is considered both a process of activity and a condition resulting from that activity (O'Block, et al, 1991, p. 15). For example, as a

process, it can be considered that security can be regarded as the utilization of people, equipment, and procedures to reduce or eliminate risk of loss of assets, tangible and intangible, from causes and events not considered to be within the boundaries of conventional speculative or profit/loss activities. As a function, security can be considered the use of "measures designed to safeguard people, to prevent unauthorised access to equipment, facilities, materials and documents (information) (O'Block, et al, 1991, p. 7).

It is argued by Post, Kingsbury and Schachtsiek, (1991, pp. 97-99) that to achieve a holistic security program for any organisation it is a requirement that physical, personnel and information security components be interrelated into a comprehensive barrier system. Whilst the level of focus each organisation places on these components will vary depending on business environment and risk exposures, from a functional approach, all three systems (Figure 2.1) must be present within every organisation to provide a comprehensive security function.

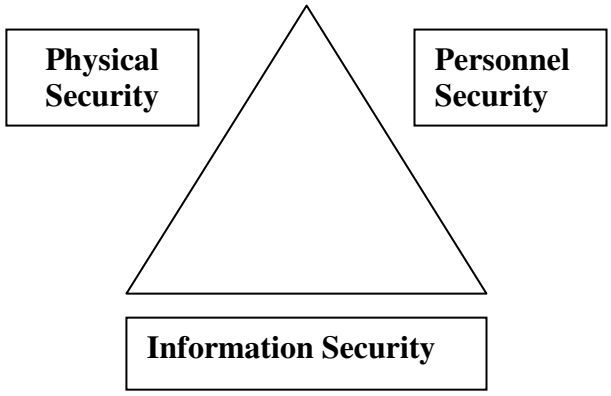


Figure 2.1 Holistic organisational security program (Adjusted from Post, Kingsbury & Schachtsiek, 1991, pp. 97-99).

2.1.2 Defence in Depth

From a functional perspective, security as a domain discipline, collectively embraces a historically consistent strategy towards preventing theft, destruction of facilities, the protection of personnel and information, referred to as *Defence in Depth* (Smith, 2003, p. 8). The theory of Defence in Depth is underpinned by the functions of deter, detect, delay, response and recovery (Standards Australia HB 167:2006, p. 3). According to Smith (2003, p. 8) this strategy (Defence in Depth) has been applied to the protection of

assets for centuries, based on the argument that a protected asset should be enclosed by a succession of barriers, to restrict penetration of unauthorised access, towards proving time for an appropriate response and recovery (Standards Australia HB 167:2006, p. 3).

In applying the theory of Defence in Depth Francis (1992, p. 2) explains that this strategy (Figure 2.2) results in further layers of protection being encountered as deeper progression occurs into a facility. Whenever a breakdown in one barrier occurs, whether by accident or deliberate breach, one or more barriers remain to maintain reliable and effective access control. The functions of Defence in Depth elements are:

- Deterrence - psychological measures or cues implemented to deter opportunistic offenders from perpetrating deviant acts;
- Detection - means to alert organisations that an attack or breach is underway;
- Delay - physical means for retarding the progress of anyone who has gained an un-authorized level of access;
- Response - an organisations' means of interrupting persons who have breached the security perimeter of a facility;
- Recovery – is a planned and prepared approach to reactivating to a realised event.

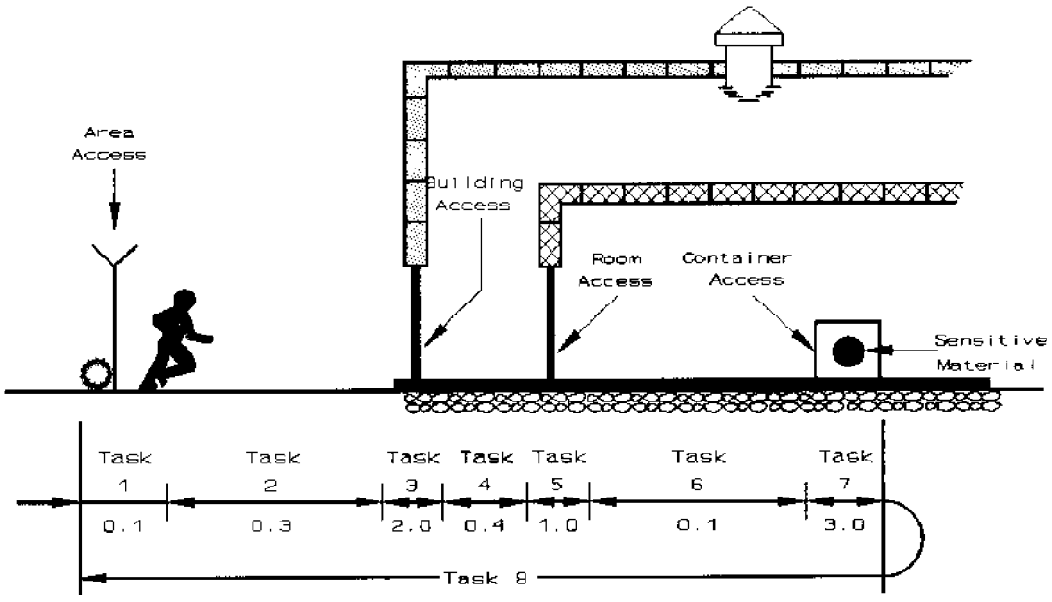


Figure 2.2 Theory of Defence in Depth (MIL-HDBK-1013/1, 1993, p. 28).

In discussing the theory of Defence in Depth further, Smith (2003, p. 8) highlights that this strategy aims to link layered security elements into a "system" incorporating;

people, technology, barriers and procedures to ensure a holistic and functional security system. For example, Figure 2.2 shows how defence in depth layers are linked into a barrier "system" incorporating discrete sequential tasks which must be successfully overcome by an adversary, before they are interrupted by a response force, to achieve their objective.

2.1.3 Security defined

In their discussion of the security industry Borodzicz and Gibson (2006, pp. 181-182) highlight that in contemporary times' security is a key aspect in organisational management, yet a universal definition remains problematic. Brooks (2008, p. 5) argued that security can only achieve definition through applied context and concept definition, where according to Brooks (2008, p. 5) concept definition may be achievable through a consensual body of knowledge. In considering such definitional barriers Borodzicz and Gibson (2006, pp. 181-182) explain that the common thread is a desire on the part of all practitioners to protect those assets, which they hold to be valuable, from deliberate malicious human intervention in the form of perceived risks and perpetrated consequences using a variety of countermeasures.

Despite a common cause within the security domain, a fundamental issue remains, to scientifically study a topic requires a definition which enables researchers to describe processes and variables by which an object, event or construct can be observed and objectively measured. Such a definition is termed an "operational definition". To facilitate objective measurement it is therefore necessary to utilize or formulate such a definition (Runyon, Coleman & Pittenger, 2000, p. 11). Given security as a profession lacks consensus in definition (Borodzicz and Gibson, 2006, p.182; Manunta, 1999, p. 58) this study engaged in thematic analysis (Liamputtong & Ezzy, 2006, p. 259) extracting common themes (factors) and key words (processes) from the available literature (see; Maslow, 1970; Felson, 1979; O'Block, Donnermeyer & Doeren, 1991; Post, Kingsbury & Schachtsiek, 1991; Manunta, 1999; Garcia, 2001; Craighead, 2003; Fisher & Green, 2004; Borodzicz & Gibson, 2006; Standards Australia HB 167; Brooks, 2007; Somerson, 2009) to establish an operational definition, operationally defining security as:

> *A stable condition stemming from a systematic process which effectively combines people, equipment and procedures, within a security context, to restrict unauthorised access to either people, information or physical assets through their ability to deter, detect, delay and respond to attacks*

which may lead to loss of, or, harm to protected assets manifested by a malevolent human adversary/s who seek/s to gain a level of unauthorised access.

This study argues that such a definition enables a security context to be established, enables direct observation of measures combined to deter, detect, delay and respond to adversary attacks therefore facilitating objective measurement of the protection systems effectiveness, which is essential in any endeavour to objectively study a phenomenon under investigation.

2.2 Underlying theory

The theory of Defence in Depth is implemented in security management using a systems approach (Garcia, 2001, p. 6), an approach supported by many published security professional (Underwood, 1984, p. xi; Fennelly, 1997; Garcia, 2001, p. 6; Fisher & Green, 2003, p. 164). As Fennelly (1997, p. 59) states "maximum security is a concept, whereas alarm systems, physical barriers, guard forces and other components of a security system do not individually (in isolation) achieve this". Fisher and Green (2003, p. 147) support Fennelly's (1997) viewpoint, adding, every security program must be an integrated "whole". As such, the underlying theory for this study was General Systems Theory (GST).

2.2.1 Systems theory, history and science

The systems approach towards operational security stems from the science of systems thinking. Systems approach originated in biology in the 1920s, through the works of Kohler to elaborate the most general properties of inorganic compared to organic systems (Bertalanffy, 1969, p. 11); however, as an area of scientific generalization, the idea of a General Systems Theory (GST) was first introduced by Bertalanffy (1950). Bertalanffy (1950, p. 142) believed a general theory of systems should be an important regulative device in science to guard against superficial analogies which he regarded as having no basis in science.

At the same time that Bertalanffy was developing GST, Wiener (1948) was developing cybernetics as a result of developments in computer technology, self-regulating machines and information theory (Bertalanffy, 1968, p. 15). Cybernetics is a theory of control systems based on communication transfer (transfer of information) between

systems, the environment and within the system, and control (feedback) of the systems' function in regards to the environment (Bertalanffy, 1968, p. 22).

These developments in systems thinking occurred simultaneously with Shannon and Weaver's (1949) information theory, and Von Neuman and Morgenstern's (1947) Game Theory (Bertalanffy, 1968, p. 15). Information theory is based on the concept of information identified by an expression isomorphic to negative entropy of thermodynamics, where the information may be used as a measure of organisation. Game Theory is a "system" of antagonistic "forces" with specifications, concerned with the behaviour of seemingly "rational" players to obtain maximal gains and minimal losses by appropriate strategies against other players (or nature) (Bertalanffy, 1968, p. 22). However, the focus for this study is the application of Bertalanffy's (1950) General Systems Theory (GST) to the security literature.

According to Bertalanffy (1950, p. 139) General Systems Theory (GST) is a logico-mathematical field, with the subject matter being the formulation and deduction of those principles which are valid for 'systems' in general. Bertalanffy (1950, p. 139) stated "there are principles which apply to systems in general, whatever the nature of their component elements, or of the relations or forces between them. Bertalanffy (1950, p. 142) considered that GST should be methodologically; an important means of controlling and investigating the transfer of principles from one field to another, where it should no longer be necessary to duplicate or triplicate the discovery of the same principles in different fields, isolated from each other.

Systems Theory according to Checkland (1981, p.5) is a meta-discipline, that is, in contrast to other disciplines, which are concerned with particular sets of phenomena such as chemistry or physics. GST's focus is towards subject matter which can be applied within virtually any other discipline. The underlying premises supporting the systems approach to science stems from the argument that, general aspects and viewpoints in different fields of science are alike, and that we find formally identical or isomorphic laws in completely different fields of science (Bertalanffy, 1950, pp. 136-138). That is, the isomorphism of natural laws are characterised by the fact that they, in general, hold for certain classes of complexes or systems, irrespective of the special kinds of entities involved.

As such, general systems laws exist which apply to any system of a certain type, irrespective of the particular properties of the system or elements involved. In discussing the premises of systems theory Checkland (1981, p.6) explains that science provides man with the phrase "a scientific approach", just as systems provides "a systems approach". Both approaches are meta-disciplines, and both embody a particular way of regarding the world.

Bertalanffy (1968, p. 6) further explains that the systems approach according to the basic propositions of science; as systems are part of the scientific tradition; assumes the world contains structural wholes, which can maintain their identity under a range of conditions and exhibit certain general principles of "wholeness". Bertalanffy (1968, pp. 36-37) considered that prior to systems theory, science attempted to explain observable phenomena by reducing it into its elementary units, independently of each other. A process Bertalanffy (1968) refers to as reductionism. However, according to Bertalanffy (1968, p. 18) conceptions in science appeared which were concerned with "wholeness", where wholeness relates to problems of organisation, phenomena not observable by respective parts in isolation.

Bertalanffy (1968, p. 18) considered "the system problem as essentially, a problem of such limited analytical procedures in science (reductionism)". According to Bertalanffy (1968, p. 18) the success of reductionism principles are highly applicable depending on two conditions. First, the interrelations between "parts" must be non-existent or weak enough to be neglected for certain research purposes. Second, the relations describing the parts be linear, only then is the condition of sumativity given i.e., an equation describing the behaviour of the total is the same form as the equations describing the behaviour of the parts.

Expanding on Bertalanffy's (1968) discussion, Checkland (1981, p. 105) explains that General Systems Theory is the skeleton of science, in that, it aims to provide a framework or structure of systems on which to hang the flesh and blood of particular disciplines and particular subject matters in an orderly and coherent corps of knowledge.

2.2.2 Defining systems

The systems approach, and more specifically its framing literature, has lead to systems being defined in many ways (Churchman, 1968, p. 29), embodying many meanings

(Midgley, 2003, p. 178). In considering a single definition of a system Aslaksen (2004, p. 271) explains that systems are defined in terms of their boundaries and interactions. A view supported by Midgley (2003, p. xxiii) who suggests GST proposes that systems of all kinds share specific common characteristics which can be described through the use of both mathematics and ordinary language.

Through the use of mathematics Bertalanffy (1968, p. 56) defines a system as a complex of interacting elements, for example, P_1, $p_2 \ldots p_n$. Interaction means that elements, p, stand in relations, R, so that the behaviour of an element p in R is different from its behaviour in another relation, R'. According to Bertalanffy (1968, p. 56) if the behaviour in R and R' are not different, there is no interaction, and the elements behave independently with respect to the relations R and R'. Bertalanffy (1950, p. 143; 1968, p. 56) explains his approach utilizing a system of simultaneous differential equations. Denoting some measures of elements, p_i (i = 1, 2, ….n), by Q_i, these for a finite number of elements and in the simplest of cases, will be in the form of:

$$\left.\begin{aligned} \frac{dQ_1}{dt} &= f_1\,(Q_1, Q_2, \ldots Q_n) \\ \frac{dQ_2}{dt} &= f_2\,(Q_1, Q_2, \ldots Q_n) \\ \frac{dQ_n}{dt} &= f_n\,(Q_1, Q_2, \ldots Q_n) \end{aligned}\right\} \qquad (1)$$

According to Bertalanffy (1950, p. 143; 1968, p. 56) change of any measure Q_i therefore is a function of all Q's from Q_1 to Q_n; conversely, change of any Q_i entails change of all other measures and of the system as a whole.

Bertalanffy (1950, p. 144; 1968, p. 57) argues that this equation can be used to a) show the structural isomorphism in different fields and levels of reality, that is, to demonstrate the possibility of a General Systems Theory whose fields of application are to be found in various sciences. Although the parameters and variables will have very different meaning in each case of application, b) discuss several general systems properties. Although nothing is said about the nature of the measures Q_i or the functions f_i-i.e.,

about the relations or interactions within the system certain general principles can be deduced.

In explaining systems through the use of language Bertalanffy (1968, p. 19) defined a system as "sets of elements standing in interaction". Bittel (1978, p. 1130) further defined a system as 'a set of interrelated components that function together within constraints towards a common purpose", whilst Waldman (2007, p. 271) considers a system to be an assemblage or combination of things or parts forming a complex or unitary whole. However, Morales-Matamoros, Tejeida-Padilla and Badillo-Pina (2010, p. 88) state that a system is defined as "a group of components that keep some identifiable set of relationships with the sum of their components (subsystems), in addition to relationships (systems themselves) to other entities".

Faithful to Bertalanffy's (1968) works, Midgley (2003, p. xxii) defines a system as a unity of organised elements, where according to Midgley (2003, p. xxii) a system's organisation is crucial as it provides rise to properties of the system which cannot be found in a disorganised collection of the same elements. For example, Midgley (2003, pp. xxii-xxiii) states "a person can only remain alive as long as their parts are organised in a set of particular relationships with one another. A random collection of organs is not a living person". Hall and Fagen (cited in Midgley, 2003, p. xxv) consider a system to be a set of objects together with relationships between the objects and between their attributes (Hall & Fagen, cited in Midgley, 2003, p. xxv).

In considering the different approaches (semantics) towards defining systems, according to Bittel (1978, p. 29) all definers' agree that a system is a set of parts coordinated to accomplish a set of goals, where according to Midgley (2003, p. 64) it is the relationships that "tie the system together". That is, such relationships create the notion of "system" useful. Midgley's (2003, p. 64) view is supported by Ackoff (1981 cited in Skyttner, 1996, p. 35) who states "a system is two or more elements which satisfy the following conditions:

- The behaviour of each element has an effect on the behaviour as a whole,
- The behaviour of the elements and their effects on the whole are interdependent,
- However, subgroups of the elements are formed, all have an effect on the behaviour of the whole, but none has independent effect on it.

Uniform to Ackoff (1981 cited in Skyttner, 1996, p. 35), Midgley (2003, p. 68) considers that from the various systems definitions, any given system can be further divided into sub-systems. That is, "in every system it is possible to identify one sort of unit, each of which carries out a distinct and separate process, and another sort of unit, each of which is a discrete, separate structure. According to Midgley (2003, p. 201) the totality of all the structures in a system which carry out a particular process is a subsystem". Tejeida-Padilla, Badillo-Pina, and Morales-Matamoros (2010, p.88) explain that a subsystem is "a greater systems component", that is, when a greater system is constructed of two or more interacting and interdependent components, where the subsystems interact in order to obtain their own purpose(s) and the purpose(s) of the system in which they are embedded.

In considering the lack of a single definition, yet common themes, this research suggests a system can therefore be summarised as "an organised collection of constituents, which are combined into various subsystems (elements), which are highly interrelated towards the accomplishment of an overall, predetermined design goal". That is, a system comprises of various smaller constituent parts which provide various inputs, which, to achieve desired outputs go through specific predefined processes.

2.2.3 The systems approach

Systems theory has a strong history and in contemporary times this approach is supported by Waldman (2007, p. 1) who states, "now" most outcomes or outputs are derived from interactions within systems composed of machines, computers and people. These systems represent thinking systems and thinking systems require system thinking. Waldman (2007, p. 1) defines thinking as "having a conscious (self-aware) mind, to some extent of reasoning, remembering experiences, making rational decision", thinking involves "volition" (Waldman, 2007, p. 272).

According to Waldman (2007, p. 278) systems thinking embodies an approach towards understanding how things work. Bertalanffy (1968, pp. 4-14) explains that systems thinking was driven by technological advances after the 2nd World War, which saw the combining of components originating in heterogeneous technologies including mechanical, electrical and chemical. In addition, within these heterogeneous technologies relations between man and machine became interrelated. These component

interrelations required a systems approach, as though systems had been studied for centuries it became a requirement to study the interactions within.

The systems approach is concerned with a holistic view of interacting components that function together towards achieving a common purpose (Bittel, 1978, p. 1130). This approach involves a rational plan of the constituent components of a system and their operational function. That is, it is about thinking about the systems purpose "what it is for". The ultimate aim of such component thinking is to discover those components whose measures of performance are truly related to the measures of performance of the whole system (Churchman, 1968, p. 43). For example, according to Waldman (2007, p. 272) if a part of the system is changed, the nature of the overall system is often changed as well. Waldman (2007, p. 272) bases this premise on the argument that by definition, a system is systemic, meaning relating to or affecting the entire system. Waldman (2007, p. 272) refers this to co-evolution, where interactive changes between system components leads to what was eventually termed "the butterfly effect".

2.2.4 The butterfly effect

Consistent with Waldman's (2007, p. 272) view that as part of the system changes the nature of the overall system changes, the butterfly effect is a phenomenon which relates to this underlying premise of systems theory (Peirce, 2000, p. 5). Systems theory considers that as small changes occur in the various systems' sub-systems, or their constituents, these small changes perturb or reverberate through the system in a manner which produces significant change. Evidence supporting this premise stems from research conducted by meteorologist Edward Lorenz (1963; 1968). Lorenz (1963) was using non-linear equations to plot weather patterns across time. As part of Lorenz's (1963) simulation process, the initial conditions of a program he was utilizing had used the numerical input 0.506127 correct to six (6) decimal places. However, when Lorenz (1963) repeated the simulation to save time, the numerical input was rounded down to three (3) decimal places, inputting 0.506. According to Peirce (2000, p. 5) Lorenz assumed that the difference, one input in a thousand, would be inconsequential. However, Lorenz (1963) found small changes as an input were not inconsequential.

Lorenz (1963) found a small difference can, over a long period of time, build to produce a large effect. Moreover, the way the difference affects the outcome is very sensitive to

small changes, finding that small perturbation of weather elements can have a large effect later on (Peirce, 2000, p. 5). Technically this is termed "*sensitivity to initial conditions*", which means that any difference in input into a system, no matter how small, will eventually produce enormous differences in output. More graphically "sensitivity to initial conditions" is referred to as the "Butterfly Effect" (Warren, Franklin & Streeter, 1998, p. 363).

The butterfly metaphor stems from Lorenz's (1968, p. 306) original metaphor for describing sensitivity to initial conditions where Lorenz (1968) stated "if the theory of atmospheric instability were correct, one flap of a sea gull's wings would forever change the future course of the weather". According to Lorenz (1968, p. 306) a disturbance created by a single flap of a sea gull's wings is a point disturbance, supposing that after some small time interval the smaller-scale errors resulting from an initial point disturbance have grown to become large in amplitude as the smaller-scale motions on which they were superimposed within a region near the initial disturbance, but the errors are still undetectable over most of the globe (at the macro level). The error energy is still then very small compared to the global kinetic energy in the same scale. However, in actuality, the error will already have entered their non-linear phase of growth, since they are large in those locations where they exist at all, and they should no longer be amplifying except near the boundary of the region in which they occupy.

This effect error propagation has come to be known as the "Butterfly Effect", based on several sea gull analogies such as "the flap of a butterfly's wings in Brazil can set off a tornado in Texas (Hilborn, 2003, p. 425), or a single butterfly flapping its wings in China might, weeks later, cause a hurricane in New York (Peirce, 2000, p. 5). Lorenz's (1963; 1968) works are considered in many variations of systems theory, where the systems approach is based on the premise that as individual measures of performance of constituent components increase, so does the holistic measure of performance of the total system (Churchman, 1968, pp. 42-43).

As such, Churchman (1968, pp. 42-43) considers that the separation of systems into their component parts provides systems analyst with information necessary for evaluating whether the system is operating properly and if and what corrective measures are required to maintain the system at its commissioning level of effectiveness. Such a segmentation process also enables systems managers' to ensure all monies spent in

maintaining the system are spent correctly, contributing to the real objectives of the system ensuring fiscal restraint of limited financial resources.

2.2.5 Different types of systems

According to Midgley (2003, p. xix) there are many different system ideas, with different systems paradigms embracing various ideas pertaining to what constitutes systems thinking. Nevertheless, there are common points, for example, Barton and Haslett (2007, p. 44) suggest systems thinking involves the scientific methods of both analysis and synthesis, that is, systems thinking lies within the dialectic between the two scientific methodologies. Analysis is defined as the procedure by which investigators break-down an intellectual or substantial whole into its constituents (component parts). In contrast, synthesis involves combining a systems constituents or elements to form a coherent whole (Ritchey, 1991, p. 1).

According to Barton and Haslett (2007, p. 145) science has debated the order in which analysis and synthesis are applied. However, Holton (cited in Barton & Haslett, 2007, p. 146) points out that Descartes and Newton agreed with Plato, that for a given initial hypothesis, analysis must precede synthesis. This sequence is based on the argument that without a previous analysis, attempting synthesis does not lead to truth. A view supported by Ritchey (1991, p. 10) who argues that every synthesis is built upon the results of a preceding analysis, where every analysis requires a subsequent synthesis in order to verify and correct its results. As such, Barton and Haslett (2007, pp. 147-148) suggest systems thinking provides a distinctive way of framing this dialectic where systems thinkers recognize that individual (analysis) events are part of a pattern (synthesis) of events. That is, the analytic process attempts to explain how something works, whilst synthesis attempts to establish understanding of its purpose. Therefore systems thinking occurs when people use the cognitive construct of thinking to frame the scientific process, defined as “a dialectic between analysis and synthesis” (Barton & Haslett, 2007, pp. 147-153).

2.2.6 System typologies

According to Midgley (2003, p. xix) there are different types of systems, with a number of dichotomies each drawing attention to particular aspects of systems thinking (Barton & Haslett, 2007, p. 151). These include whole versus parts, soft versus hard, complex versus simple and open versus closed systems; however, according to Barton and Haslett (2007, p. 151) the most significant development in scientific method towards

systems thinking has stemmed from the open versus closed dichotomy. In considering the various systems dichotomies this thesis focused on the closed versus open approach and briefly discuss these approaches within a complex aspect.

2.2.6.1 Closed systems

Bertalanffy (1968, p. 39) defines closed systems as those considered isolated from their environment, meaning a concrete system with impermeable boundaries through which no materials (energy or information) can enter or leave (Midgley, 2003, p. 182). Midgley (2003, p. 182) explains that within a closed system whatever matter-energy happens to be within the system is finite and it gradually becomes disordered. Closed systems theory therefore emphasises the tendency towards equilibrium (Keren, 1979, p. 312), where according to the laws of thermodynamics, closed systems attain a time-independent equilibrium state, with maximum entropy and minimum free energy (Bertalanffy, 1950, p. 23). Thermodynamic equilibrium (Figure 2.3) describes a condition in a system where the distribution of mass and energy moves towards maximum entropy (Pidwirny, 2006).

Figure 2.3 The thermodynamic equilibrium of a system over time (Pidwirny, 2006).

Thermodynamic equilibrium (entropy state) is a measure of the amount of heat and work that is associated with a system, as left to itself accordant with the laws of thermodynamics, a physical system tends to maximise its entropy (Lovey & Manohar, 2007, p. 99; Styer, 2000, p. 1).

2.2.6.2 Open systems

In contrast to closed systems, there are those systems which by their very nature and definition are not closed systems. According to Midgley (2003, p. 182) most concrete systems have boundaries, which are at least partially permeable, permitting magnitudes of at least certain sorts of matter-energy or information transmissions to cross them. These systems are defined as open systems. Traditional physics and physical chemistry

exclusively focused on closed systems; however, the need to consider organisms and other living systems meant that it was necessary to generalise systems theory (Bertalanffy, 1950, p. 155).

According to Bertalanffy (1950, p. 155) open systems theory has lead to new and revolutionary consequences and principles for the discipline of physics, as it provides for important generalization of physical theory, kinetics and thermodynamics. This approach has lead to new principles and insight, such as the principle of equifinality, the generalization of the second thermodynamics principle (second law of thermodynamics), and the possible increase of order in open systems (Bertalanffy, 1968, p. 102).

Open systems theory considers the interaction with the environment as crucial to the adoption and evolution of complex systems. Open systems depend on their environment for resources and are constrained by its influences (Bittel, 1978, p. 1130). For an open system, the ability to change in response to environmental pressures ensures the systems' long term viability. Open exchange with the environment implies adjustment, both as adaption and innovation (Keren, 1979, p. 316).

In contrast to a closed system which eventually attains a time-independent equilibrium state, an open system may attain (certain conditions presumed) a stationary state where the system remains constant as a whole and in its phases, through a continuous flow of the component materials. Such a state is referred to as a steady state (Bertalanffy, 1950, p. 23) defined by Martin (2000, p. 210) as a state encompassing very little change, which according to Honkasalo (1998, p. 134) describes a situation where the flow of energy is constant and the increase in entropy is at a minimum. According to Martin (2000, p. 210) the amount of change in a steady state can be considered as a percentage of a preset threshold level, where Bertalanffy (1950, p. 157) explains that a system's steady state condition is maintained through a continuous exchange, between the in-flow, and out-flow of feed-back materials, where a steady state equilibrium (Figure 2.4) shows an average condition of a system where the trajectory (average) remains unchanged over time (Pidwirny, 2006).

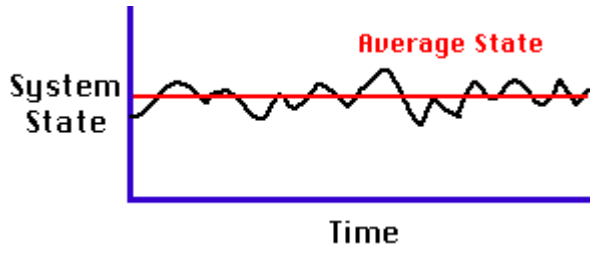


Figure 2.4 A steady state system (average condition) over time (Pidwirny, 2006).

Whilst the final state in a closed system depends on the components given at the beginning of the process, steady state systems (open systems) show equifinality (Bertalanffy, 1950, p. 158). If a steady state is reached in an open system, it is independent of the initial conditions and determined by the system's parameters. Equifinality in open systems can be characterised by phenomena such as overshoot, false start and asymmetry, (Figure 2.5) where the system may initially proceed in one direction, which is opposite to, or different from that which eventually leads to its steady state condition. For example, in Figure 2.5, path A indicates that a steady state can be achieved from an initial condition of overshoot, whereas path B shows an asymmetric approach to a steady state, and path C shows a fake start towards achieving a steady state condition (Bertalanffy, 1968, p. 143).

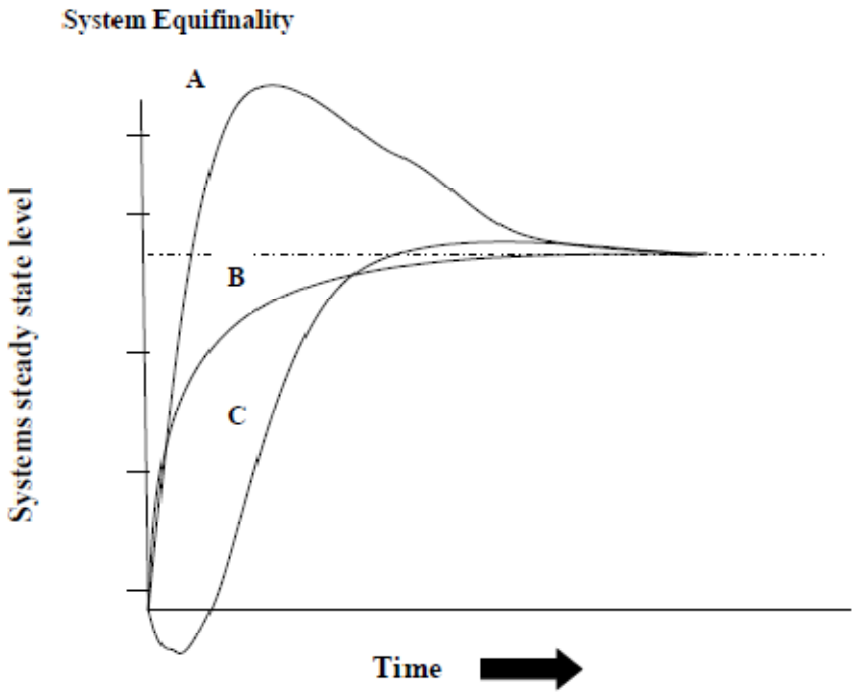


Figure 2.5 System Equifinality (Bertalanffy, 1968, p. 143).

According to Bertalanffy (1968, pp. 142-143) the steady state in an open system is maintained in distance from true equilibrium and therefore is capable of doing work, in contrast to closed systems in equilibrium. That is, the system remains constant in its composition, regardless of continuous irreversible processes, import and export, and building up, and breaking down, taking place.

In discussing the characteristics of open systems Checkland (1981, p. 83) explains that the steady state of an open system may be thermodynamically unlikely, creating and/or maintaining a high degree of order, whereas closed systems by their isolated nature have no path to travel except towards increasing disorder (high entropy). The steady states in open systems are not defined by maximum entropy, but by the approach of minimum entropy production. Entropy in open systems may decrease where the steady states with minimum entropy production are generally stable systems. Therefore, if one of the systems variables is altered, the systems manifests changes in the opposite direction (Bertalanffy, 1950, p. 26), this property is consistent with Lorenz's (1963) findings, and "Butterfly" metaphor.

In discussing an open systems capacity to maintain their steady state (homeostasis), Keren (1979, p. 316) points out that open systems theory emphasises the role of feed-back in systems survival. Feed-back is the process where energy is imported from the environment beyond that which has been expended. As open systems are energy-processing, they feed on throughputs of energy to sustain order or negative entropy (negentropy) and can therefore, through their feed-back processes remain in a sustainable condition of disequilibrium (Morales- Matamoros, Tejeida-Padilla & Badillo-Pina, 2010, pp. 75-76). In an open system Feed-back means from the output of a machine a certain amount is monitored back (Figure 2.6), as information to the input towards regulating the output to stabilize as directed the action of the machine (Bertalanffy, 1950, p. 160).

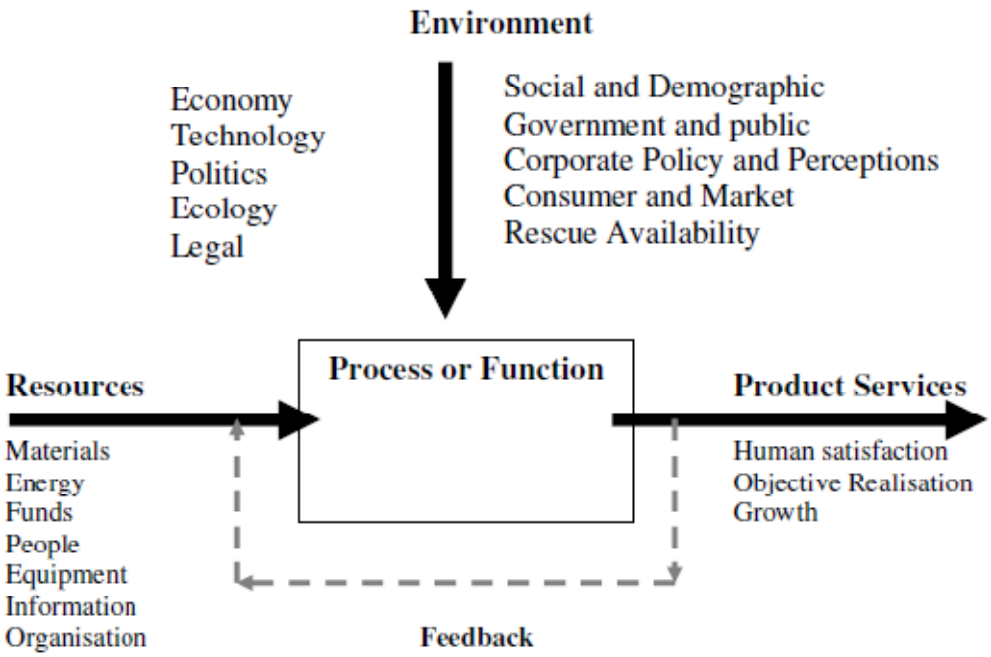


Figure 2.6 Open system typology with feedback mechanism (Bittel, 1978, p. 1131).

Figure 2.6 demonstrates the processes of an open system, where resources such as energy, financial inputs and people, etc., become the systems inputs. These inputs are put through a pre-determined process, influenced by the environment in which they exists towards producing the desired product as the systems macro-state output. From the product output, for an open system, a feed-back loop is maintained to ensure appropriate energy inputs sustain the system at a distance away from equilibrium (steady state).

2.2.7 System complexity

Systems are generally classified as concrete (physical), conceptual, abstract or unperceivable, where the most common system being concrete or physical systems. Physical systems are those which exist in physical reality of space and time, and are defined as those systems consisting of at least two units or objects. Concrete systems can be living or non-living, natural or man-made, and can be classified according to their level of complexity. Complex behaviour can occur in any system made up of a large number of interacting components with non-linear coupling (Morales-Matamoros, et al, 2009, p. 72). In an organised-complexity system only a finite but large number of components will define the system (Skyttner, 1996, p. 43). According to Smarr (1985 cited in Corning, 1995, p. 93) complexity is a multi-dimensional, multi-disciplinary concept, where there is no single right means to either define or measure it.

For example, Smarr (1985 cited in Corning, 1995, p. 93) explains that a mathematician might define complexity in terms of the number of degrees of freedom in computational operations, whereas a physicist may be more focused with the number and frequency of interactions in a system of interacting gas molecules. In contrast, Waldman (2007, p. 271) considers a bicycle to be a complex system based on the variety of its parts and their interrelations.

In considering a standard definition of a complex system Sheard and Mostashari (2008, p. 296) have adopted that previously developed by scientists conducting research focusing on complexity theory and its descendants. Sheard and Mostashari (2008, p. 296) define a complex systems as "systems that do not have a centralizing authority and are not designed from a known specification, but instead involve disparate stakeholders creating systems that are functional for other purposes and are only brought together in the complex system because individual agents of the system see such cooperation as being beneficial for them".

According to Sheard and Mostashari (2008, p. 296) complex systems have autonomous components, where the elements are heterogeneous. In addition, complex systems are self-organizing, showing a decrease in entropy due to utilizing energy from the environment. They display emergent macro-level behaviour which emerges from the actions and interactions of the individual constituents, and their interactions among the parts matters dramatically. Finally, complex systems elements change in response to imposed "pressures" from neighbouring elements. Such a discourse regarding what constitutes a complex system is supported by Midgley (2003, p. 386) who refers to a complex system as one constructed of a large number of parts that interact in non simple ways. According to Midgley (2003, p. 386) in such systems the whole is more than the sum of its parts, not in an ultimate metaphysical sense, but in the important pragmatic sense that, given the properties of the parts and the laws which govern their interaction, it is not a trivial matter to infer the properties of their whole.

2.2.8 Benefits of systems thinking

In considering the literature relating to systems theory Waldman (2007, p. 1) argues that such an approach has significant benefits. According to Waldman (2007, p. 1) systems thinking results in silo framed thinking styles being avoided. Silo thinking is a phenomenon where humans think and react individually and locally rather than collectively or globally. Silo thinking aims to simplify or reduce complexity

(reductionism) towards a phenomenon being investigated, whereas systems thinking aims to analyse and integrate as part of the same thought process (Albrecht, 2010, p. 2).

Silo thinking refers to a metaphor drawn from large grain silo's and its term suggests that just as each silo stands alone, each aspect of a problem (such as a system) is solved in isolation, standing alone. According to Waldman (2007) such thinking often degrades net system outcomes, whereas systems thinking forces people to focus on processes, interactions and causes of outcomes, rather than the components in isolation. In contrast, GST is considered the scientific exploration of "wholes" and "wholeness" (Schaefer, Hensel & Brady, 1977, p. 12). For example, giving a drug to a patient to improve kidney function without considering its effects on the liver is an example of silo thinking (Waldman, 2007, p. 1). In short, the system model considers the whole system in action, not just the output of the system (Keren, 1979, p. 314).

In applying GST to the application of physical security the underlying assumptions of systems theory can be traced through history; however, Fredrich Hegel (1770-1831) formulated four generic and significant statements concerning systems theory which hold true in contemporary systems thinking:

- The whole is more than the sum of its parts,
- The whole defines the nature of the parts,
- The parts cannot be understood by studying the whole,
- The parts are dynamically interrelated and interdependent (Skyttner, 1996, p. 30).

2.2.9 The systems approach to physical protection

Designed physical systems exist as a direct result of an identified specific need in some human activity (Checkland, 1981, p. 119). For security systems, Garcia (2001) explains that the designed goal is the successful interrupting of an adversary**.** To achieve their goal security systems require resources from their environment. That is, consistent with the premises supporting open systems in general, security systems rely on the input of finances, people, energy, equipment, information and organisation to achieve their service product. This product is the successful interruption of a malevolent human adversary.

2.3 Conclusion

The chapter provided stage one of the study's first phase in the research process. In this chapter security's diversity and lack of definitional consensus among published authors was discussed. Nevertheless, the chapter highlighted that despite such diversity a common thread was the systems approach utilized to employ the theory of Defence in Depth towards protecting organisational assets. These themes set the theoretical frame for the study. Consistent with these themes and conforming to the writings of Runyon, Coleman and Pittenger (2000, p. 11) this chapter presented a systems based operational definition of security, establishing a measureable context for discussing physical security decay.

Congruous with the study's operational definition of security, the chapter presented and discussed General Systems Theory (GST) as the study's underlying theory. Within the context of GST, Section 2.2.1 discussed Systems Theory, history and science. In addition, a number of GST concepts and principles were discussed including defining systems, the systems approach, the Butterfly effect, different types of systems and typologies such as closed and open systems. These combined concepts and principles lead to a discussion on the benefits of systems thinking. As a result of this discussion a systems approach for considering the concept of physical security consistent with the writings of such published security professional (Underwood, 1984, p. xi; Fennelly, 1997; Garcia, 2001, p. 6; Fisher & Green, 2003, p. 164) was established. This discussion provided a detailed theoretical underpinning to be taken forward into Chapters 3 and 4 for considering the concept of security decay within an open systems approach to physical security.

CHAPTER 3

AN OPEN SYSTEMS APPROACH TO PHYSICAL SECURITY

Introduction

This chapter presents the second stage of phase one of the study; establishing an open systems framed physical security benchmark. Consistent with the principles of the conceptual review of literature, the chapter brings forward the writings from Chapter 2 to establish an open systems physical security benchmark. Section 3.1 discusses an open systems approach to physical protection. This discussion applies the underpinnings of General Systems Theory (GST) highlighting how the systems interrelations achieve the systems output goal. Section 3.2 combines the available literature defining Physical Protection Systems (PPS) within GST frame. Accordant with the study's operational definition of security, Section 3.3 presents a discussion on measuring a Physical Protection System's effectiveness. This discussion embeds a quantitative approach to physical security for discussing physical security decay. Central to establishing a steady state PPS Section 3.4 discusses security and risk management which underpins the systems established level of Defence in Depth elements. The chapter concludes with Section 3.5.

3.1 An open systems approach to physical protection

In applying the systems literature to physical security, the physical components of an organisational security program relates to the establishment of barriers including fences, locks, gates, vaults, alarm systems, sensory devices, protective lighting and security personnel (Post, Kingsbury and Schachtsiek, 1991, pp. 97-99). Within a systems approach these physical components of the holistic security program are defined by Garcia (2001, p. 6) as a Physical Protection System (PPS). Concordant with the study's operational definition of security, an effective security system must be able to detect an adversary then delay this adversary long enough along their attack path to provide sufficient time for a facility's response force to arrive and neutralize the threat before the adversary accomplishes their desired goal (SAND Report, 2002, appendix D). As such, congruous with the theory of Defence in Depth the primary functions of such a system are the detection and assessment of any adversary's intrusions, the delaying of the adversary's progress along their attack path exposing them to a prompt response (Spencer, 1998, p. 3).

Concordant with the writings of Bertalanffy (1950, p. 26; 1968, p. 39; Bittel, 1978, p. 1130; Keren, 1979, p. 316; Checkland, 1981, p. 83) a Physical Protection System (PPS) is defined as a complex, open system. Bittel (1978, p. 1131) explains that for open systems, external constraints become important parts of the definition of the system boundary. The characteristics of such systems are constitutive, that is, those which are dependent on the specific relations within the complex. As such, for understanding such characteristics their parts and their interrelations must be known. That is, the system must be spelt out (mapped) (Bertalanffy, 1968, p. 55). Conforming to the systems philosophy Garcia (2001; 2006) explains that a PPS must achieve its objectives by either deterring, or a combination of detection, delay and responding to unauthorised security events. Therefore, in order to map the system the various components of deter, detect, delay and response, and their systems based interrelations must be spelt out in detail.

3.1.1 Deterrence

According to the theory of defence in depth the first element is deterrence (Smith, 2003, p. 8). All security systems have some level of deterrence which is related to level of dedication and sophistication of the threat agent and the relative value and/or criticality of the asset requiring a level of security (MIL-HDBK-1013/1, 1993, p. 24). Mosely and Coleman (2000, p. 101) consider it is the systems deterrence value which is saliently important when protecting a site against low level opportunistic offenders. As such, according to Broder (2006, pxiv) true to the first element of Defence in Depth cost effective security measures should be designed, refined and evaluated to deter would-be offenders, where Broder (2006) considers that to deter an attacker the perimeter must have the appearance of being too difficult to defeat and/or being able to inflict injury.

Deterrence can be defined as ‘something which discourages (from acting) or prevents (from occurring) usually by instilling fear, doubt or anxiety (Collins Dictionary, p. 342). As such, deterrence as a concept is argued to be a perceptual phenomenon (Nagin, 2002, p. 5), which according to Walker (1988) stems from the Latin word deterre, meaning ‘to frighten’. Walker (1988, p. 11) suggests that experience and research supports the argument that offenders are not immune to fear as a deterrent. Therefore, in designing security systems the psychological aspects governing offenders are considered towards persuading them that it is not worth their while to make an attempt against an asset, or

that if they do try, they will fail or be caught in the act (Walker, 1988, p. 11). In considering the concept of deterrence Tilley (2005, p. 268) explains that where there are predictable systems, risks, rewards, effort needed and the tools required for success can all, in principle, be gauged in advance.

The application of GST, that is, a systems philosophy to the deterrence, is related to the concept of free choice, where according to Bertalanffy (1986, p. 114) free choice from a system perspective is described by formulations of Game Theory and Decision Theory. Axiomatically both Game Theory and Decision Theory are concerned with "rational choice". Rational choice refers to a choice which "maximises" an individual's utility or satisfaction, that the individual is free to choose among several possible courses of action and decides among them on the basis of their consequences of their actions, what stands highest on the list, "they" prefer more of a commodity to less, other things being equal. This discussion of "rational choice" includes everything that can be meant as "free will".

The concept of deterrence is considered within the rational choice framework where it is argued that an attack will occur if; $EU_{offence} > EU_{legal} + U_{taste}$ (Winoto, 2003, p. 2), where such expected utility decisions are based on the decision making formula: (1), the expected gain from committing the offence symbolised by, $EU_{offence}$, an offender acts according to their expected utility, represented by: $EU_{offence} = (1-p)\ U_1 + p_c U_2$. Where U_1 is the return from the offence, P_c is the perceived probability of conviction, and U_2 is the punishment. (2), Expected gain from not committing the offence, EU_{legal}. (3), Taste (or distaste) and preference for offence, U_{taste}- a combination of moral values, proclivity for violence, and preference for risk. Based on this model an offender will attempt an offence/attack if $EU_{offence} > EU_{legal} + U_{taste}$ (Winoto, 2003, p. 2).

Based on Winoto's (2003) formula, it is purported that the sequential strategy of Defence in Depth aims to, and for deterrence to be achieved must, communicate to an adversary that $EU_{offence} < EU_{legal} + U_{taste}$ (adjusted from, Winoto, 2003, p. 2) resulting in a rational choice by adversaries to refrain from their desired course of action, deterring them from ever attempting a penetration against an organisation (Cornish & Clarke, 1987, p. 934).

Within a linear relationship each function of the theory of defence in depth strategy must be achieved in their sequential order, where deterrence is achieved through systematic application of detect, delay and respond (D-DDR) (Garcia, 2006, p. 240), in this sequential combination (Garcia, 2001). This systematic combination aims to communicate to potential adversaries that the risks outweigh the benefits influencing their (however rudimentary) cost benefit equation (Cornish & Clarke, 1987, p. 934).

However, according to Cioffi-Revilla (1999, p. 243) deterrence must be supported by an efficacious capability for the risks to be perceived at the cost benefit analysis as greater than the potential gains. That is, deterrence is not a protection strategy; rather it is the anticipated result of implemented security measures at a facility (Garcia, 2006, p. 240). This supports deterrence as "a perceptual phenomenon", where, according to Hamlyn (1969, p. 3) contemporary psychological theories of perception have their roots, in one way or another, in Gestalt Theory. Gestalt in the German language has two meanings, its connotation with shape or form as an attribute of things, and a concrete entity which has, or, may have, a shape as one of its characteristics (Kohler, p. 104).

Gestalt principles help explain how people subjectively organize perception, drawing on the principles of proximity, closure, similarity, simplicity and continuity (Weiten, 2002, p. 109). Gestalt is a product of organization, organization, the process that leads to a Gestalt. That is, organization as a category is completely opposed to more side-by-side or random distribution. In the process of organization, "what happens to a part of the whole, is determined by intrinsic laws inherent within this whole" (Koffka, 1963, pp. 682-683).

Weiten (2002, p. 109) explains, sometimes "wholes", as they are perceived, may have qualities which do not exist in any of their parts. This "insight" became the basic tenant of Gestalt psychology (Weiten, 2002, p. 109), where according to Hamlyn (1969, p. 58) the most general thesis of Gestalt theory is that humans not only see whole objects or forms rather than parts which are synthesized, but there is a tendency to see such forms, "gestalten", as being as simple or "good" as possible. Hamlyn (1969, p. 3) points out, Gestalt psychologists purport that humans generally don't perceive the gaps between things, that is, unless they attend to them specifically with care (Hamlyn, 1969, p. 84).

Gestalt in English is used to refer to a concept of wholeness (Collins Concise Dictionary, N.D. p. 516), represented by the phrase "the whole is greater than the sum of its parts" (Gestalt, Psychology and Psychiatry, 2010), this phrase, drawn from Gestalt Theory, is congruous with the first of Fredrich Hegel's (1770 cited in Skyttner, 1996, p. 30) four statements concerning systems theory, which still hold true in contemporary systems thinking, Hegel (1770 cited in Skyttner, 1996, p. 30) also suggested as part of his systems thinking paradigm "the whole is more than the sum of its parts". It is this aspect of perception, "the view of wholeness" which it is argued that lends some offenders to view the security program as a "whole", and determine that the risks outweighs the benefits, ultimately "deterring" them. This is consistent with Underwood (1984, p. xi) who stated "it is important that security is seen as a whole", it is argued that the perceived ∑ detect, delay and response, as a form of "wholeness" is what drives the deterrence value of a PPS, where according to Garcia (2001, p. 2) the deterrent value of a true PPS can be very high.

Deterrence can be useful in discouraging attacks from opportunistic offenders'. However, the deterrence function of a security system is difficult to measure with no substantiated key performance indicators. As such, the reliance on successful deterrence can be risky (Garcia, 2001, p. 2). This is a view supported by Cioffi-Revilla (1999, p. 243) who states "sometimes deterrence works and sometimes it fails". Therefore, based on a two type offender typology (opportunistic/deliberate) (Underwood, 1984, pp. 3-4), where an adversary's internal drive is great enough, including situations stretching beyond personal gain towards subversion, systems must be designed for defeating attacks which are going ahead regardless of their overt deterrent value (Walker, 1988, p.11). Robinson (1999, p.38) supports such a view, stating "all targets can be breached given enough time". Therefore, "the aim of a protection system is to provide initial detection, then enough time for a response force to arrive and thwart an attack".

3.1.2 The physical protection system

When deterrence fails conforming with the remaining elements of defence in depth and Standards Australia HB 167 Security Risk Management (2006, p. 63) for a PPS to meet its objectives there must be an awareness that an attack is underway (detection), the slowing of an adversary's progress to the target (delay) and enough time for the response force to interrupt or stop the adversaries (response) before they achieve their goal. Physical Protection Systems (PPS) integrate people, procedures and equipment for

the protection of assets (Jang, Kwak, Yoo, Kim & Ki Yoon, 2008, p. 747) which makes them heterogeneous in nature. For example, Figure 3.1 highlights the functional elements of defence in depth and their interrelationship within PPS.

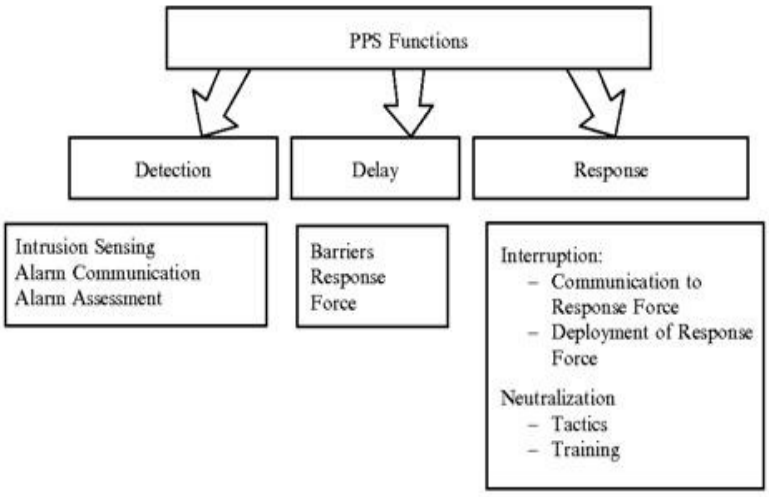


Figure 3.1 Functional elements and components (constituents) of a physical protection system (Garcia, 2006, p. 34).

3.1.3 System performance

According to Churchman (1968, p. 43) within a systems thinking approach, the ultimate aim is to discover those components whose measures of performance are truly related to the measure of performance of the whole system. A systems performance is proven by providing objective evidence that the program and/or system are doing what the designer states they are doing (Robinson, 1999, p. 58). Accordant with the premises of systems theory according to Churchman (1968, p. 30) system objectives must be some precise and specific measures of performance of the overall system.

In applying Churchman's (1968, p. 43) approach it is argued that a salient focus must be towards a systems macro-state performance measure and the various sub-system measures which combine to produce this macro-state measure. That is, the component measure must be analysed where ultimately a synthesis process must occur to achieve a macro-state output measure; where according to Dillon (1983, p. 183) mathematics provides the means of expressing such functional relations to which operational significance (measures of performance) can be attached. According to Dillon (1983, p. 183) from such mathematical relations logical deductions can be drawn through numerical manipulation. A systems performance measure is therefore a score which

describes how well the system is actually doing. Such objective evidence of a systems performance is also essential for a security system (PPS). For security professionals operating at levels from medium to high-risk facilities it is important to be able to determine the likelihood (probability) that, if their facility was attacked, the attacker(s) would be denied their success.

In considering a total system evaluation Churchman (1968, p. 29) suggests that when evaluating a system it is necessary to spell out in detail what the whole system is, the environment in which it lives, what its objectives is/are and how this is supported by the activities of its parts. Compatible with this study's definition of security Garcia (2001, pp. 242-249) explains that a PPS is a complex configuration of detection, delay and response elements, and that system performance measures should include probability of detection, delay times, and response times. This literature suggests that the best effectiveness measure (macro-state) for a PPS is one which combines these functional elements of defence in depth into a functional whole.

The holistic performance measure for a PPS (its macro-state) is the principle of timely detection, represented as its probability of interruption (Pi) (Garcia, 2001, p. 246). Pi is calculated from the variables of detection, delay and response (Jang, Kwak, Yoo, Kim & Ki Yoon, 2008, p. 748) and is the probability of intercepting an adversary before any theft or sabotage can occur, defined by Garcia (2001, p. 246) as "the cumulative probability of detection where there is enough time remaining for the response force to interrupt adversaries". Overall system performance measures are achieved through the combining of component subsystem performance measures (Spencer, 1998, p. 3), where consistent with the theory of Defence in Depth; the overall performance measure for a PPS is the measure of the sum of the detection, delay, and response function of the PPS (Garcia, 2001, p. 246).

Congruous with the study's definition of security, the scientific principles of analysis and synthesis facilitate the calculation of PPS effectiveness in terms of its degree of success in producing detection, delay and response functions of Defence in Depth (Jang, Kwak, Yoo, Kim & Ki Yoon, 2008, p. 748). According to Jang, Kwak, Yoo, Kim and Ki Yoon (2008, p. 748) due to the complexity of PPS its quantitative macro-state performance measure (P_I) is usually evaluated using computer modelling techniques, where Garcia (2001, p. 252) suggests this can be achieved utilizing the Estimate of

Adversary Sequence Interruption (EASI) model. This model referred to as EASI was developed in the 1970s and models one adversary path at a time, as selected by the model user. EASI uses specific quantitative input parameters representing the PPS functions of: detection, transmission, assessment, communication, delay and response performance values to compute the probability of interrupting an adversary before they accomplish their objectives (Spencer, 1998, p. 4). Such quantitative methods are systematic, repeatable and based on objective measures and demonstrate high statistical validity (SAND Report, 2002, p. 11). The input parameters for EASI require:

- Detection and communication inputs as probabilities that the total function will be successful; and
- Delay and response inputs as mean and standard deviation time measurements for each element.

EASI is a simple calculation tool which draws on the basic laws of probability (see Howell, 2008, p. 128) to combine through calculation the quantitative performance measures of the systems constituent subsystems to determine the macro-state of the PPS (Garcia, 2001, p. 252).

3.1.4 Intrusion detection

For an adversary to be caught, their penetration must be detected (Walker, 1988, p.19). Detection is the second element of defence in depth (Smith, 2003, p. 8) and the first required function of a security system (SAND report, 2002, p. 39). In discussing and achieving detection Underwood (1984, p. 137) refers to the geometry of detection stating an adversary can be detected when they cross a line (linear protection), when they enter a space (volumetric protection) and when they contact an object (point protection), and that this is employed from the perimeter inwards. In addition, once a sensor has activated the detection system must then transmit this signal notification to a location where it can be displayed with meaning to generate an appropriate facility response (Garcia, 2006, p. 14). As such, detection not only includes sensor activations but also alarm assessment, alarm communication and display, and entry control as subsystems synthesised together. The detection subsystem of a PPS therefore includes exterior and interior intrusion sensors, alarm assessment and alarm communication (Garcia, 2006, pp. 13-14).

In evaluating the detection function of a PPS, conforming to systems principles (Barton & Haslet, 2007, p. 44; Ritchey, 1991, p.1) the detection constituents are initially broken

down for analysis, then the constituents are combined through a process of synthesis to form a coherent whole in order to verify it's operating according to purpose.

3.1.4.1 Detection

According to Armstrong and Peile (2005, p. 34) for intruder detection purposes each application requires a sensor, irrelevant of its technology, to perform a particular function. For the detection system its quantitative performance function is calculated as a product, where Garcia (2001, p. 64) explains that for an ideal sensor the probability that it would detect an unauthorised intrusion would be 1.0 (100%). For example, according to Armstrong and Peile (2005, p. 35) the probability of detection is calculated from the result of three trials in a controlled environment.

In discussing the key performance indicators of the detection subsystem Garcia (2001, p. 56) states that the probability that an individual sensor will sense unauthorised activity is its probability of sensing (Ps). This view is supported by Adams, Snell, Green and Pritchard (2005, p. 2) who denote this as $P_{(sensing)}$ which is the product of:

- P_F= the probability that the sensor is functioning at the time of the attack (measured between 0.0 and 1.0);
- P_R = the reliability of the sensor itself at the time of the attack (measured between 0.0 and 1.0); and
- P_S = probability that the sensor generates an alarm-that is, senses an intrusion (measured between 0.0 and 1.0).

Drawing on the multiplicative law of probability (see Howell, 2008, p. 129), this is summarized by the equation:

$$P_{(sensing)} = P_F \times P_R \times P_S \quad (2)$$

This equation argues that the probability of sensing is the accomplishment of many phenomena. As such, drawing on the writings of Garcia (2001, pp. 63-64) the probability of detection is represented by the equation:

$$Pd = P_{(sensing)} \text{ coupled with } C_L \quad (3)$$

The P_D is measured between 0.0 and 1.0, and C_L = a confidence level, where confidence levels can vary, generally with the number of trials. Usually CL levels are equal to values ranging between .90 or 90%, .95 or 95%, or .99 or 99%. In addition, EASI uses the input $P_{(Detection)}$ as its probability of detection inputs for detection element

performance indicators along an adversary's path. EASI also uses location parameters of delay for calculating $P_{(Detection)}$ where EASI assigns detection relative to delay along an adversary's path to more accurately model system effectiveness. For example, an entry of B in the location column is added where delay occurs before detection, an entry of M is added for delay between the before and end of detection (middle) and an E is entered where delay falls after detection (Garcia, 2001, pp. 256-260).

In establishing a measure of detection towards obtaining an overall effectiveness measure for a PPS Adams, Snell, Green and Pritchard (2005) consider slightly smaller factors into some of their component terms than Garcia's (2001; 2006), however, congruous with the basic laws of probability the general construct used in EASI is the same. As such, for this study, an individual sensors performance measure will be denoted by Pd, where Pd represents the EASI input of $P_{(Detection)}$, through the equation: Pd = P_S coupled with C_L

(4)

Where:

- P_S = probability of sensing unauthorised activity (measured between 0.0 and 1.0);
- C_L = the product confidence level (measured between 0.0 and 1.0) including Adams et al, (2005, p. 2) P_F (measured between 0.0 and 1.0) × P_R (measured between 0.0 and 1.0).

Accordant with the basic laws of probability and the premises of systems theory (see Howell, 2008, p. 128 and Churchman, 1968, p. 42) theoretically this is summarised as: Pd = P_S coupled with C_L for each detection sensor along an adversary's path. However, the EASI performance measure of intrusion detection along an adversary path is calculated as the probability of non-detection which is the complement of P_D. That is, consistent with the additive law of probability (mutually exclusive events) non-detection is the mathematical complement of Pd. This measure means the systems probability of non-detection along an adversary's path is a combined measure of between 0.0 and 1.0 as product of probability. For example, along an adversary's path there may be three (3) intrusion technologies, the theoretical Pd along this path = Pd for S_1 × P_D for S_2 × P_D for S_3, that is, 0.95 × 0.95 × 0.95 = P_D = 0.85. However, to account for an adversary getting to the next layer along their path EASI draws on the probability of non-detection (Garcia, 2001; 2006) with a variation for where the sensor is located relative to delay measures (Garcia, 2001, pp. 256-260). Thus, in this example, this

would be S_1.05 x .S_2 .05 x .S_3 .05, or .000125, then after multiplying the probabilities of non-detection, the final product is subtracted from 1 to give the Pd: 1 - .000125 provides a Pd of .99.

In considering the efficacy of detection constituents, Ball (2007, p. 11) considers that for detection technologies, their probabilities of detection may vary due to factors beyond the control of the systems designer. Therefore, as an alternative for a commissioned system, a detection rate can be utilized towards establishing the detection systems key performance indicators. This view is based on the work of Armstrong and Peile (2005, p. 35) who argue that Pd is not a real probability of detection. As a sensor with a P_D of .5 (50%) can deliver three successful trials in a row. Therefore, for a commissioned system, true probability of detection is a product of an actual detection rate (walking, running, crawling, jumping climbing etc), where this product is calculated as:

$$\frac{Number\ of\ true\ alarm\ events\ detected\ \times 100}{Total\ number\ of\ true\ alarm\ events} \quad (5)$$

3.1.5 Alarm communication (transmission) and display

Alarm communication and display (AC&D) as a subsystem within a PPS transports alarm and video information to a human operator for assessment purposes (Garcia, 2006, p. 17). As such, in line with the systems approach, the EASI performance measure for this constituent sub-system is also a calculated as a product, that is, the probability that an alarm indication will be successfully transmitted to an evaluation or assessment point, referred to as probability of transmission (P_T) measured as a product between 0.0 and 1.0 (Garcia, 2001, p. 253).

3.1.6 Intruder assessment

In discussing an intruder assessment key performance indicators Garcia (2006, p. 15) explains that there is no detection without assessment, therefore once an alarm has been generated it must be assessed. Therefore the key performance indicator for the assessment sub-system must include a consideration of human factors, adversary tactics and technology aspects of this sub-system. Alarm assessment requires direct observation of an alarm source by people, or immediate capture of an image of a sensor detection zone at the precise time of an alarm event (Garcia, 2006, p. 15).

Contemporary assessment systems use fixed video cameras focused on a specific field of view for designated detection zones to automatically capture images of alarm zone at the precise time the alarm was generated and display these images on a screen for assessment by a person to determine the alarm cause (Garcia, 2006, p. 16). This approach requires effective processing of the sensor detection where the alarm computer processes the alarm appropriately, effective display so that the relevant information can be understood (clear) by a human operator through an appropriate interface, and an operator makes the correct assessment of the alarm source (Adams, et al, 2005, pp. 2-3).

Congruous with systems theory, the assessment subsystems combined process provides the performance measure of probability of accurate assessment (P_A). This probability is the combined effects of video image quality (resolution), speed of capture for images, proper installation and integration of detection sensor zones with appropriate camera fields of view coverage (Garcia, 2006, p. 16). According to Garcia (2006, p. 149) in practice, the probability of assessment (P_A) as a quantitative probability is expressed using three (3) levels of numerical assessment; 0.25, 0.5 and 0.95.

3.1.7 Detection sub-system

Accordant with the premises of systems theory and the requirement of synthesis to follow analysis (Barton & Haslet, 2007, p. 44; Ritchey, 1991, p.1), conforming with the basic laws of probability the Estimated Adversary Sequential Interruption (EASI) model, interrelates sensor detection, alarm transmission and probability of accurate assessment to provide a macro detection subsystem key performance measure. This subsystems performance measure is the probability of assessed detection (Pd), where the relationships are expressed by Garcia (2001, p. 253) in the equation:

$$Pd = P_S \times P_T \times P_A. \quad (6)$$

However, for this study the detection sensors key performance indicator denoted as P_D and the EASI detection constituents inputs of $P_{(Detection)}$, this study uses the equation:

$$Pd = P_D \times P_T \times P_A. \quad (7)$$

The detection systems constituent's performance measures relationships are represented by Figure 3.2, where the detection functions of sensor activation, signal transmission,

and alarm assessment are synthesised to achieve the sub-system performance measure of Pd.

Figure 3.2 Detection systems performance measure relationships.
(Adjusted from Garcia, 2001; 2006).

Figure 3.2 emphasises how analysis of the constituents precedes synthesis, and how synthesis of the detection constituents functions in a PPS interrelates the micro-state key performance indicators for the whole detection sub-system (Garcia, 2006, p. 36). These combined functions aim to initiate the security systems response time line (MIL-HDBK-1013/1, p. 75).

3.1.8 Entry control

Entry control is the provision of security controls whereby personnel, vehicles and materials are identified and screened to discriminate authorised from unauthorised personnel and vehicles, and to detect contraband or other undesired materials such as explosives (MIL-HDBK-1013/1, p. 31). The entry control sub-system must afford maximum security while minimising delay in the flow of authorised traffic (MIL-HDBK-1013/1, p. 71). The entry control subsystem contributes in a total PPS by allowing the movement of authorized personnel and material through normal access routes, and by detecting and notifying facility personnel of unauthorized movements and delaying unauthorised progression through portals. The entry control subsystem encompasses all the technologies, procedures, databases, and personnel used to monitor the movement of people and materials into and out of a facility (Garcia, 2006, p. 16).

Garcia (2006, p. 154) explains that the entry control sub-system uses probability of detection P_D as its primary measure of effectiveness. For example, the performance measures for entry control components of a PPS include throughput rates and error rates. Throughput rates are a measure of the time it takes for an authorised person or materials to successfully pass an entry or exit point. A systems error rates relates to falsely rejecting authorised access, and falsely accepting the improper acceptance of an unauthorized person. In addition, when considering the performance measures of this

sub-system a strong consideration of the security objectives is required as systems can be set to minimize false rejects or minimize false accepts, however access control systems cannot be set to minimize both types of errors simultaneously (Garcia, 2001, pp. 178-179).

Garcia (2006, p. 155) states "the false accept rate is the mathematical compliment of P_D and is equal 1- P_D". According to Garcia (2006, p. 155) this is a key measurement of sub-system performance because it represents the probability of defeat of the device. For example, facility characterization may require a high probability of detecting metal weapons. In this case, entry control technologies (contraband detectors) are incorporated as part of the detection sub-systems functions which provide a probability of detecting those materials they have been installed to detect.

3.1.9 Alarm communication

Communications are essential for facilitating an effective facility response, organizing responders, directing them to the scene, and successful interruption towards neutralization where necessary. This constituent sub-system starts with alarm reporting and ends with deployment of guard force and interruption (Garcia, 2006, p. 21). The performance measure for this constituent system is the probability of guard communication (P_C) measured between 0.0 and 1.0, and the time required for communication (Garcia, 2006, p. 39) where the time taken to communicate is included in the response time (Garcia, 2001, p. 253). According to Garcia (2001, p. 253) most effective systems operate with a P_C around 0.95 (95%). In addition, where the time to establish accurate communications increases the probability of communication also increases. For example, Figure 3.3 emphasises the relationship between guard communication time and probability of accurate communications. Figure 3.3 Variation of probability of communication with time (Garcia, 2006, p. 39).

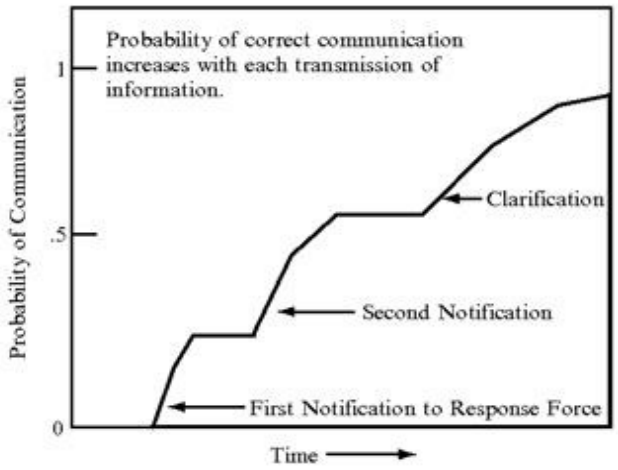


Figure 3.3 Variation of probability of communication with time (Garcia, 2006, p. 39).

3.1.10 Delay

Delay is the third element of Defence in Depth (Smith, 2003, p. 8) and the second required function of a security system (SAND report, 2002, p. 39). In establishing the delay key performance indicator for a PPS, Garcia (2006, p. 19) explains that the aim of delay within a PPS is to slow an adversary's penetration down to gain time for alarm assessment and where necessary facility response to unauthorised entry events. Ultimately strategies which establish this key performance indicator impede an adversary's progress and are accomplished through the placement of fixed, passive or active barriers (SAND report, 2002, p. 40). These barriers form the various delay microstates within a PPS, and are defined by O'Block, et al, (1991, p. 349) as "a system of devices or characteristics intended to withstand unauthorised penetration for a specified period of time". In addition, for this delay to be meaningful in a system, it must occur after detection.

3.1.10.1 ***Passive delay***

Passive barriers are defined by Fisher and Green (2003, p. 148) as either natural or structural and are the physical elements which define boundaries initially aiming to deter unauthorised access. Natural barriers comprise site specific topographical features which contribute to impeding or denying access to a protected area. In contrast, structural barriers are permanent or temporary devices constructed to impede unauthorised penetration for a specified period of time. Garcia (2001, p. 202) considers that this category of delay includes structural elements such as doors, walls, locks and fences.

3.1.10.2 *Active delay*

Active barriers are those delay resources which utilize a sensing device to initiate the dispersement of liquids, foams and other irritants to impede unauthorised penetration (Garcia, 2001, p. 202). According to Garcia (2001, p. 202) whilst passive barriers can be weak against some threat agents depending on their capabilities, dispensable barriers when implemented properly can maximise delay to an asset, and due to their characteristics can be threat independent, maintaining their intended delay regardless of adversary tactics. Within a PPS barriers are placed along a potential adversary's pathway between the attacker and specific assets requiring protection (Moseley & Coleman, 2000, p. 100).

3.1.10.3 *Measuring delay*

In discussing the effectiveness of physical barriers Moseley and Coleman (2000, p. 101) highlight that no single barrier or series of barriers is impenetrable, as with the appropriate means including time and equipment a determined attacker will eventually penetrate, or scale any number of physical barriers. The effectiveness of material barriers depends upon the amount of time they can withstand physical attack, where the longer a barrier remains intact, the greater the chances of prevention and apprehension (O'Block, Donnermeyer & Doeren, 1991, p. 349). As such, the key performance effectiveness measure for the delay element of defence in depth within a PPS is calculated as a sum, and is measured by time (Garcia, 2001, p. 2005; MIL-HDBK-1013/1, pp. 31-32; Jang, Kwak, Yoo, Kim & Ki Yoon, 2008, p. 748).

To analyse individual delay constituents true to the principles of analysis and synthesis individual barrier penetration times are defined as the time interval required for an intruder to successfully create a man-passable opening through a barrier, or pass over or around a structure, or move cross an open area. Therefore, when evaluating the physical barrier the delay time must be assessed against the time it takes an adversary to pass through, over, or under the barrier and enter their next task. For penetration evaluations, uniform to the Military Handbook of Physical Security (MIL-HDBK-1013/1, p. 32), this study defines a man passable opening as an opening of 96 square inches (0.06 sqm), which is at least 6 inches (150mm) wide or high.

In establishing barrier penetration times, analysis can be based on working time or elapsed time, where working time does not include variables such as intervals for

changing tools, changing operators, etc. A working time assessment results in a more conservative penetration time (MIL-HDBK-1013/1, pp. 29-32).

In establishing penetration time, Garcia (2001, pp. 203-204) suggests that the penetration time starts at a distance two feet in front of a barrier and ends at a point two feet beyond the barrier. For vehicle penetrations Garcia (2001, pp. 203-204) suggests that a vehicle has successfully penetrated when the ramming vehicle passes through or over a barrier and is still functioning, or a second vehicle can be driven through the breached barrier. However, this study contends that allowances must be made for a vehicle penetration of a barrier to occur and then for the attack to proceed on foot from that point. However, the distance to travel is still a remaining barrier and would be calculated as the next barrier in the attack. The time it takes to penetrate all barriers along an adversary's path is the adversary task time. Given that all barriers can be defeated in time, the most successful barrier would be the one that could increase task time (resist a threat) until appropriate action can be taken.

Accordant with the principles of analysis and synthesis, synthesis of the delay constituents occurs by calculating the cumulative delay time which is the total time an intruder is impeded from gaining unauthorised access to a secured asset. This means that an adversary's task time (ATT) is the cumulative sum of all delay measures along an adversary's path. For example, Table 3.1 shows that the penetration time for each delay constituent is measured in seconds and listed as individual tasks which must be achieved in their sequential order. Whilst each individual task may only take several seconds, Table 3.1 shows that the adversary's task time is the cumulative sum of all six sequential tasks during scenario 1, ingress route. In addition, where an adversary is required to remove an asset (scenario 2) then they must retrace their steps back through their previous penetration path to leave the facility or take an alternative exit path.

Table 3.1 Adversary estimated delay time.

Estimated Delay Time		
Scenario 1: Ingress		
Task	**Mean Time (seconds)**	**Task Description**
Y1	60 seconds	Cut through outer fence
Y2	90 seconds	Cross open ground
Y3	90 seconds	Penetrate building outer door
Y4	12 seconds	Cross room floor
Y5	40 seconds	Breach filing cabinet
Y6	15 seconds	Find and remove required file
Scenario 2: Escape		
Y7	12 seconds	Cross room floor
Y8	90 seconds	Cross over open ground
Y9	15 seconds	Climb back through outer fence
Standard total adversary task time is represented by the sum: $$\sum_{i=1}^{9} Yi \quad (8)$$ The cumulative adversary task time (ingress and egress) = 424 seconds.		

However, the EASI performance measure for the delay sub-system requires the mean and standard deviation of adversary task time, in seconds as formula inputs, represented by the formulas:

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n} \quad (9)$$

The standard deviation of adversary task time is represented by the formula:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \mu)^2}{n - 1}} \quad (10)$$

Congruous with the systems approach, barrier effectiveness relates to the barriers integration with other security subsystems (Moseley & Coleman, 2000, p. 101). For example, according to Garcia (2001, p. 204) as an adversary encounters a series of progressively more difficult barriers, it becomes increasingly difficult as it will require more and different equipment, which adds weight or people to the attack scenario, which either slows them down or makes them easier to detect. Furthermore, although the egress path would be quicker as all forced breaching would have been completed, the response force may still arrive and cut off the adversary's egress path, interrupting their escape.

3.1.11 Response

Response is the fourth element of defence in depth (Smith, 2003, p. 8) and the third required function of a security system (SAND report, 2002, p. 39). Response is a facility's means of interrupting an adversary along their attack path (Garcia, 2001, p. 223). In considering and establishing the response key performance indicator within a system Garcia (2001, p. 21) highlights two interrelated factors associated with maintaining an effective response capability, these are the performance measures for the desired response to be placed into effect and the effectiveness of that response. As a holistic key performance indicator, response is a combination of and an interrelationship between interruption and neutralization (SAND report, 2002, p. 40).

The response key performance indicator is initially established by focusing on the probability that the organisation's response personnel will interrupt an adversary along an attack path. Interruption is defined as "the response forces arrival at the correct location to stop an adversary attempting to gain a level of unauthorised access to an asset (SAND report, 2002, p. 40). In achieving successful interruption Adams, et al, (2005, p. 3) considers that for successful interruption to occur a response force must muster, gather their necessary equipment and travel to the alarm site. As such, in considering the key performance measures for response Bitzer and Hoffman (N.D., p. 5) highlight that information collected by security equipment (CCTV) must initially be reviewed and acted upon by human security personnel. For example, Cummings (1992, p. 177) points out, closed circuit television systems are only as effective as the personnel viewing them and interpreting their findings. Bitzer and Hoffman (N.D., p. 6) explain that ultimately a person viewing a scene on a monitor must interpret incoming information and make key decisions about if and what actions to should be taken. Such

a salient point is why a differentiation exists between surveillance and assessment. Therefore, the measure of effectiveness for interruption is the time from alarm notification of a penetration to the response forces arrival at the correct location to interrupt the adversary/s (SAND report, 2002, p. 40; Garcia, 2006, p. 38).

3.1.11.1 *Measuring response*

In establishing the response key performance indicator, response time is calculated as a sum, measured in time, where response time is modelled in EASI in seconds (or minutes but not both) as the time between the generation of an alarm signal by a sensing device and the confrontation of the adversary by a response force. According to Garcia (2001, p. 254) this time consists of the sum of tasks listed in Table 3.2.

Table 3.2 Facility response times inputs.

Facility Response Time Inputs		
Input 1	Alarm communication time (A_{CT})	X_1
Input 2	Alarm assessment time (A_{AT})	X_2
Input 3	Guard communication time (G_{CT})	X3
Input 4	Time required by guard force to prepare and gather equipment and start their vehicle (preparation time) (G_P)	X4
Input 5	Guard travel time (G_{TT})	X5
Input 6	Time to deploy at incident scene (G_{DP})	X6

These response force tasks represent the various micro-states of the PPS's response capability, where total response force time is calculated through the sum:

$$\sum_{i=1}^{6} Xi \qquad (11)$$

In addition, as an EASI effectiveness measure input, response time is the mean and standard deviation of the sum of the response input values, where the mean is calculated through the formula:

$$\mu = \frac{\sum_{i=1}^{n} x_i}{n} \qquad (12)$$

The standard deviation is the square root of the variance in a set of scores, summarised as:

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \mu)^2}{n - 1}}$$

(13)

The variance averages the effects of large and small deviations from the mean and can be used to characterise how much the typical score deviates from the mean (Runyon, Coleman & Pittenger, 2000, pp. 79-101). This interrelationship between response tasks is emphasised in Figure 3.4.

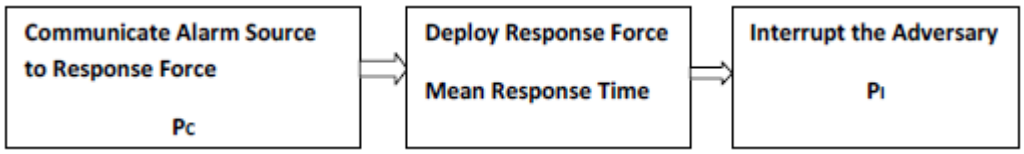


Figure 3.4 Interrelationship of response functions. Adjusted from Garcia (2006, p. 38).

3.1.12 Total system synthesis

Once initial constituent analysis has taken place to achieve element synthesis, conforming to Bertalanffy (1968, p. 56), the system can be defined mathematically; where total system synthesis is calculated through the equation:

$$P(I) = P(D1) \times P(C1) \times P\,(R/A1) + \sum_{i=2}^{n} P(R/Ai)\, P(Ci)\, P\,(Di) \prod_{j=1}^{i-1} (1 - P(Di)) \quad (14)$$

In this equation, the first part combines the detection, communication, delay and response values to produce an initial macro-state output. For example, in the first part of the equation: $P(I) = P(D_1) \times P(C_1) \times P(R/A)$. Where step 1 multiplies the probability of detection $P(\text{Detection})$ with the probability of communication $P(C)$. This process produces a combined value referred to as probability of alarm $P(A)$, represented by the equation: $P(A) = P(D) \times P(C)$.

Step 2 of the EASI equation then multiplies this probability of alarm $P(A)$ with the probability of the response force arrival prior to the end of an adversary's action

sequence, given an alarm. This probability is summarised as P(R/A), which is a combination of time remaining on the path after a sensor activates (TR) and response force arrival time (RFT). To achieve an effective interruption TR – RFT > 0, that is, the adversary's task time minus the response forces arrival time must be greater than 0 seconds.

In calculating this aspect of the EASI equation it is assumed that the variables TR and RFT are independent, and normally distributed around the mean. Therefore the random variable X = TR − RFT. P(R/A) = μx (Mean) = E (TR) − E (RFT) and $\sigma \frac{2}{x}$ (Variance) (TR) + (RFT). Where through statistical assumptions P(R/A) = P (X > 0).

Furthermore, for two or more sensors the conditional probability of response force arrival, P (R/A), for each sensor must be calculated as previously described. For example, for a path with two detection locations, summarized by the equation:

$$P(I) = P(D_1) \times P(C_1) \times P(R/A_1) + (1 - P(D_1)) \times P(D_2) \times P(C_2) \times P(R/A_2). \quad (15)$$

In addition, Step 3 of EASI considers the impact of previous detection opportunities not detecting, incorporating a joint probability of non-detection across multiple points in a layered PPS, hence the joint probability of non-detection:

$$(Di) \prod_{j=1}^{i-1}(1 - P(Di)). \quad (16)$$

As stated above, the EASI equation for calculating (synthesizing all security elements PKI's) into a whole system is:

$$P(I) = P(D1) \times P(C1) \times P(R/A1) + \sum_{i=2}^{n} P(R/Ai)\, P(Ci)\, P(Di) \prod_{j=1}^{i-1}(1 - P(Di)). \quad (17)$$

3.1.13 System effectiveness

As previously stated, response is a combination of, and an interrelationship between interruption and neutralization (SAND report, 2002, p. 40). Therefore, total systems effectiveness $P_{(effectiveness)}$ needs to consider the efficacy of a facilities response. Different threats require different levels and capabilities in response force personnel. That is, response force capability must be suitable with regards to the anticipated threat. This response includes the guard's presence as a deterrent, or delay, and use of either less lethal and lethal force options. Garcia (2001, p. 227) explains that the decision

pertaining to the required level of response is a risk management one, based on the facilities analysed risk requirements. Whilst the constituents of neutralization are beyond the scope of this thesis, this key performance indicator can be added to the EASI PPS key performance indicator (Pi) product. According to Adams, et al, (2005, p. 1) this can be summarized by the equation:

$$P_{(effectiveness)} = P_{(interruption)} \times P_{(neutralization)} \quad (18)$$

Neutralization is a product of all neutralization sub-system constituents measured between 0.0 and 1.0.

3.1.14 Relationship of physical protection system functions

The interrelationships between the functions of the PPS (Figure 3.5) commences with the element of detection, which begins on receipt of the first alarm and ends with accurate assessment. Nevertheless, as discussed, the delay function must slow down the adversary to allow the response force enough time to deploy and interject the adversary. This delay time must be more than the response force time, which is the total time required for the adversary to accomplish their desired goal. The delay times are the adversary task times, and this time must be less than the time it takes to respond to be effective. And, it must be after detection.

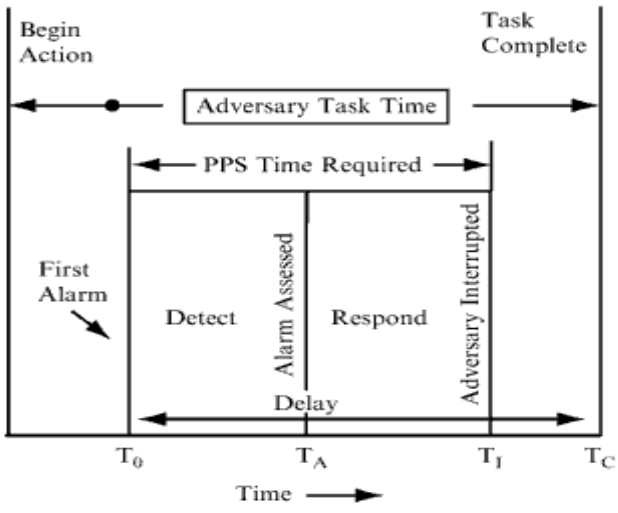


Figure 3.5 Interrelationships of physical protection system functions (Garcia, 2006, p. 39).

Figure 3.5 emphasises the interrelationships of PPS functions. For example, a sensor activates at time T_O, the time at which the alarm is assessed to be valid is labelled T_A. At this point in time, the location of the alarm must be communicated to the response force. The time at which the response force interrupts the adversary is labelled T_I, and the adversary task completion time is T_C. For a PPS to accomplish its objective of interrupting an adversary, T_I, must occur before T_C. In addition, detection should occur as early as possible and T_O, T_A and T_I should be as far to the left on the time axis as possible (Garcia, 2006, pp. 37-38). According to Adams, et al, (2005; Jang, Kwak, Yoo, Kim and Ki Yoon, 2008, p. 747) the interrelationships between the constituents, their elements, and the systems macro-state output depends on a range of complex phenomenon to successfully interrupt an adversary.

3.2 Defining a physical protection system

Accordant with Bertalanffy (1950, p. 26; 1968, p. 39; Bittel, 1978, p. 1130; Keren, 1979, p. 316; Checkland, 1981, p. 83; Jang, et al, 2008, p. 747) this study argues that a Physical Protection System is defined as a complex, open system (Figure 3.6), that is, it is not isolated from its environment. For example, uniform with Bittel (1978, p. 1131) a PPS relies on its environment for resources such as energy, financial inputs and people, etc. These inputs are put through a pre-determined process, influenced by the environment in which they exist towards producing the desired product as the systems macro-state output. From the product output, for an open system, a feed-back loop is established and maintained to ensure appropriate energy inputs sustain the system in a steady state at a distance away from equilibrium.

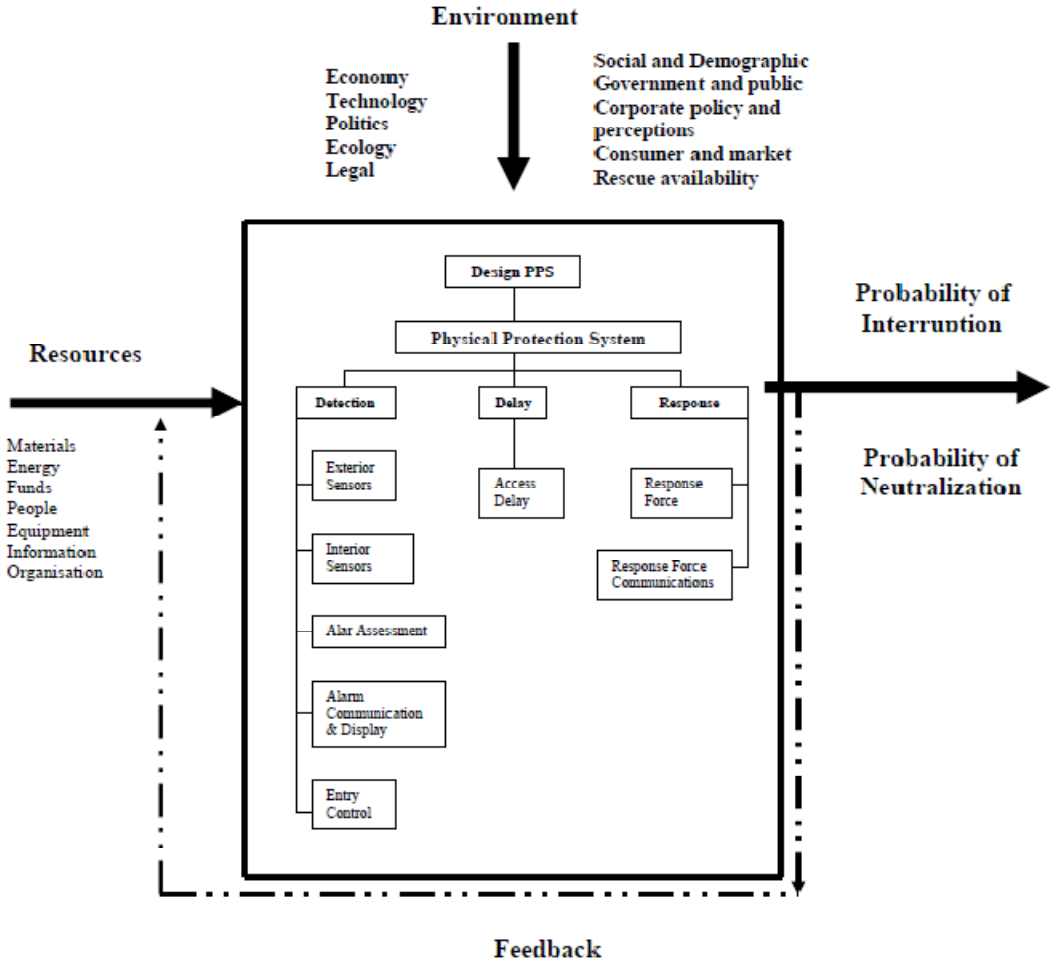


Figure 3.6 Open systems approach towards a Physical Protection System (Adjusted from Garcia, 2001, p. 4; Bittel, 1978, p. 1131).

3.3 Measuring physical protection

The application of systems thinking, that is a functional definition of a system, and the scientific process of analysis and synthesis enables this thesis's operational definition of security to be measured, where the elements of detect, delay and response combined provide a security systems macro-state measure and perceived deterrence value of the security system. That is, it is argued that the equation:

$$P(I) = P(D1) \times P(C1) \times P\ (R/A1) + \sum_{i=2}^{n} P(R/Ai)\ P(Ci)\ P\ (Di) \prod_{j=1}^{i-1}(1 - P(Di))\ (P_{(neutralization)}). \quad (19)$$

provides the means of measuring the system's stable condition. Consistent with the study's operational definition, this condition stems from the systematic process which combines people, equipment and procedures to restrict unauthorised access to either people, information or physical assets through their ability to deter, detect, delay and

respond to attacks by a malevolent human adversary/s who seek/s to gain a level of unauthorised access to a facility. In addition, within the security domains body of knowledge, anecdotally, the theory of defence in depth is summarized by the formula "3DR" to summarily represent the inclusion of all defence in depth elements into a "system". It is argued this summary is facilitated through the mathematical relationships established during the analysis and synthesis process required to obtain the systems macro-state. As such, this thesis adopts the 3DR formula as a means of representing the elements of defence in depth in summary form.

3.4 Security risk management

In discussing the implementation of Defence in Depth within a systems approach, all the elements of defence in depth are equally important and must be operated in an integrated manner. That is, none can be eliminated or compromised if an effective security system is to be achieved (MIL-HDBK-1013/1, 1993, p. 24). However, in implementing defence in depth economic judgements and pressures are continually brought to bear on security measures, where pressure is applied at the immediate field level, setting the costs of defence against the loss (Underwood, 1984, p. x). In setting a physical security benchmark, that is, determining the required level of key performance indicators across the system, the objective is to identify an integrated physical security system design that achieves a cost-effective application of security system resources (MIL-HDBK-1013/1, 1993, p. 33). Therefore in establishing a Defence in Depth system individual security measures must be justified where a protection case has been constructed (Manunta, 2007).

In establishing a Defence in Depth protection case Manunta (2007) explains that such a justification process requires managers to evaluate security strategies within a costs benefit analysis framework. Such an analysis incorporates a combination of potential harm, financial impact and relevant political concerns. Manunta's (2007) view is supported by Underwood (1984, p. x; Walker, 1988, p. 18; Cumming's, 1992, p. 2). For example, Walker (1988, p. 18) states "the law of diminishing returns applies to the security function", where according to Cumming's (1992, p. 2) the amount of time and capital spent towards risk control and management depends on the value of the product being protected. Walker (1988, pp. 18-22) adds, as the value of the asset increases so does the requirements underpinning a security systems design, where components are selected based on perceived suitability for the relevant risk environment.

In practice, to facilitate the manipulation of risk it is necessary to firstly define the sources and nature of an organisation's risk exposure. For example, for security risk management, according to Underwood (1984, p. 1) malevolent attacks against an organisation saliently stem from two offender typologies:

- Opportunists, those who may watch or notice holes in the desired level of security and are tempted by their presence;
- Deliberate criminals, those who plan an attack on a security systems highest level of capability (Underwood, 1984, p. 1).

Garcia (2001, p. 245) supports Underwood's (1984, p. 1) two type offender typology, suggesting that the adversary factor is interrelated with the design characteristics of a PPS. According to Underwood (1984, p. 3) the opportunist is the most common danger and at times difficult to manipulate as opportunist do not consider an attack based on the value of gain, but rather in-line with Manunta's (2007, p. 58) definition of security, that is, the coincidence of attacker (themselves) and the absence of suitable protection. McCrie (2004, p. 16) supports such a view, arguing that for opportunity based asset loss the security controls relationship can be expressed in the formula:

$$Asset\ loss = \frac{Opportunity}{Controls} \tag{20}$$

In protecting a site against opportunistic offenders Mosely and Coleman (2000, p. 101) suggest that true with the first element of Defence in Depth it is the deterrence value which is saliently important**.** However, in contrast to opportunists deliberate offenders plan an attack against a security system, and may expend skills, time and effort on planning their assault against the normal level of security (Underwood, 1984, p. 3-4).

Underwood's (1984) view is supported by Robinson (1999, p. 74) who states, "There are those people who, through training, extensive experience, firm dedication, and the promise of significant reward, attack when they perceive the advantage to be on their side". These individuals take the necessary time to gather intelligence, know how to avoid security measures, and when they perceive the risks to be reasonably low and the rewards reasonably assured make their approach on the system. For example, according to Underwood (1984, p. 4) it has been known that the degree of pre-planning involved

for attacks on super-risks such as bullion vaults to take several years in planning and execution.

In considering a systems approach to physical security, and ultimately security decay, it is argued that the measures of performance for the system, that is the systems output goals, must be considered accordant to the systems strategic purpose. For example, Underwood's (1984, p. 4) considerations are supported by Garcia (2001, p. 245) who explains that the adversary factor is strongly interrelated with the effectiveness measure of the PPS. That is, in applying a systems approach towards developing the objectives of Defence in Depth, determining the level of 3DR, the designer must understand the facilities operations and threat (Garcia, 2001, p. 3).

Drawing on HB 167 (2006, pp. 55-56) it is argued the PPS objectives can be determined based on the traditional security definition of threat, considered as: Threat = Intent X capability. Intent as a characteristic is considered the motivational factors which drive someone to wish to penetrate the defences of a facility. In contrast, capability considers attributes of potential aggressors including their knowledge, skills and resources. In defining a threat against a Defence in Depth system, it is argued that the capabilities of the threat must be considered based on a population sample, in relation to their capability to defeat each element of Defence in Depth within the system.

In determining this threat, HB 167 (2006, pp. 59-60) draws on the Swiss cheese model to indicate how many layers of security controls will exist within a Defence in Depth system, where under normal circumstances the holes in each slice of cheese will be covered up by subsequent layers of controls. The summation of these controls represents the effectiveness of the system in managing an attack against the system. For example, Figure 3.7 presents the Swiss cheese model from HB 167 (2006, p. 60). As such, it is argued that in defining a facilities threat, and therefore developing the objectives of the system, each functional element's resilience must be considered within a population sample.

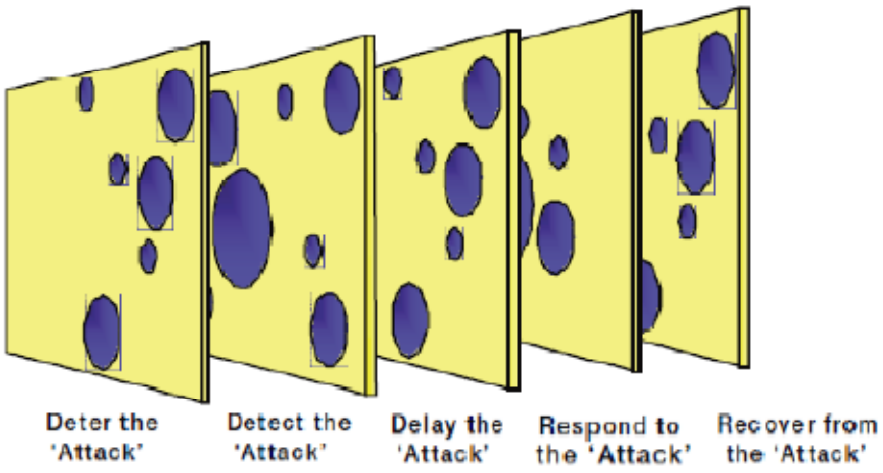


Figure 3.7 The Swiss cheese model of a layered security system (HB 167, 2006, p. 60).

3.4.1 Defined threat and the normal curve

The aim is to implement a system which as a sum can repel a defined threat. For example, according to Weiten (2002, p. A-10) virtually all data sets are characterised by some variability. Variability relates and refers to how much individual scores tend to vary or depart from the mean score of a data set. Weiten (2002, p. A-10) provides the example of golf scores, comparing a mediocre, erratic player against a mediocre, consistent player. The scores of the consistent player would display less variability than those of the erratic golfer, where Weiten (2002, p. A 10) points out, a great many traits and qualities are distributed in a manner which closely resembles a bell shaped cure, Figure 3.8 which is referred to as The Normal Distribution or Gaussian distribution (Runyon, Coleman & Pittenger, 2000, p. 119). The horizontal axis shows how far above or below the mean score is and the vertical axis shows number of cases obtaining each score. In a normal distribution, most cases fall near the centre of the distribution Figure 3.8, so that 68.26% of cases fall within plus or minus one (1) standard deviation of the mean. In addition, the score placed on The Normal Distribution can be converted to percentile scores which indicate the percentage of people who score at or below another score (Weiten, 2002, p. A-11).

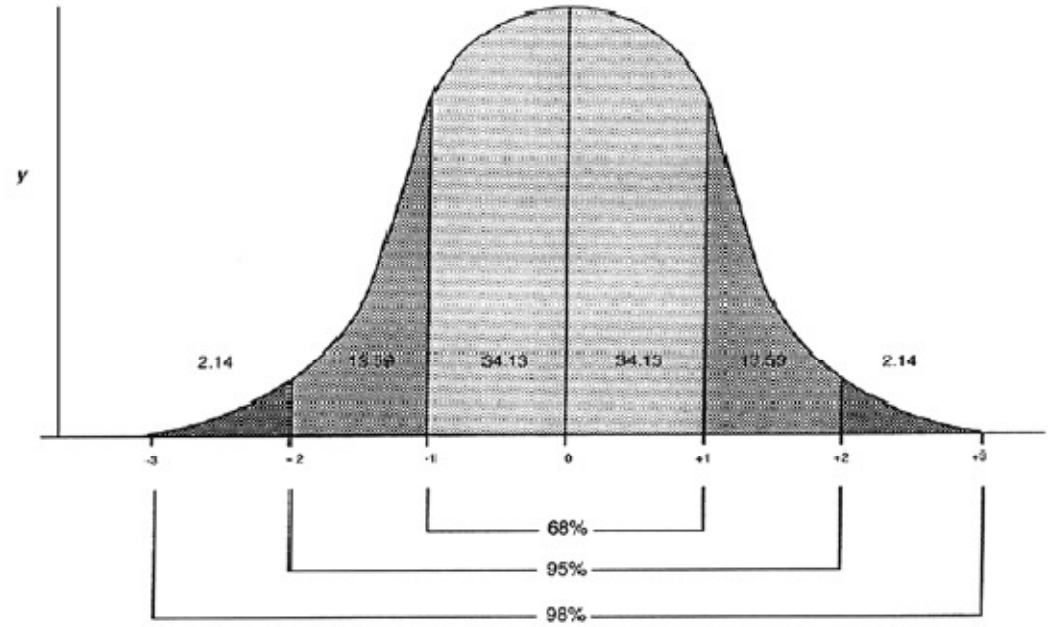


Figure 3.8 The Normal Distribution (ASCD, 2010).

According to Weiten (2002, p. A-10) the Normal Distribution provides a precise means, statistically, of measuring how people compare to each other. As such, in determining the defined threat, it is assumed that the collective skills, knowledge and resources required to defeat a Defence in Depth system (PPS) also need to be considered based on a population sample. That is, some threat agents may have the technical knowledge and skill to defeat intrusion detection systems, yet lack the skills to defeat barriers in a timely manner, or overcome response personnel. However, by population sample, others may possess the skills to easily defeat physical barriers and overcome some lower levels of response, yet do not possess the knowledge and skills to defeat technology or overpower a higher level armed response.

It is therefore argued that in defining the threat and therefore the systems objectives, a holistic appreciation is required where a threats collective capabilities are determined based on their abilities within a population sample to defeat the collective elements of Defence in Depth. For example, Figure 3.9 indicates how an adversary's capabilities to defeat various elements of Defence in Depth layers is considered within a normal distribution for each layer, where the sum of the defined threat is the sum of the threat's capabilities across all element distributions.

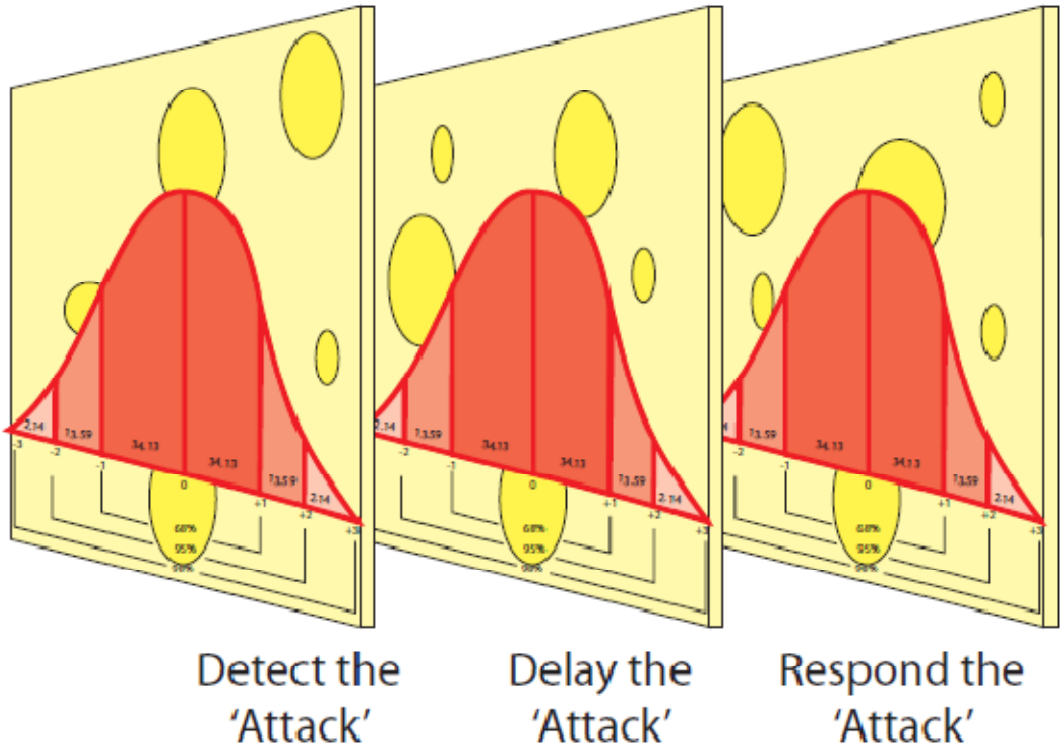


Figure 3.9 the Standard Distribution applied to the Swiss cheese model. (Adjusted from HB 167, 2006, p. 60; ASCD, 2010).

3.4.2 Defining risk

The application of security principles, techniques and hardware therefore requires that costs are balanced against the desired effectiveness of the whole system based on an organisations risk profile (Post, Kingsbury & Schachtsiek, 1991, pp. 97-99). In establishing an organisation's security risk profile, Garcia (2001, p. 272) provides a quantitative definition, defining risk through the formula:

$$Risk = Threat \times Vulnerability \times Criticality$$

.

According to Garcia (2001, p. 272) risk is score defined in mathematical terms through the equation:

$$R = P_A \times [1-(P_I)] \times C \quad (21)$$

Where;

- R= Risk
- PA = Likelihood (threat) of an adversary attack measured between: 0-1.0
- 1 = Vulnerability: the highest the effectiveness can be.
- Pi = Probability of interruption measured between: 0-1.0
- C = consequences (criticality) value measured between: 0-1.0

Garcia's (2001, p. 272) formula is a measure of PPS performance and does not include neutralization. This approach is supported by Standards Australia HB167: 2006, which establishes the security risk management context as a combination of threat assessment, vulnerability assessment and criticality assessment (Standards Australia, 2006, p. 14). Where according to HB 167 (2006, p. 62) vulnerability can be based on an assessment of the effectiveness of the controls in managing the threat's interaction with the critical asset.

In discussing the resource requirements and output product of an open system, Olzak (2006, p. 1) suggests "which security layers to implement and to what extent is a risk management decision". Therefore, the total cost of the security system is determined within the theory of defence in depth by the degree of security control required to achieve the amount of time delay judged necessary after detection, to facilitate an appropriate response in relation to the risk of the asset being protected (Post, Kingsbury & Schachtsiek, 1991, p. 89; Garcia, 2001, p. 272). It is argued that these controls must be implemented to achieve a steady state risk reduction capability. For example, according to McClure (1997, p. 4) effective security refers to a state where, the need for security has been established, its role defined and the appropriate amount of protection achieved. McClure (1997, p. 4) explains that an effective security state exists when the level of risk exposure is reduced, through various means, to a level that is acceptable to the organisation.

In addition, Spencer (1998, p. 2) suggests the costs/benefits associated with the implementation of specific measures can be measured against the reduction in vulnerability. As the level of vulnerability decreases, a decision may be made where the system has reached the point of "acceptable risk" below which decision makers are willing to accept the remaining vulnerability as additional system measures are not justifiable. The sum of this literature is supported by McCrie (2004, p. 16) who explains that either vulnerability or negligence (opportunity) eventually result in a security loss event.

3.4.3 Establishing a steady state physical protection system

In applying the systems literature to physical security, such an approach includes the component resources of people, techniques, procedures, design features, materials and

educational programs integrated to construct a holistic security program (Post, Kingsbury & Schachtsiek, 1991, p. 23). Based on the available literature, it is therefore argued that in line with the theory of defence in depth and the justification of security measures within a cost benefit frame work, the situation can be represented in mathematical terms, where from a functional approach to security the relationship can be summarized as:

$$Security = \frac{\sum 3DR}{Risk\,[Threat \times Vulnerability \times Criticality]} \quad (22)$$

That is, for an effective state of security to be achieved, a security system must demonstrate effectiveness in response to a facilities analysed risk level based on its defined threat (Garcia, 2006, p. 30), which must consider Underwood's (1984, p. 1) two offender typology. The defined threat can be more than one level or group. As such, system effectiveness varies with a threat's capability. Therefore a system would perform differently against low, medium and high threats agents.

A PPS functions by combining people and equipment into an integrated system of subsystems along an adversary path (Garcia, 2001, p. 61). An adversary path is an ordered series of activities against a facility which if completed results in successful theft, sabotage or other malevolent outcome (Garcia, 2001, p. 242). The objective of a PPS is to achieve balanced protection defined by Garcia (2001, p. 60) as, 'a system when, regardless of the adversary path chosen, effective elements will be encountered, where, the minimum time to penetrate each of the barriers would be equal, and the minimum probability of detecting penetration of each of these barriers should be equal". There are potentially many adversary paths within a facility. The critical path is the one with the lowest probability of interruption, therefore the critical path characterises the effectiveness of the overall protection system in detecting, delaying and interrupting an adversary (Garcia, 2001, p. 247).

In addition, according to Underwood (1984, p. 3) the daily levels of security inevitably rise and fall in operation. Based on such real world fluctuations, it is argued that consistent with Martin's (2000, p. 210) percentage of fluctuations in relation to a steady state, a zone of tolerance, that is, a preset threshold level to characterise a steady state, should be established within the system towards ensuring the sequential strategy continually communicates to offenders that $EU_{offence} > EU_{legal} + U_{taste}$.

The theory of Defence in Depth, which this study argues needs to be implemented within an open systems frame, delivers; effective risk based decisions, enhanced operational effectiveness, and a reduction in overall risks and costs (Trusted Information Sharing Network, 2008, p. 2). According to Garcia (2001, p. 277) the use of the risk equation (Garcia, 2001, p. 272) and Pi (systems performance measure) will enable effective cost-benefit decisions to be made towards implementing security controls which reduce an organisations risk to an acceptable level. For example, Figure 3.10 highlights from an open systems frame the level of desired security implemented based on the risk equation and PPS system performance measure. Such parameters can be achieved whilst being cognizant of maintaining a system's deterrent value during daily fluctuations. Based on this approach, uniform with the objectives of other open systems (Honkasalo, 1998, p. 135) the overall aim of a PPS is to reach a steady state where the flow of energy is constant and the increase of entropy is at a minimum. This steady state condition according to Roos (1997, p. 6) implies an exchange of either matter or energy within the environment, such that there is a balance of inputs, outputs and internal processes.

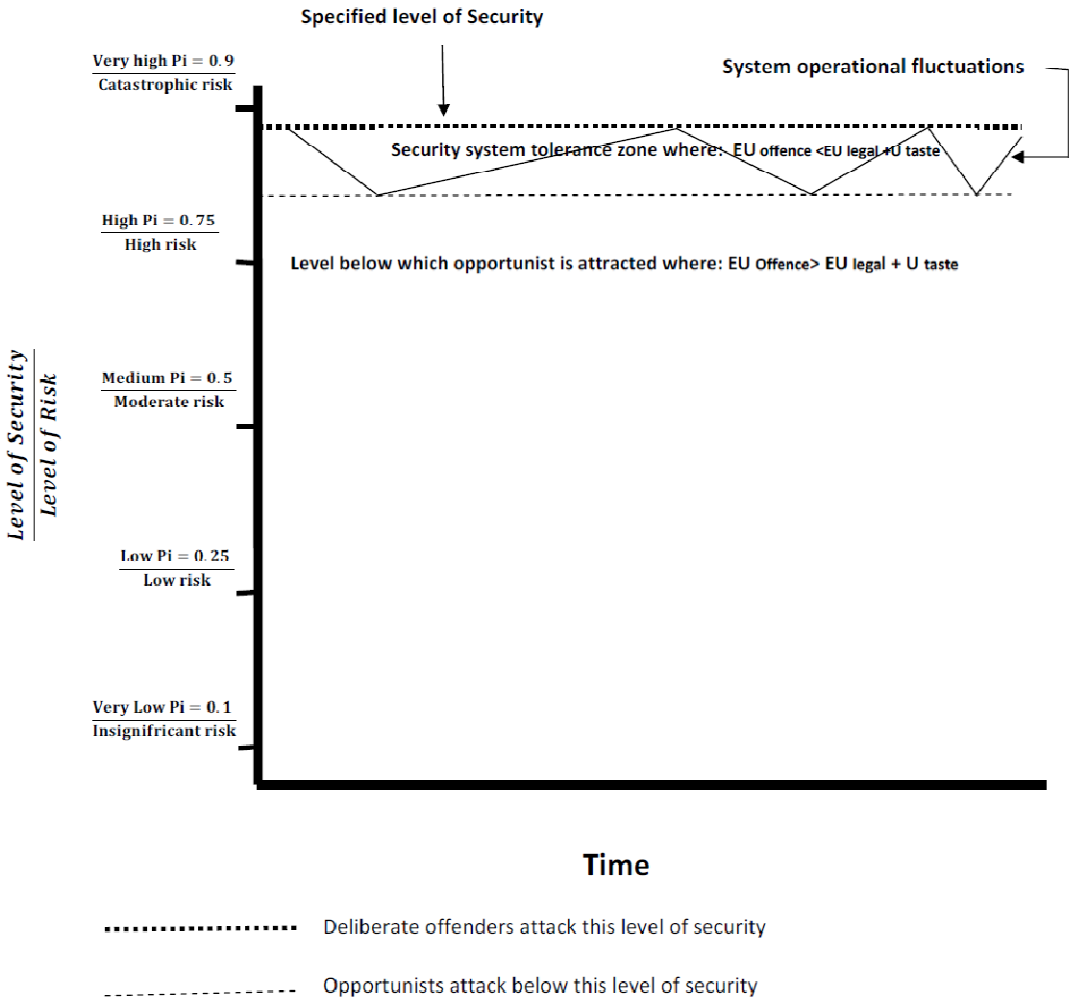


Figure 3.10: implemented security levels diagram, adopted from the literature of Underwood (1984; Martin, 2000, p. 210; Garcia, 2001, 2006; Pidwirny, 2006; Standards Australia HB167 Security Risk Management, 2006).

In addition, there are varying states of the facility, which affect the security system where accordant with the open systems characteristic of equifinality, for a PPS this desired level of security (steady state) can be reached from different conditions depending on the changing system parameters. That is, consistent with Figure 2.5 (see Section 2.2.6.2) a desired Pi can be reached via a symmetric approach to implementing desired security controls, an initial overshoot where the levels of security are initially above that which is required for the assessed risk state, or a fake start where the desired level of security does not meet the required levels of security and therefore further controls are added to the system to achieve the desired level steady state condition of the PPS.

3.5 Conclusion

The chapter presented the second stage of phase one of the study; establishing an open systems benchmark within a physical security context. This chapter established a documentary benchmark for considering an open systems approach to Physical Protection Systems (PPS). For example, Bertalanffy (1950, p. 139) states that "General Systems Theory is a logico-mathematical discipline, which is in itself formal, but applicable to all sciences concerned with systems", where in-line with the available literature, the study purports that a Physical Protection System (PPS) is a complex open system, and subjected to the laws and principles of science which govern systems of all types.

Central to the establishment of an open systems approach to security risk management within a physical security context is the design, implementation and management of Physical Protection System (PPS). A PPS aims to provide a level of desired risk reduction commensurate to a facility's defined threat, where measures exist to ascertain such a level of efficacy. Within this open systems frame the processes of analysis and synthesis within and between the various PPS elements and their constituents' indicates, through mathematics, that all constituents within a PPS have a direct relationship with the systems macro-state. This macro-state is based on a desired level of security risk reduction, where a desired level of interruption is achieved through incorporating various measures of constituents through their ability to add to the systems capability to detect, delay and respond to unauthorised access events. In this chapter it was argued that through Defence in Depth's sequential combination the systems "deterrence" set would be established. The benefit of such a quantitative approach is the establishment of a security benchmark for considering security decay within an open systems frame.

CHAPTER 4

PHYSICAL PROTECTION SYSTEM DECAY

4.0 Introduction

This chapter presents the third stage of phase one of the study; establishing an open systems framed benchmark for considering physical security decay. This chapter brings forward the writings from chapters two and three to establish a benchmark for considering physical security system decay. Section 4.1 provides a discussion on physical system degradation, including the laws of thermodynamics. Specifically how the orderly relationships within Defence in Depth elements and their constituents, established utilizing systems thinking to achieve an effective macro-state (Pi), can be impeded by the concept of entropy.

Section 4.2 presents a discussion on entropy and its negative effects on physical system effectiveness. This discussion highlights how entropy relates to every single physical activity that human kind engages in, and specifically how it relates to the degradation of Physical Protection Systems (PPS). Section 4.3 presents the theory of entropic security decay, the sensitivity within a Physical Protection System (PPS) and the effects of entropic security decay. Section 4.4 presents the measurement of security decay. Section 4.5 provides a discussion on security decay and risk management, and the effects of decay on critical path. Section 4.6 presents a discussion on avoiding and countering entropic security decay. Section 4.7 concludes the chapter.

4.1 Physical system degradation

In establishing a benchmark for system degradation/decay, this study draws on the writings of Lovey and Manohar (2007, p. 99) and Styer (2000, p. 1) who argue that all physical systems, if left to themselves, tend to maximise their entropy, concordant with the laws of thermodynamics. Entropy is discussed within the system literature and is a concept derived from a metric defined as a measure of disorder in a system and a process characterised with: decay, disintegration, running down, becoming disordered (Bohm & Peat, 2000, p. 137; Herman, 1999, p. 86; Bertalanffy, 1968, p. 42), and in all irreversible processes, entropy must increase (Bertalanffy, 1968, pp. 41-42). For a system, as entropy increases (its entropy level) capability decreases, based on the

argument that systems rely on order and cohesion. Entropy is the combination of the Greek word “tropos”, which means transformation or evolution, and “energy”. The term entropy was first used in the middle of the eighteenth century by Rudolf Clausius and is a quantity to measure the level of evolution of a physical system, but can be used to measure the ‘disorder” of a system (Vannini, 2005, p. 94).

The literature embodying systems thinking (GST) discusses the concept of entropy and its negative effects on system sustainability (Bertalanffy, 1950, p. 23; 1968, p. 39; Keren, 1979, p. 312; Checkland, 1981, p. 83; Styer, 2000, p. 1; Midgley, 2003, p. 182; Pidwirny, 2006; Morales- Matamoros, Tejeida-Padilla & Badillo-Pina, 2010, pp. 75-76), where according to Callister (1997, p. 482) entropy increases with increasing disorder. The principle of entropy introduces into physics the idea of irreversible processes, such as that energy always moves from a state of high potential to a state of low potential, tending to a state of equilibrium (Vannini, 2005, p. 93).

In discussing the concept of irreversibility Price (2003, p. 3) explains that as a concept, irreversibility relates to the thermodynamic arrow, or, arrow of time. The arrow is concerned with the seemingly irreversibility of many common physical phenomenon. Physical processes at the microscopic level are believed to be time symmetric. This approach means that the theoretical statements that describe them remain true if the direction of time is reversed; however, when physical processes at the macroscopic level are described this is not the case. The thermodynamic arrow of time considers that in an isolated system, entropy increases with time. As entropy can be considered a measure of microscopic disorder, according to the second law of thermodynamics time is asymmetrical, as it relates to the amount of order in an isolated system. As time increases, a system statistically moves towards a state of disorder. That is, entropy evolves in only one direction, towards death and the elimination of any form of organization and structure (Vannini, 2005, p. 94).

However, the concept of entropy is tremendously difficult to grasp and is a concept previously discussed within the field of physics (Styer, 2000, p. 1; Lovey & Manohar, 2007, p. 99). In applying the concept of entropy Rifkin (1982, p. 8) explains that the laws of thermodynamics provide the overarching scientific frame for the unfolding of all physical activity in the world. Rifkin’s (1982, p. 8) view is supported by Soddy (cited in Rifkin, 1982, p. 8) who states, “every single physical activity that humankind

engages in is totally subject to the iron clad imperatives expressed in the first and second laws of thermodynamics, where according to Rifkin (1982, p. 6) the entropy law is the second law of thermodynamics.

4.1.1 The laws of thermodynamics

The science of thermodynamics provides a general framework of ideas which facilitates the understanding of particular systems (Adkins, 1975, p. 2) and was developed as a means of describing physical systems during the nineteenth century. Thermodynamics is primarily concerned with the interchange of energy and its expression as either work or heat (Roos, 1997, p. 5). A thermodynamic system is that portion of the universe which is selected for investigation (Atkins, 1986, p. 2). For example, according to Oster and Desoer (1971, p. 221) an electrical network is a non-equilibrium thermodynamic system.

The science of thermodynamics sets out to describe and correlate the directly observable properties of substances; the volume of gas, the expansion of a wire; the polarization of a dialectic wire. These are all macroscopic quantities, properties of materials in bulk. The laws of thermodynamics enable people to interrelate the macroscopic quantities without making microscopic assumptions. The avoidance of commitment to any particular microscopic interpretations means thermodynamics is not limited to particular applications. However, it is possible to associate particular macroscopic behaviour with certain general kinds of microscopic change (Atkins, 1986, p. 2).

4.1.2 The first law of thermodynamics

The first law of thermodynamics is a conservation law, the law of conservation of energy. This law states “all matter and energy in the universe is constant, it cannot be created or destroyed, only transformed from one state to another, where only its form can be changed but never its essence” (Landsberg, 1956, pp. 365-374; Rifkin, 1982, p. 7; p. 78; Dillon, 1983, p. 65), where according to Roos (1997, p. 5) work is done in the process, therefore work, heat and energy are convertible.

In discussing thermodynamics Midgley (2003, p. 171) explains that matter is anything which has mass (M) and occupies space. Energy (E) is defined in physics as the ability to do work. Matter may have (a) kinetic energy, when it is moving and exerts force on other matter, (b) potential energy, because of its position in a gravitational field, or (c) rest-mass energy which is the energy that would be released if mass were converted into

energy. The relation between mass and energy is expressed by the equation: E = mc^2, where c is the speed of light, m is the mass and e is the energy (Vannini, 2005, p. 96). Mass and energy are equivalent. One can be converted into the other in accordance with the relation that rest-mass energy is equal to the mass times the square of the velocity of light. This is the principle of the first law of thermodynamics (Midgley, 2003, p. 171).

4.1.3 The second law of thermodynamics

According to Midgley (2003, p. 173), Gibbs (1902) formulated the second law of thermodynamics, the law of degradation of energy. This second law (the entropy law) states "matter and energy can only be changed in one direction, that is, from an available to unavailable, or from an ordered to disordered state (Landsberg, 1956, pp. 374-385; Rifkin, 1982, p. 6; p. 78). That is, when transforming energy part is lost to the environment. When energy lost to the environment is distributed in a uniform way, a state of equilibrium is reached where it is no longer possible to transform energy into work. Entropy measures how close a system is to its state of equilibrium, and is a measure of the quantity of energy which is lost to the environment (Vannini, 2005, p. 93). As such, Herman (1999, p. 86) broadly defines entropy as the steady degradation of a system—where entropy increases within a system, capability decreases—based on the argument that systems rely on order and cohesion.

4.1.4 The third law of thermodynamics

The third law of thermodynamics is derived from the second law and is the law of disorder. This law states "within an isolated system entropy cannot diminish. That is, the dissipation of energy is an irreversible process, since dissipated energy cannot be recaptured and used again, and that the entropy of an isolated system can only increase until it reaches a state of equilibrium since isolated systems cannot receive information or energy from outside" (Vannini, 2005, p. 93). According to Bertalanffy (1977 cited in Vannini, 2005, p. 98) information is any element which reduces entropy, suggesting information can take the form of a project, an organisation, a structure, or generally a system, and was referred to as neg-entropy; negative entropy.

4.2 Entropy

Entropy as a concept is a state function of a system (Roos, 1997, p. 5). A state is a description of the system in terms of its properties at any instant time. When a system changes from one state to another the difference in properties depend solely on the states and not on the manner, or pathway by which the change occurred. According to

Rifkin (1982, p. 6) in essence, the second law says that everything in the entire universe begins with structure and value and is irrevocably moving in the direction of random chaos and waste. For example, the laws of physics state disorder must always increase, as in classical physics the laws of nature are perfectly time-reversible, where all of the processes people see occurring do so in one direction only, as reversal would go against the laws of statistical probabilities (the second law of thermodynamics) (Felder, 2001, p. 1). That is, total entropy of the universe can never decrease, as according to Lovey and Manohar (2007, p. 99) this law states that transformations of one form of energy into another in natural process is accompanied by a loss because of increasing entropy. Entropy is therefore a measure of the extent to which available energy in any subsystem of the universe is transformed into an unavailable form.

Whilst the second law of thermodynamics states, "all energy in a system moves from an available to unavailable or from an ordered to a disordered state", the minimum entropy state is one where order and concentration are highest and available energy is at its maximum (Rifkin, 1982, pp. 42-78). As such, an entropy increase results in a decrease in "available" energy (Rifkin, 1982, p. 35). Whilst entropy in closed systems is always positive, as closed systems rely on disordered states, where order is continually destroyed, in open systems the production of entropy is negative (Bertalanffy, 1968, p. 41).

In discussing the positive and negative aspects of entropy Bertalanffy (1968, p. 39) explains that entropy in a closed system is considered a measure or probability, and therefore a closed system tends towards a state of most probable distributions (Bertalanffy, 1968, p. 39). For example, according to Bertalanffy (1968, p. 39) when considering temperature as an example of a system's macro-state, the most probable distribution of molecules having different velocities, is a state of complete disorder. That is, it is highly improbable to have all the fast molecules, high in temperature on the right side of a room, and all of the slow moving molecules (low in temperature) on the left. So the tendency is towards maximum entropy, where the most probable distribution is the tendency towards maximum disorder.

4.2.1 Microscopic/macroscopic relationship

In discussing entropy further, Felder (1999, p. 2) explains that it is a relationship between macroscopic and microscopic quantities within a system, a view supported by Bohm and Peat (2000, p. 137) who discuss the role and influence of constituents within a system utilizing temperature as an example. According to Bohm and Peat (2000, p. 137) the temperature of a system defines a macro state, whereas the kinetic energy of each molecule in the system defines a microstate. In this example the macro state variable is recognized as an expression of the average of the microstate variables, an average of kinetic energy for the system. Based on this example, if the molecules of a gas (microstate) move faster, they have more kinetic energy resulting in the temperature (macro state) rising (having direct affect on the macro state) (Bohm & Peat, 2000, p. 137).

According to Felder (1999, p. 2) the micro state of a system consists of a complete description of the state of all constituent element of the system, whereas the macro state consists of a description of a few macroscopically measurable quantities. As such, for any macro state of the system there are possibly many different microstates. Therefore the entropy of a system in a particular macro state can be defined as the number of possible microstates that the system might be in.

4.2.2 System effectiveness

The science of thermodynamics enables the quantity known as entropy to be measured objectively in terms of the amount of heat and work that is associated with a system, as left to itself a physical system tends to maximise its entropy accordant with the laws of thermodynamics (Lovey & Manohar, 2007, p. 99; Styer, 2000, p. 1). For example, Bohm and Peat (2000, pp. 138-139) explain the concept of entropy in an isolated system of interacting particles. Each particle within such a system acts as a contingency for all others in a way where the overall motion tends to be chaotic. When such systems are left to themselves they move towards what is referred to as thermal equilibrium, a condition resulting in zero net flow of heat or energy within the system and regular suborders vanishing almost entirely. In this state of equilibrium, the entropy of the system is at its maximum.

Maximum entropy is associated with a systems inability to carry out work, transfer useful energy from one region to another or in any other way, and generate global

orders of activity. Motz and Weaver (1989, p. 168) suggests that all systems strive towards disorder, which when achieved the system will be in a state of equilibrium. Complete equilibrium in a system results in the death of the system. According to Coole and Brooks (2009, p. 22), for a system the situation can be represented by the formula:

$$System\ effectiveness\ = \frac{capability}{entropy} \tag{23}$$

(Coole & Brooks, 2009, p. 22).

4.2.3 Entropy within an open systems frame

According to Midgley (2003, p. 39) traditionally physics only dealt with closed systems, as such, physicist argued the laws of thermodynamics only apply to closed systems, in particular the second law (Bertalanffy, 1968, p. 39). For example, as a closed system moves towards equilibrium energy is converted to work, but as it approaches equilibrium, the available energy decreases. However, Roos (1997, p. 13) explains that there are systems which by their nature are not closed. In addition, to maximise work output from a system a steady state is preferable, where the system is maintained in pseudo-equilibrium by new inputs and the removal of outputs.

The expansion of physics to include open systems frames has enabled the generalization of the second law of thermodynamics to include open systems. In open systems there exists the production of entropy due to irreversible processes, which is also negative. However, open systems maintain themselves in a steady state which can therefore avoid the increase in entropy, and may even develop towards states of increased order and organization (Midgley, 2003, pp. 40-41). In an open system, the system can be maintained in the pseudo-equilibrium state provided inputs approximately match outputs. Energy is required to prevent increase in entropy to prevent the system running down (Roos, 1997).

4.2.3.1 Prigogine's open systems approach to entropy

The earlier extension and generalization of thermodynamical theory was the work of Prigogine (Bertalanffy, 1950, p. 26). Prigogine (1987) proposed a way of defining complex systems, arguing that a wide class of systems existed which he referred to as dissipative systems, which tended to loos energy over time. This loss energy according

to Prigogine (1987, p. 98) cannot be regained, as the processes that dissipative systems went through were irreversible in time-they were path dependent. Prigogine (1987, p. 98) argued that any system which tended to loos energy over time, fairly quickly reached thermodynamic equilibrium. As such, complex dissipative systems must make up for their loss of energy by importing new energy from their environment and exporting accumulated entropy.

Prigogine focused his attention on irreversible thermodynamics and particularly on specific phenomenon which are far from equilibrium (Dillon, 1983, p. 119). Prigogine was able to show mathematically and through experiment that in near equilibrium conditions a natural physical system acts to minimise entropy production (Meara, 2005, p. 9). According to Prigogine (1950, p. 99) steady states in open systems are 1) not defined by maximum entropy, but by the approach of minimum entropy production; 2) entropy may decrease in such systems; 3) the steady states with minimum entropy production are , in general stable. Therefore, if one of the system variables is altered, the system manifests changes in the opposite direction.

According to Prigogine (1947 cited in Bertalanffy, 1950, p. 26; 1968, p. 144), the total change of entropy in an open system can be written as: $dS = d_e\mathrm{S} + d_i\mathrm{S}$. Where $d_e\mathrm{S}$ denotes the change of entropy by import, $d_i\mathrm{S}$ denotes the production of entropy due to irreversible processes in the system. The term $d_i\mathrm{S}$ is always positive, according to the second law of thermodynamics however, $d_e\mathrm{S}$ may be negative, as well as positive. Therefore the total change in entropy in an open system can be negative as well as positive.

Nevertheless, according to Midgley (2003, p. xxviii) Prigogine's theory suggests that while in most of the universe there is movement towards entropy (equilibrium, or the even distribution of energy) there are islands of structures (negentropic systems) that concentrate and maintain their energy levels for periods of time and exists in states far from equilibrium. Prigogine's (1950; 1987) theory of dissipative structures focuses on the importance of bifurcations. Bifurcation points are places at which the solution to various equations may, at a particular point, offer more than one possible solution (Dillon, 1983, p. 119).

Prigogine's (1950; 1987) view is the idea that systems reach points of relative instability where they may take alternative directions, and even the tiniest influences may have a major effect on the future direction of the system (Midgley, 2003, p. xxviii). In the Prigogine analysis bifurcation points are very important, if an equation was describing some physical condition of the system, at the bifurcation point two options are presented. If the system proceeds along option A, its structure and functions may be quite different than if B had been selected. It is considered that in a complicated system there might well be whole series of Bifurcation points (Dillon, 1983, p. 119). Prigogine's (1950; 1987) theory argues dissipative structures are able to circumvent the second law by being open, or energy-processing in character. They feed throughputs of energy to sustain order or negative entropy and can remain in a sustained condition of disequilibrium (Morales-Matamoros, Tejeida-Padilla & Badillo-Pina, 2010, pp. 75-76).

Throughout history technologies and institutions have served as transformers of energy; facilitating the flow of energy from the environment through to human's social system (Rifkin, 1982, p. 94). The various technologies and institutions which humans have developed are a reflection of the kinds of energy environments which they have lived in. This reflection is because different energy environments require different types of transformers. Rifkin (1982, p. 263) states "the greatest physicist A.S. Edington, hailed the entropy law as the supreme law of nature", where according to Schrodiyer (cited in Rifkin, 1982, p. 5) every living thing in the world survives by drawing from its environment negative entropy.

4.2.4 The isomorphism of entropy

In applying the concept of entropy to the state of various systems, the validity of its isomorphic application must first be considered and established. According to Morales-Matamoros, et al, (2009, p. 72) despite the variety of specific systems and their complexity, there are universal laws of various phenomena which are essential to our understanding of systems generally. Schaefer, et al, (1977, p. 12) explains that there are interdisciplinary properties of General System Theory, including hierarchical structure, stability, teology, differentiation, approach to and maintenance of steady states, goal directedness etc. Such interdisciplinary properties means that in many research fields, the systems approach has turned out to be the optimal and most powerful tool for systematic analysis (Byeon, 2005, p. 223), where according to Byeon (1999, p. 284) entropy is a term that whilst originated in thermodynamics is applicable to all systems.

The concept of entropy has been seen as a foundational concept in many current research trends, especially in contemporary systems theory. Although the term originated in the field of thermodynamics, it has both theoretical and mathematical interpretations, as well as wide spread applications in other disciplines (Byeon, 2005, p. 224). According to Byeon (2005, p. 224) a large number of useful terms and concepts have been transported into other disciplines from their original discipline. Since its original inception by Clausius in classical thermodynamics, entropy has witnessed a series of subsequent incarnations. As such, according to Bailey (1990 cited in Byeon, 2005, p. 224) the term entropy can be used as long as it is qualified by a prefix, as in, social entropy. This approach enables various isomorphic applications of entropy to be differentiated from Clausius' entropy, or Boltzmann's' entropy, or biological entropy, or any other concept which lacks certain prefix.

In considering the isomorphic aspects of entropy, according to Midgley (2003, pp. 74-75) there are instances in many sciences where the techniques and general structure bears an intimate resemblance to similar techniques and structures in other fields. That is, a one-to-one correspondence between objects which preserves the relationships between the objects is called an isomorphism. In considering the isomorphic aspects of entropy, Roos (1997, p. 16) argues that it is scientifically acceptable for one discipline to borrow concepts from another discipline. Such a process has resulted in important theoretical innovations. As stated by Atkins (1986, p. 2) "the avoidance of commitment to any particular microscopic interpretations means thermodynamics is not limited to particular applications".

As such, the concept of entropy is becoming increasingly popular and used to discuss the state of various systems, see Rifkin, (1982; Herman, 1999; King, 2008; and Lovey & Nadkarni, 2007). For example, the second law of thermodynamics (entropy law) has been applied to many domains including information security (King, 2008), organisational systems (Lovey & Nadkarni, 2007), combat systems (Herman, 1999), communications, biology, economics, sociology, psychology, political science and art (Rifkin, 1982, p. 263). It is argued by this thesis that a PPS is a complex, open system, dependent on its elements, each element's constituents and their interrelationships through systematic application. Entropy is a concept conceived to discuss the

degradation, disorder and decay within a system relating to a systems ability to carry out work.

The study argues due to the isomorphic aspects of science and the literature applying entropy to open systems, following the path of GST the concept of entropy can be applied to a PPS to discuss the gradual degradation, disorganisation and decay of and within a PPS. That is, security decay can be explained in terms of an entropy state. The theory of entropic security decay recognises that entropy processes exist in PPS, where we can distinguish both a given entropy state at a particular time, and how the general processes of entropy increase and decrease over time.

4.3 The theory of entropic security decay

Consistent with the isomorphic principles of science (Bertalanffy, 1950; 1968) this study discusses and draws on the literature relating to systems theory within an open systems frame, Defence in Depth, and the science of thermodynamics to present a theory for explaining and measuring PPS degradation over time. The theory of entropic security decay was conceived within grounded theory principles, where according to Strauss and Corbin (1990 cited in Liamputtong & Ezzy, 2006, p. 266) grounded theories are those inductively derived from the study of the phenomenon they represent.

The theory of entropic security decay has been conceived, developed and provisionally verified through systematic data collection and analysis of published literature relating to the gradual degradation in the efficiency and effectiveness of a security system. This development was achieved through the identification of the interrelationship between the concepts of Defence in Depth, the systems approach applied to implementing Defence in Depth and the science of thermodynamics, specifically the concept of entropy. In applying this literature, it is argued that the system, mapped out, with its key performance indicators provides a framework for defining and measuring entropic decay within PPS.

Congruous with the writings of Bertalanffy (1950, p. 26; 1968, p. 39; Bittel, 1978, p. 1130; Keren, 1979, p. 316; Checkland, 1981, p. 83; Corning, 1995, p. 93; Skyttner, 1996, p. 43; Midgley, 2003, p. 386; Sheard & Mostashari, 2008, p. 296; Morales-Matamoros, et al, 2009, p. 72) this study defined a Physical Protection System (PPS) as a complex, open system. Such systems have a large number of interacting components

with non-linear coupling and significant interactions with their environment, depending on it for resources to maintain its product goal. A PPS transforms energy into (1) a product or services towards the detecting, delaying and responding to unauthorised intrusions (2), the product or service results from the exchange of energy between system constituents, individuals and groups towards achieving the protection goal. In light of the available literature, this thesis applies the concept of entropy within an open systems frame to discuss the natural and foreseeable decaying effects on such a system (PPS).

King (2008, p. 1) initially introduced the concept of entropy into the security literature. According to King (2008, p. 1) security controls inevitably degrade over time, where such "security system degradation is the result of such systems suffering from natural entropy". Honkasalo (1998, p. 136) explains that degradation measures the irreversible increase of entropy, which is the amount of usefulness lost. King's (2008, p. 1) statements introduce and applies the concept of entropy to the security domain body of literature. King's (2008, p. 1) view is abstractly supported by Howlet (1995, p. 222) who adds, even the best systems will deteriorate over time and use. The isomorphic application of entropy to a PPS is supported by Lovey and Manohar (2007, p. 99) who assert, various systems suffer from entropy. The application of the second law of thermodynamics, specifically the concept of entropy, to a PPS re-introduces the concepts of degradation and decay into the security risk management literature.

The argument that security controls can degrade over time reducing their commissioned levels of risk treatment was first considered by Underwood (1984), who referred to this as decaying security, stating, "Security Decay is the most serious threat to a security system", and that "security decay must be expected", "avoided", and "countered" (Underwood, 1984, p. xi). Decay is defined as a "*gradual decline*" in health, prosperity or excellence, a process of decline or deterioration (Collins Australian Pocket Dictionary of English Language, 1994), or less good or less strong (The New Oxford School Dictionary, 1991), based on these definitions, as a systems entropy level increases, system decay increases.

System degradation results from entropy production which reduces the efficiency and effectiveness within a system, impeding it to achieve its output goal (Bohm & Peat, 2000, p. 137). However, according to Denbigh (2009, p. 4) for entropy to have an effect

on a system it must have initially been considered orderly, where orderliness is capable of being quantitatively stated. For a system to be defined as orderly, its elements must be appropriately distributed in space and/or time, where the rule of orderliness states that a set of three or more objects will display a certain orderliness if they exist in a linear arrangement, for example objects A, B and C. In this context, the objects obey the rule as B is to the right of A, and C is to the right of B, etc. In addition, the same objects will display the kind of orderliness if a relationship also exists between successive separations AB, BC, AC, etc, resulting in a more comprehensive state of order.

The study argues that entropy relates to a security system as the Defence in Depth functions must be performed in their sequential order and within a length of time, which is less than the time required for the adversary to complete their task (Garcia, 2001, p. 6). These functional requirements of Defence in Depth are distributed in space and/or time according to Denbigh's (2009, p. 4) entropy rule. The available literature indicates that the space and time distribution of the defence in depth elements create a comprehensive state of order in relation to a PPS macro level of effectiveness. The micro states within Defence in Depth include the constituents within the elements of deter, detect, delay, and response, which may be considered a linear arrangement (Denbigh, 2009, p. 4; Garcia, 2001, p. 6) Deterrence (element A) is linear to detection (element B), which is linear to delay (element C) followed by a linear response (element D).

Orderliness also exists within a PPS (Denbigh, 2009, p. 4) for example, deterrence. Deterrence is achieved by altering the cost benefit analysis of a rational choosing adversary (Singh, 2005). Within a PPS each function of the defence in depth strategy within this linear relationship must be achieved in their sequential order, achieving deterrence through systematic application of detect, delay, response (Garcia, 2006, p. 240) and recovery, in this sequential combination. Deterrence is related to an adversary's chances of being detected (B), the difficulty in achieving their goal (C), and the chances of getting caught (D). Therefore deterrence has an orderly relationship with all other elements within a PPS, being A=BCD.

In addition, another orderliness relationship exists between response (D) and detection (B). Response is an organisations means of interrupting an adversary before they achieve their goal; however, for response to be achieved there must be knowledge that

an attack is underway (detection). Therefore a relationship exists between response and detection, namely B×D. Further delay is the means by which the facility provides their response force with enough time to interrupt an adversary. Therefore delay has an additional kind of orderly relationship with response, C×D. Furthermore, each element of defence in depth has a vertical relationship with its constituents, which combined provides the specific capability for that element within the linear relationship.

Coole and Brooks (2009) argued that for the system of Defence in Depth to be effective, the relationships between the constituents and elements must be orderly and each constituent must be at its desired level of effectiveness. That is, for a PPS a time penetration continuum exists (Figure 4.1) based on this integrated systems approach incorporating the elements of defence in depth linear, orderly relationships, and the elements constituents vertical orderly relationships.

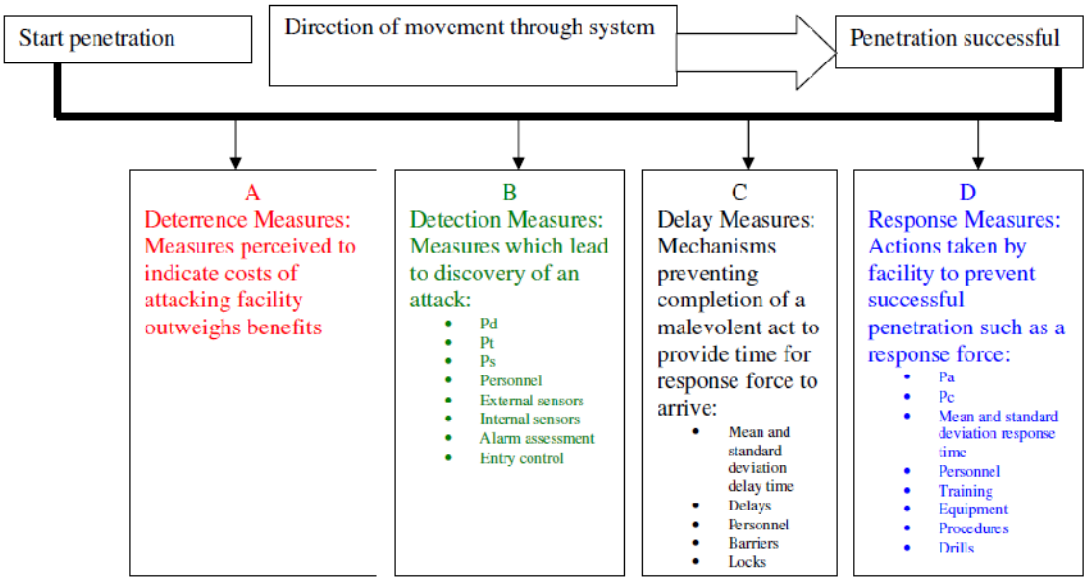


Figure 4.1 Defence in Depth time penetration continuum (Adjusted from Garcia, 2001, pp. 6-7).

Such a process is based on the definition of entropy offered by Bohm and Peat (2000, p. 137; Bertalanffy, 1968, p. 42; Herman, 1999, p. 86; Rifkin, 1982, p.8), where degradation and disorder within and between elements increases, decay increases and capability decreases.

4.3.1 System sensitivity

In applying the concept of entropy to Physical Protection Systems (PPS), the available literature states "a security system is only as good as its parts, when a single part fails, this failure can cause degradation within the total system" (Konicek & Little, 1997, p. 184: King, 2008, p. 1). Garcia (2006, p. 29) supports this view, stating "system effectiveness can become degraded through the reduction in effectiveness of individual components" (microstates). These views are consistent with the literature relating to, and discussing the principles of systems theory, where according to Waldman (2007, p. 272) if part of a system is changed, the nature of the overall system is often changed as well. Midgley (2003, p. xxviii) expands on such a view stating, "even the tiniest influences may have a major effect on the future direction of the system".

These views are consistent with Lorenz's (1968) findings, technically termed "*sensitivity to initial conditions*", meaning that any difference in input into a system, no matter how small, will eventually produce enormous differences in output (Warren, Franklin & Streeter, 1998, p. 363). According to Jang, et al, (2009, p. 750) for a PPS the sensitivity value is defined as the change of the Pi according to increments of detection probability and/or delay time along an adversary's path. However, this study contends that response force aspects such as time are also included in this sensitivity value. In addition, the sensitivity of the system is also related to the location of detection capabilities along an adversary's path.

Such sensitivity considerations are consistent with Dillon's (1983, p. 119) views suggesting within a complicated system such as a PPS there are a whole series of Bifurcation points. Such a focus on the relationships between the micro and macro states within a security system towards maintaining system effectiveness is supported by King (2008, p. 1) who states "it is the gradual erosion of seemingly minor security controls which eventually lead to major incidents". It is this aspect of GST that applies the concept of entropy to discuss the health of PPS.

Lorenz's (1963; 1968) work described how small changes occur at a specific point (point disturbance) in a system, which then expand to the boundaries of the areas for which they occupy. Consistent with Lorenz's (1963; 1968) works, entropic decay theory purports that constituent decay enters the systems at a specific point, regardless of aetiology, then manifests itself at this specific point in the PPS along an adversary's

attack path, then in line with the established relationships between the elements of Defence in Depth, propagates through the remainder of the system along this attack path, directly reducing the systems macro-state measure (Pi). Such a scientific, systems approach to analysing the whole was supported by the early works of Isaac Newton who stated, "the extension, hardness, impenetrability, mobility and inertia of every object depends on the extension, hardness, impenetrability, mobility and inertia of its component parts (The Open University, 1976, p. 68).

4.3.2 The effects of entropic decay on a PPS

This study's interpretation of the effects of entropy, specifically from a point disturbance, is abstractly supported by Howlet (1995, p. 220) who explains that a poorly maintained security system will have many unexplained alarms leading to the guard force losing their confidence in the system and eventually ignoring a true alarm as just another false alarm. As such, this study contends that consistent with Lorenz's (1968; Warren, et al, 1998, p. 363; Midgley, 2003, p. xxviii; Howlet, 2005; Waldman, 2007; Jang, et al, 2009, p. 750) works, the original decay, located within the detection element (point disturbance), expands to the boundaries of the detection elements key performance indicator, resulting in a failure to effectively detect the threat. This failure to detect the threat, due to the interrelationships between the defence in depth elements, results in the system becoming disordered ultimately resulting in this point disturbance propagating through the remainder of the defence in depth system.

Drawing on the assumption that an immediate response to an event exists, either by guards or law enforcement, It is argued that such decay propagation, manifested in high nuisance alarm rates impedes on the human factor within the system reducing the effectiveness of the alarm assessment (P_A) key performance indicator. As this breakdown in the various subsystem key performance indicators propagates throughout the remainder of the system it removes the probability of guard force communication (P_C) performance indicator, resulting in the guard force never being dispatched, meaning the delay time becomes diminished. Based on the notion of an integrated system, subject to entropy, It is proposed that the macro-state effect of this point disturbance results in the adversary not being interrupted, therefore achieving their desired goal, resulting in the adversary defeating the defence in depth system due to decay manifested in the first element.

For example, to be effective, a detection capability must ensure its sensors are correct for their application, installed correctly, have a low nuisance alarm rate and be difficult for the threat to defeat (Garcia, 2006, p. 14). For the transmission system to be effective it must be able to successfully transmit an alarm from the sensor to the security control room, where factors such as corroded wires could impede this capability (Adams, et al, 2005, p. 2). For the assessment system to be effective the video images containing the alarm source must provide quality of detail so that a person can accurately determine the cause of an alarm. For the entry control subsystem, the software must correctly receive electronic information from the installed entry control devices, compare this information to data stored in a data base, and generate unlock signals to the portal locking device when data comparisons match (Garcia, 2006, pp. 14-17). In addition, the systems mean times for both delay and response must be maintained at their commissioning levels of effectiveness. That is, all of the various system subsystems must be at their commissioned level of effectives to maintain the systems commissioned macro-state performance measure (Pi) over time.

4.3.3 Entropic security decay defined

The starting point in evaluating the validity of entropic security decay in a PPS must include a theoretical definition of the concept. Based on the available literature it is argued that conforming with the concept of entropy the constituents of a PPS move from an available to unavailable state or from an ordered to a disordered state. Such entropy production impedes on a systems capability to achieve its macro-state output, therefore reducing the effectiveness of the "whole" system. Whilst the concept of entropy is becoming increasingly popular and used to discuss the state of various systems see Rifkin, 1982; Herman, 1999; Lovey & Nadkarni, 2007; King, 2008), as a concept entropy is tremendously difficult to grasp. Entropy is a concept previously discussed within the field of physics (Styer, 2001, p. 1; Lovey and Monahar, 2007, p. 99) where its meaning is difficult to define and not well understood outside of academic circles. Such definitional ambiguity has lead to ubiquitous usage and minimal general understanding. Whilst various definitions and understandings are applied to entropy, a central theme or common thread is how various components of a system relate to one another towards producing a coherent whole. Where according to Bohm and Peat (2000) entropy is characterised by terms including disorganisation, disintegration and decay, whilst Herman (1999, p. 86) adds steady-degradation.

This study argues that the concept of entropy provides a framework for explaining and measuring the gradual degradation of a physical protection system after its commissioning. For example, according to Aslakse (2004, p. 272) the condition or state of an element within a system is represented by the ability of that element to support interactions with other elements, which have some form of internal structure of their own. If left to themselves, that is remained closed, each element will decay or fail. As such, if a system is to continue in some form of operating state there needs to be processes and maintenance to achieve this. It is argued that such a view is what Underwood (1984, p. xi) refers to when he wrote, decay occurs when building fabric and hardware deteriorate and frequently, when human frailties accumulate.

4.4 The measurement of security decay

In considering the measurement of security decay, Thompson (2002, p.1) explains that entropy is an idea born from classical thermodynamics and is therefore a quantitative entity rather than something intuitive, defined via an equation. This view is supported by Dillon (1983, p. 183) who points out that mathematics is a significant and important aspect of science and therefore, it is only natural that mathematical techniques will be employed. That is, according to Lindsay (cited in Dillon, 1983, p. 183) physics is quantitative in the sense that it aims to answer the question how much, rather than merely "how".

As the expression of quantity requires numbers, physicist' use mathematics to deal with the numbers and the various operations which may be performed by them. Mathematics provides the simple means of expressing functional relations between symbols to which operational significance can be attached, and from such relations logical deductions can be drawn (Dillon, 1983, p. 183). For example, according to Thompson (2002, p.1) the specific definition of entropy via an equation comes from Clausius (1865) who defined entropy by the equation:

$$S = Q/T \tag{24}$$

Where S = the entropy, Q is the heat content of the system, and T = the temperature of the system.

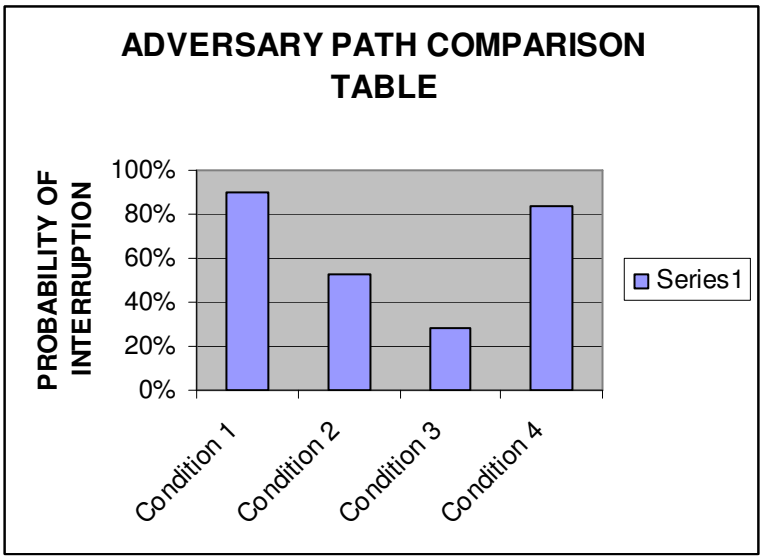
The benefits of such a quantitative approach are emphasised by Martin (2000, p. 210) who states "when conducting research one of the first things to do is to establish a base-

line, that is a steady state", where according to Martin (2000, p. 210) the amount of change can be considered as a percentage of a preset threshold level. Such an approach is supported by Lorenz (1968, p. 290) who considered that once the initial state of a system is known, then any change in this state , beyond its preset threshold level, can be regarded as its measure of error. Accordant with Coole and Brooks (2009, p. 23) the study argues that entropy can be quantitatively measured for a Defence in Depth system by drawing on the EASI equation:

$$P(I) = P(D1) \times P(C1) \times P(R/A1) + \sum_{i=2}^{n} P(R/Ai)\, P(Ci)\, P(Di) \prod_{j=1}^{i-1} (1 - P(Di)) \quad (25)$$

This equation was used to establish the systems commissioning, or operational level macro-state (Garcia, 2001) in chapter two. Congruous with the premises of systems theory EASI quantitatively demonstrates the various mathematical relationships among the constituents and elements performance measures within PPS. The elements key performance measures are the cumulative sum of the various subsystems within a PPS, where any changes in these inputs have an overall effect on the output (probability of interruption). Therefore, accordant with the principles of systems theory, changes in the microstates have a direct effect on the macro-state of the PPS. For example, Table 4. 1 indicates the direct effects on the macro-state of the PPS with small changes in the microstates when calculating the probability of interruption using EASI adversary path analysis. For Table 4.1 probabilities are numbers between 0 and 1, however it is common practice to convert such probabilities to a percentage. Therefore Table 4.1 represents the probability of interrupting an adversary as a percentage.

Table 4.1: Adversary path comparison table (Coole & Brooks, 2009, p. 24).



For Table 4.1, condition 1 presents a Pi of 90% (very high chance of interruption) after entering the microstate data from condition 1 Table 4.2. However, condition 2 indicates a much lower Pi after making small changes in the systems microstates as a result of a detection sensors reduced effectiveness due to decay resulting in a higher nuisance alarm rate and by slight increases in response time due to decay in the facilities response capability. This condition indicates a Pi of just 53% (medium chance of interruption) after entering the microstate data from condition 2, (Table 4.2). Condition 3 (Table 4.1) indicates how the probability of interruption can be further reduced with a change in the facility's probability of communication due to decay in the communications system. This condition shows Pi of just 28% after entering the microstate data from condition 3 (Table 4.2).

Table 4.2: Physical Protection System microstate data (Coole & Brooks, 2009, p. 24).

Physical protection system microstate data

Condition	P_D	P_D	P_D	Pcomms	Mdelay (secs)	Mdelay SD (secs)	Mrespond (sec)	Mrespond SD (sec)
1	0.9	0.9	0.9	0.95	332	99.6	200	60.0
2	0.5	0.9	0.9	0.95	332	99.6	300	90.0
3	0.5	0.9	0.9	0.50	332	99.6	300	99.6
4	0.9	0.9	0.9	0.95	452	135.6	300	90.0

With small changes in the systems microstates through correcting the detection fault, slightly increasing the facility's mean delay time and correcting the communication systems degradation, condition 4 (Table 4.1) shows an increased Pi of 84% (high chance of interruption) after entering the condition 4 microstate data from Table 4.2. These examples emphasise that the macro-state of the Defence in Depth system is recognised as an expression of the average of the microstate variables collectively, where sensitivity changes in microstates (Defence in Depth constituent elements) directly affect the macro-state. These results from an EASI analysis are concordant with Lorenz's (1963) findings indicating that small differences can, over a long period of time, build to produce a large effect. For example, the first half of the EASI equation interlinks the probability of alarm (P/A) with the delay and response aspects of the system. However, the second half of the equation considers the probability of non-detection (P_{ND}), therefore, as probability of detection decreases, the probability of non-detection increases.

Consistent with the quantitative aspect of entropy, and the sensitivity of the systems macro-state to changes within the various micro-states, this study argues that once a systems state has been established, based on the security risk management requirements, then any change within the various key performance indicators, and the systems macro-state, beyond a preset threshold level, quantitatively represent both the amount of decay and its location within the PPS. In considering this assertion, Tester and Modell (1997, p. 82) point out that entropy meters do not exist. According to Tester and Modell (1997, p. 82) a change of state is defined by a change in the value of at least one property, where Pitzer (1995, p. 30) highlights that entropy is an extensive property, where the entropy of a system is equal to the sum of the entropies of its parts. That is, the entropy of as system is a macro-state.

In considering the entropy of and within a PPS, Pitzer (1995, p. 26) explains that when measuring a quantity a standard must initially be chosen. Then there needs to be a means of comparing the measurement of the object of interest with this standard. Based on the available literature, specifically drawing on Clausius's (1865) reasoning, it is argued algebraically that entropic security decay within a PPS can also be represented through Clausius's (1865) entropy equation:

$$S = Q - T$$

(26)

Where S = the measure of system entropy (entropic security decay); Q = the initial commissioning state of a PPS (Pi); and T = the current analysed state after a defined period of time (Pi).

4.5 Security decay and risk management

In applying the concept of decay into the security risk management literature, this study argues that such decay within a PPS reduces the effectiveness of risk controls which increases facility vulnerability. This view is supported by Garcia's (2001, p. 272) vulnerability equation, highlighting vulnerability through the formula:

$$\text{Vulnerability} = 1 - (Pi)$$

(27)

Such increase in vulnerability increases a facilities security risk state. Such a view is uniform to Standards Australia HB 176 (2006, p. 62) which states "it is also important to consider that a small change in control effectiveness may have a substantial effect on vulnerability". This premise is congruous with the definition of entropy offered by Bohm and Peat (2000, p. 137; Bertalanffy, 1968, p. 42; Herman, 1999, p. 86; Rifkin, 1982, p.8), where degradation and disorder within and between elements increases, decay increases and capability decreases. For example, Somerson (2003, p. 13) explains that where strategies in place are insufficient to deter, detect, delay, respond to and where necessary recover from risks, then a higher opportunity vulnerability exists for an organisation. That is, based on the Normal Distribution, as control shrinkage occurs, the population samples with the capabilities to penetrate a facility would increase, rather than the desired decrease as decay manifests. In addition, for the defined threat the situation becomes more compounding, as demonstrated by Figure 4.3.

The concept of decay is one of "*gradual*" degradation, where, as stated by King (2008, p. 1), "it is the erosion of seemingly minor security controls which eventually leads to a security incident resulting in a loss event". That is, congruous with McCrie (2004, p. 16) the result of decay interlinked with a facility's risk rating and the effectiveness of its security controls can be summarized through the equation:

$$Oportunity = \frac{Risk\ [Threat\ \times Vulnerability\ \times Criticality]}{\sum 3DR}$$

(28)

For example, Figure 4.2 indicates that as the constituent's key performance indicators decay gradually, the system as a whole decays, reducing the macro-state effectiveness measure below its commissioning measure. Such decay is congruous with the data from Tables 4.1 and 4.2. However, perceptually the system may appear to maintain its steady state. It is argued that this premise is supported by the writings of Howlett (1995, p. 219) who states "*from the time of taking a system into use it will start to deteriorate. No system, however well designed, can be completely reliable without proper maintenance. If left without attention, it will become unserviceable. However, the operator may not be aware of it, but the system will not perform as intended*". This "*subtle"* degradation results in the system performing below the level of risk control considered necessary for a specific security risk context. That is, in relation to the normal distribution of a defined threat's capabilities, the systems effectiveness may be below its defined threat. In addition, as the system is perceived to be degraded by potential adversaries it can be argued that the deterrence element of Defence in Depth is also degraded (see Figure 4.2) leading to the perception by opportunistic offenders that the benefits outweigh the costs leading to a decision within the rational choice framework to attempt a penetration.

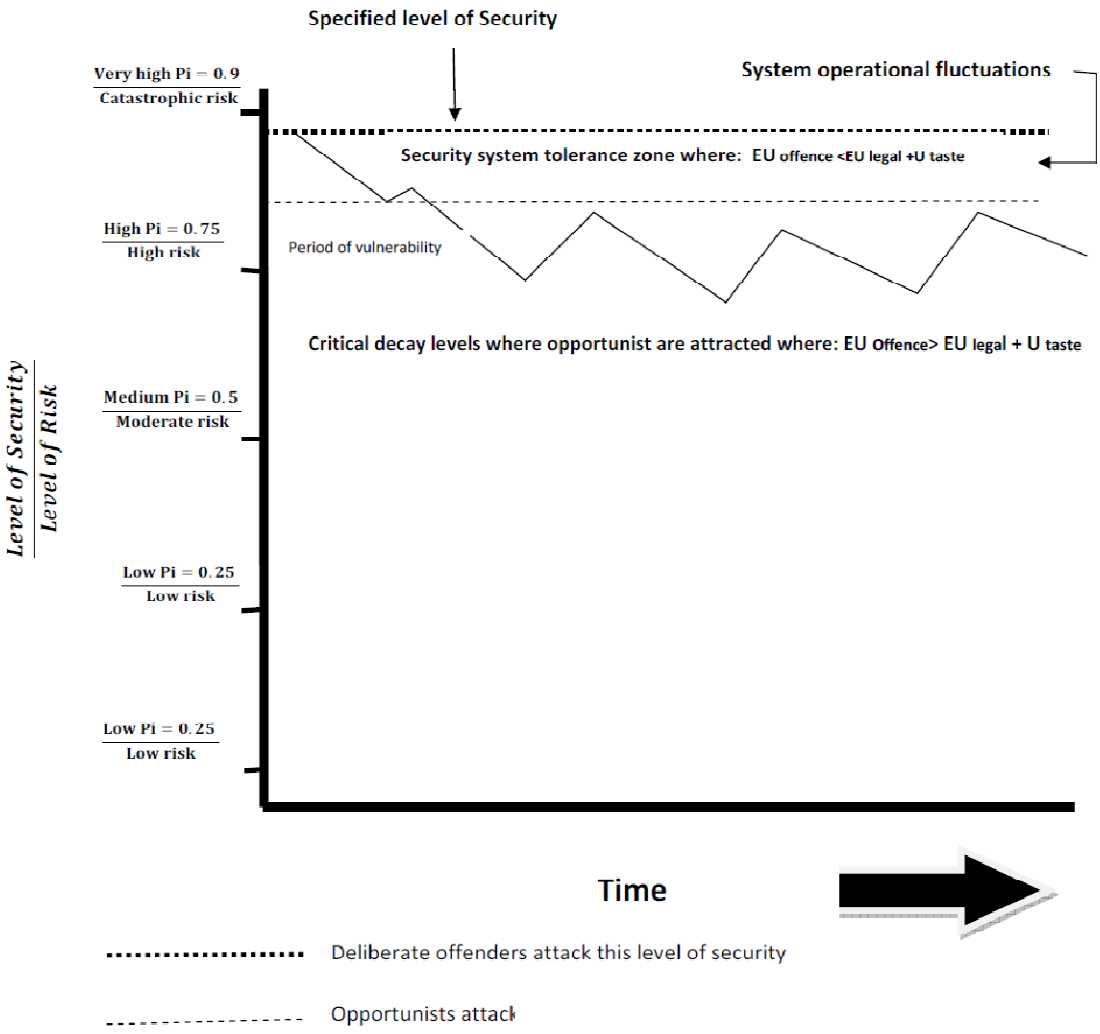


Figure 4.2 Effects of decay on implemented security levels (Adopted from Underwood, 1984; Martin, 2000; Garcia, 2001, 2006; Pidwirny, 2006; HB 167, 2006).

Consistent with the principle of equifinality (Figure 2.5,see Section 2.2.6.2), Figure 4.2 indicates the effects of decay on the systems commissioning level of effective security when utilizing the Pi and Risk Equation to establish cost benefit based levels of security. Adjusted from Underwood (1984; Martin, 2000, p. 210; Garcia, 2001, 2006; Pidwirny, 2006; Standards Australia HB167 Security Risk Management, 2006).

4.5.1 The effects of entropy on the critical path

The study operationally defined security as "a stable condition stemming from a systematic process which effectively combines people, equipment and procedures, within a security context, to restrict unauthorised access to either people, information or physical assets through their ability to deter, detect, delay and respond to attacks which may lead to loss of, or, harm to protected assets manifested by a malevolent human

adversary/s who seek/s to gain a level of unauthorised access". When considering the concept of entropic decay in relation to such a definition Garcia (2001, pp. 242-247) explains there are many possible paths for an adversary into a facility, however it is the critical path which characterises the effectiveness of the overall protection system in detecting, delaying and responding and interrupting an adversary.

The critical path is defined as the most vulnerable path, that is, the path with the lowest probability of interruption (Pi). However, the theory of entropic security decay considers that constituent degradation along the other alternative paths into a facility may result in effectiveness regression so they become the critical path. That is, the alternative paths effectiveness in detecting, delaying and responding to an adversary's actions are lesser than those calculated measures for the critical path.

4.6 Avoiding and countering entropic security decay

Systems are subject to dynamic behaviour which includes growth, unstable growth, stagnation, cyclical instability and decay (Bittel, 1978, p. 1135). In addition, open systems exist in a dynamic relationship with their environment, receiving various inputs which are transformed in some way and then export outputs (Byeon, 1999, p. 285). The receipt of inputs in the form of matter/energy and information enables open systems to offset the natural entropy processes (Laszlo cited in Byeon, 1999, p. 285). That is, due to natural entropy, survival of the system would not be possible without continuous inflow, transformation and outflow (Byeon, 1999, p. 285). Consistent with Hankasalo (1998, p. 131), like any other open system, a PPS needs low-entropy input where low-entropy means both ordered materials and available energy, and it must be able to emit high entropy output into its environment. For example, a physical system which is totally isolated from all information and energy inputs (closed) will quickly degrade, just as will the classical thermodynamic closed system (Byeon, 2005, p. 283).

According to Byeon (1999, p. 287) non-equilibrium thermodynamics suggests that open framed systems are able to circumvent the effects of the second law of thermodynamics (the thermodynamic arrow of time) through their feedback processes. That is, certain systems have the property of feedback, that is, a portion of their outputs or behaviour is fed-back as input to affect succeeding outputs (Midgley, 2003, p. 73). According to Midgley (2003, p. 73) man-made system possess many of the properties possessed by natural systems, where simple notions such as wholeness, segregation and summativity

have meaning for both types of systems. This feedback process is aimed towards the irreversible aspects of the laws of statistical probabilities, by importing negative entropy (negentropy) into the system above that amount of entropy production (S), therefore reversing the effects of natural entropy upon the system. From a thermodynamic view point, a PPS where the appropriate feed-back mechanisms are in place would be negentropic, where transfers of information and energy/matter from the external environment can decrease entropy production so that total system entropy may remain constant, or even decrease over time.

The available literature suggests that a PPS should be designed, implemented and managed as a system. In applying an open systems frame to the discussion of decay within a PPS this study contends that for a PPS to be managed as a system, the necessary open systems feedback must be included within the risk management cycle. Where feed-back is achieved during the monitor and review process. As such, the concept of security decay should be considered an important component of security risk management. Such a view is supported by the writings of Lovey and Manohar (2007, p. 99) who assert that various systems suffer from entropy, therefore organisations must understand that for a system to operate efficiently they must continually invest in resources to maintain system adequacy to reduce natural entropy. Underwood (1984, p. 249) supported this view, stating "A*fter an attack the immediate reaction is often to increase the originally established security resources. However, usually this is not necessary, as all which may be required is the re-establishment of the intended level of protection*".

To some degree, such security decay is recognised by Standards Australia HB167 (2006, p. 87), which incorporates a monitor and review stage in the risk management process. Standards Australia HB167 (2006) suggest that the monitor and review stage is a critical component in security risk management, based on the argument that security risk environments are dynamic rather than constant, sometimes discretely changing and other times, dramatically over short periods. According to Robinson (1999, p. 58) for systems it is also important to know when a process is not fully satisfying the performance criteria, to plan for corrective action. Therefore the security risk management cycle has to in some form incorporate the effects of decaying risk reduction strategies (Figure 4.3).

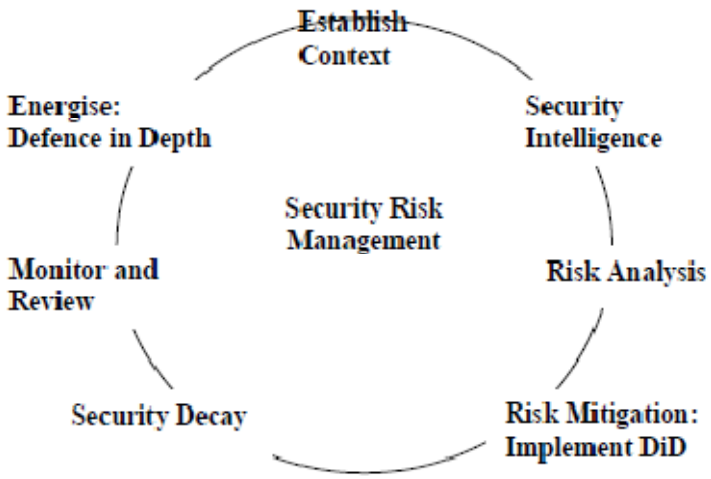


Figure 4.3 Security risk management cycle (Coole & Brooks, 2009, p. 25).

It can be argued the monitoring and review stage of the security risk management process should aim to energise or put-back energy into the system to eliminate entropy. That is, it is at this stage where a PPS engages in the necessary feedback mechanisms to maintain the system in a steady state, and detect micro changes within the systems constituents to ensure an appropriate level security is maintained to ensure the necessary level of risk reduction.

4.7 Conclusion

This chapter completes phase one of the study; the establishment of a systems framed security decay benchmark. The chapter applied the concept of entropy within systems theory literature to discuss how the output goal of a Physical Protection System (PPS) can be impeded by the effects of natural entropy characterised by terms such as disorganisation, disintegration, decay and steady-degradation. It has been argued in this chapter that the concept of entropy within a system approach has isomorphic application encompassing all systems (see Section 4.2.3), and without the appropriate feedback mechanisms which characterise open systems, a system is either closed or becomes closed.

Closed systems inevitably move towards a state of thermodynamic equilibrium. That is, accordant with the laws of thermodynamics, closed systems attain a time-independent equilibrium state resulting in the death of the system. However, by importing negentropy from their environment, open systems can reach a time-independent state

where the system remains constant as a whole, referred to as a steady state, that is, a state encompassing very little change over time (see Section 4.6). For a PPS the objective is to commission a system which implements measures that combine to deter, detect, delay and respond to adversary threats based on a defined threat, where such a system maintains its commissioned level of risk treatment over time, that is, it is able to circumvent the effects of natural entropy to ensure it constantly achieves it output goal.

Phase one of the study presents the argument that the concept of entropy provides a framework towards measuring the gradual degradation of a Physical Protection System (PPS) after its commissioning. Study Phase 1: Security decay textual benchmark; the theoretical foundation of security decay, lead to the proposition that security decay could be defined as:

> The gradual degradation of the microscopic quantities (constituents), or the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system.

CHAPTER 5

MATERIALS AND METHOD

5. 0 Introduction

This chapter presents the methodology and supporting literature drawn on to achieve phases two, three and four of the study. The chapter presents the study design (Section 5.2) and a number of supporting theories (Section 5.3) which provide the research design's scientific frame. This presentation includes a description of the Delphi method used for conducting research that draws on expert groups and the concept of expertise and expert opinion which underpins the Delphi method. In addition, the literature describing the use of interview techniques in qualitative research is presented. Section 5.4 presents a potential alternative methodology and explains the reasoning supporting the choice of a qualitative design. Furthermore, Section 5.5 presents the study's target population (N=6) with a discussion on the difficulties in establishing a valid security expert sample, and how participants for the study were selected based on Section 5.3.

This chapter also presents Section 5.6 materials, explaining the informed consent process and interview questionnaire. Section 5.7 discusses the research procedure and ethics, and Section 5.8 presents how the study's collected data was analysed in a two stage process facilitating the interpretative design of the study. Section 5.9 presents the concepts of reliability and validity and their underpinnings in qualitative research. This discussion is facilitated through a description of the safe guards within qualitative research which aim to ensure research findings are considered both reliable and valid, and how these techniques have been employed within this research design towards establishing truthfulness in this study's interpretation of collected data. The chapter is summarised with a conclusion in Section 5.10.

5.1 The theory of entropic decay

The theory of entropic security decay was conceived based within grounded theory principles, where according to Strauss and Corbin (1990, p. 23) such theories are "those which have been inductively derived from the study of the phenomenon they represent". A theory is a set of concepts used to define and/or explain some phenomenon, where such concepts form the basic units of analysis when researching into specific phenomena. Theories consist of plausible relationships produced among concepts and sets of concepts (Silverman, 2002, p. 77), where in the development of grounded theory,

concepts, categories and themes are identified and developed whilst the research is being conducted (Strauss & Corbin, 1990, pp. 23-25).

Theory building occurs in an ongoing dialogue between pre-existing theory and new insights generated as a consequence of research (Liamputtong & Ezzy, 2006, p. 266). The theory of entropic security decay was inductively conceived within the principles put forward by Strauss and Corbin (1990, p. 23), where researchers' do not begin with a theory then seek to prove it, rather they begin with an area of study and what is relevant to that area is allowed to emerge. As such, the theory of entropic security decay was inductively conceived through the conceptual review of literature relating to a systems approach towards security risk management, the argument that security controls degrade over time and the application of systems degradation literature, specifically the concept of entropy. This study aimed to evaluate and expand this inductive theory utilizing a qualitative research approach.

5.2 Study design

A qualitative approach was adopted to achieve the outcomes of this study. Such a design enabled the study's sub-questions and research question to be responded to through the gathering of security expert's knowledge and experience within their respective security domains as it related to the concept of security decay. Security experts' "expertise" within their discipline specific areas provided the research data towards establishing whether they through their experience, supported the various premises presented within the theory. An interpretation of such support required a consensus of security expert's opinions relating to the factors associated with each of the research sub-questions, underpinned by their deep thoughts, feelings and emotional insights.

The choice of a qualitative research methodology is supported by Morrison (1998 cited in Cohen, Manion and Morrison, 2005, p. 22) who states, "for people multiple interpretations and perspectives exist in relation to events and situations". "Therefore "reality is multi-layered and complex". As such, researchers should therefore examine phenomenon through the eyes of participants rather than themselves. Cohen, et al, (2005, p. 24) explain that such research designs enables the investigation of knowledge which is considered "commonsense", "taken for granted" assumptions from lived experience. This approach is achieved by way of "reflexivity" that is, imputing meaning retrospectively, by the process of looking back on the past.

5.3 Research theories

To explore the theory of entropic security decay required participants who intuitively understand this theory's basis and where necessary, were able to move their previously established positions relating to security decay based on new, incoming information. This exploration required a specific depth of knowledge from professionals who had extensive expertise in the security industry. It was therefore argued that a panel study in the form of a Delphic poll was the most appropriate methodology for such a contemporary, rigorous query of expert's opinions relating to the concept of security decay.

5.3.1 The Delphi Methodology

The Delphi technique is a viable research methodology for building theory, specifically the generation of grounded theory (Okoli & Pawlowski, 2004, p. 27). It is therefore argued the Delphi methodology is more appropriate than a traditional survey questionnaire for evaluating theory inductively derived at utilizing grounded principles. Such an argument is based on the literature of Okoli and Pawlowski (2004, p. 19). According to Okoli and Pawlowski (2004, p. 19) traditional surveys require researchers to select a sample size suitable for averaging and detecting statistically significant effects in a population. Their focus is towards random statistical sampling of a population of interest, towards generalizing their results to a larger population. In contrast to this focus, a Delphi study aims to arrive at an answer to difficult, technical questions through purposive panels of chosen experts.

As Okoli and Pawlowski (2004, p. 19) explain, Delphi study results do not depend on sample sizes and statistical power, but rather group dynamics towards arriving at a consensus among experts. The Delphi approach has been supported by studies which have consistently shown that for questions requiring expert judgment, the average of individual responses (survey results) is inferior to results produced by group decision making processes.

5.3.1.2 Delphi methodology benefits

Delphi studies build theory (Okoli & Pawlowski, 2004, p. 27), specifically, data gathered during Delphi studies can be analysed as part of an inductive process for the generation of grounded theory (Eggers, Ohio & Jones, 1998, p. 58). This characteristic of the Delphi technique was of significant importance for this study as the theory of entropic security decay was inductively conceived by drawing on grounded theory principles. Because Delphi studies solicit information from experts who have a wide range of experience, they extend the empirical observations from which initial theory is based, strengthening the grounding of the theory and increasing the likelihood that the resulting theory will hold across multiple settings (Okoli & Pawlowski, 2004, p. 27).

As a research methodology, Delphi originated from a series of studies by the RAND Corporation during the 1950s (Okoli & Pawlowski, 2004, p. 16), referred to as project DELPHI (Dalkey & Helmer, 1963, p. 458). Delphi is a carefully designed, systemic iterative research method towards providing information for better decision making. This method is utilized for structuring anonymous group communications from geographically dispersed individuals who have special knowledge to share relating to complex and important issues which can be collated for judgment. Delphi employs sequential individual interrogations interspersed with information and opinion feedback (Ribbens & Cole, 1989, p. ii; Eggers, Ohio & Jones, 1998, p. 54; Okoli & Pawlowski, 2004, p. 16).

As a research methodology Delphi is based on the premise that several heads are better than one when formulating conclusions from incomplete evidence and that experts, within a controlled intuitive process, will make such conjectures based upon rational judgment and shared information as opposed to simply guessing (Eggers, et al, 1998, p. 54). This premise is supported by a series of studies conducted by Dalky (1969) which found that when anonymous and controlled feedback was provided to members of a decision making group, more accurate decisions were produced than when such groups engaged in face to face discussions.

According to Delbecq, Van de Ven and Gustafson (1975, p. 10) Delphi is used towards the achievement of various objectives, including:

1. To determine or develop a range of possible program alternatives;
2. To explore or expose underlying assumptions or information leading to judgments;
3. To seek out information which may generate a consensus on the part of a respondent group;
4. To correlate informed judgments on a topic spanning a wide range of disciplines;
5. To educate the respondent group as to the diverse and interrelated aspects of the topic.

This study drew on these Delphi objectives to gather security expert's knowledge and experience as it related to the concept of security decay. The strength of these objectives in explaining contemporary issues is supported by Okoli and Pawlowski (2004, p. 16) who state "researchers have applied the Delphi method to a wide variety of situations as it does not attempt to be representative of any population through statistical sample but rather is a group decision tool", to consider opinions for solving research problems utilizing a group of subject matter experts (Schmidt, 1997, p. 764). The purpose of a Delphic Poll is to gather a consensus of expert opinions relating to a topic under investigation using several rounds of questionnaires or interviews (Sproull, 1995, p. 242), and can be used to notify study participants of recent scientific advances.

Delphi as a research methodology facilitated the identification, evaluation, and clarification of factors pertaining to the concept of security decay from a systems approach, and established positions by drawing on the current knowledge of the study's participating experts (Delbecq, et al, 1975, p. 84). This approach is supported by Schmidt (1997, p. 764) who explains that Delphi has been used in fields such as "public administration (Preble, 1983), medicine (Spiby, 1988), technology diffusion (Gray & Nilles, 1983), social work education (Ruskin, 1994), and operations management" (Malhotra, Stelle, & Grover, 1994). Delphi is used in situations where complex issues are to be understood which do not lend themselves to precise analytical solutions

(Eggers, et al, 1998, p. 55). A specific strength of the Delphi technique is that it can deal with very technical issues (Effective Engagement, N.D., p. 2).

Such strength characteristics of the Delphi technique provided significant benefits for this study as the concept of security decay within the framework of the theory of entropic security decay is a concern framed by very technical literature. That is, Delphi studies encourage innovative thinking towards a research problem (Sproull, 1995, p. 242) and play a vital role in research projects where developing consensus among experts in a particular discipline field is critical (Eggers, et al, 1998, p. 64). Such a philosophy was considered significant in achieving the aim and objectives of this study due to the contemporary nature, and scale of the subject matter and the dearth of dedicated published literature surrounding the concept of security decay generally, and from a systems approach.

According to Sproull (1995, p. 242) Delphi research designs are based on a number of assumptions, including:

- Experts are the best sources of opinions,
- Expert opinion will be even better if experts respond independently and anonymously,
- Opinions will be even better if respondents are allowed to modify their responses after receiving feedback on how the rest of the group responded
- Several rounds of questionnaires and feedback of results will bring about a consensus of opinions.

5.3.1.3 Delphi methodology disadvantages

Nevertheless, Delphi polls do have some disadvantages. As Sproull (1995, p. 242) advised, Delphi is a time consuming and costly research methodology. Delphic polls usually require 3-5 rounds of interviews or questionnaires. Sproull's (1995, p. 242) concerns were considered in establishing this study's procedure, and cognisant with these disadvantages, due to budgetary and time constraints this issue was overcome by conducting only two (2) rounds of interviews, following the pilot study. Conducting only two (2) rounds of interviews produced some limitations within this study's findings (see Section 10.3).

In considering such limitations Delbecq, et al, (1975, p. 106) explains that some Delphi studies do stop after a second round, in particular if an additional round is not required or further clarification is not important. Concordant with Delbecq, et al, (1975, p. 106) it was not considered necessary to conduct further additional rounds of panel interviews. It was considered more appropriate to analyse, reflect and interpret the data gathered across this study and based on this study's outcomes, make future recommendations towards refocusing the research enquiry, adding additional, objective insights.

5.3.2 Expertise

Based on its methodology and underlying principles, the selection of experts is critical to the results of a Delphic poll. The use of experts' opinions provides a particular study with the benefit of relatively fast utilization of the expert's compressed knowledge (Erricsson, Charness, Feltovich & Hoffman, 2006, p. 749). According to Erricsson, et al, (2006, p. 749), the core aspect of an expert's role consists of providing experience-based knowledge which novice individuals could themselves attain if they had enough time to undertake the necessary learning. The overall objective is to obtain the most up-to-date and reliable consensus of opinions from a study's expert panels (Okoli & Pawlowski, 2004, p. 16). However, experts should be selected using a defensible selection method (Sproull, 1995, p. 242). In considering the above, according to Eggers, et al, (1998, p. 55) the term "expert" and how it is used is a controversial issue. Walton (1992 cited in Eggers, et al, 1998, p. 54) contends there are three ways to distinguish experts from lay people:

- Experts are people with sufficient knowledge and experience to have mastered the advanced skills of a particular domain of knowledge or experience;
- Experts are proficient in their actions and have specific ways of applying their knowledge to a task in their area of expertise;
- Experts are also proficient at identifying problems in their areas and then being able to tell if identified problems are solvable, then experts solve them.

This view is supported by Delbecq, et al, (1975, p. 88) who consider the key points in selecting an expert is to identify the desirable knowledge and qualifications of potential participants. For example, according to Bedard and Chi (1992, p. 135) studies have shown that a large, organized body of domain knowledge is a prerequisite to expertise.

That is, experts have a greater quantity of domain-relevant knowledge than do novices. In addition, the knowledge of experts is organized in ways that makes it more accessible, functional, and efficient. Also, experts knowledge is extensively cross-referenced with a rich network of connections among concepts resulting in richer processing, whereas, novices have fewer and weaker links among concepts (Bedard & Chi, 1992, p. 135). Cornford and Athanasou (1995, p, 11) add, occupational expertise is based on case and episodic knowledge accumulated over extensive periods of time, and involves both positive and negative instances. Weiten (2002, p. 223) explains, the episodic memory system is constructed of chronological, or temporally dated recollections of personal experience. That is, episodic memory is a personal record of things a person has done, seen or heard.

It is argued that significance in defining an expert is the concept of knowledge, where knowledge can be discussed in terms of its quantity or its structure (Bedard & Chi, 1992, p. 135). According to Novak and Gowin (1984 cited in Brooks, 2007, p. 3) knowledge is constructed, through the expansion of existing concepts. As new knowledge is gained, it changes a person's understanding of their existing knowledge. According to Bedard and Chi (1992, p. 135) such knowledge may be based on previous knowledge (built upon) and individual's experience, and an individual's interaction within their environment. Such a large organized body of domain knowledge influences the perceptual processes and strategies of problem solving. A view which is supported by Rennie and Gribble (1999 cited in Brooks, 2007, p. 4) who point out, knowledge can be considered a perceptual understanding towards a subject matter and may not be necessarily concrete or fact. Cornford and Athanasou (1995, p, 11) add, episodic knowledge is associated with isolated pieces of knowledge or incidents which, when brought together by cognizant individuals, build up a more coherent domain specific picture.

Stake (2010) supports the application of knowledge to the concept of expertise. According to Stake (2010, p. 13) professional work depends on science, but each profession has its own separate body of knowledge. It is therefore considered that professional knowledge differs from scientific knowledge, although overlaps exist. Professional knowledge is the lore gained from working with others having similar training (scientific knowledge) and depth of experience. What especially characterises professional knowledge is a focus on the fact that how knowledge is applied varies with

the situation, that is, congruous with Walton (1992 cited in Eggers, et al, 1998, p. 54) experts draw on their expertise (episodic knowledge) to solve problems. For example, Bedard and Chi (1992, p. 136) found, in problem solving, the greater amount and better organization of an expert's knowledge compared to novices, results in two very different styles of problem solving.

Bedard and Chi (1992, p. 136) point out these differences have been shown to exist in problem representations, problem solving strategies and the quality of decisions. For problem representation, representations consist of a person's interpretation or understanding of the problem. Such an interpretations are based on people's domain related knowledge and their organisation of this knowledge. People represent problems by classifying them as a particular type, where classification is based on a person's solution procedures attached to each type of problem. However, to classify a problem one needs to pick out the most relevant features, or must infer additional aspects about the problem, given the explicitly stated features. Both these feature-identification processes are more efficient and superior among experts.

In addition, such identified differences are more salient in ill defined problems, where the problems structure lacks definition in some respect. In solving ill defined problems experts spend considerable amounts of time developing problem representations by adding many domain-specific and general constraints to the problem, as if they are modifying the problem from an ill defined to a well defined problem. However, novices attempt to solve the problem without defining it (Bedard & Chi, 1992, p. 136).

Cornford and Athanasou (1995, p. 12) explain that in problem solving, the situation can be summed up as; novices seek logical, fairly consistent all purpose rules to guide their behaviour. Advanced beginners start to employ experience problem solving processes. Competent level practitioners exercise greater authority in problem solving, they set priorities and make plans, they determine what is important and that the order of priority may change. Proficient practitioners may no longer consciously think about adjustments, for them intuition or "know-how" becomes important. These practitioners notice similarities between events, with greater analysis and decision making with more flexible observance of rules. However, experts have an intuitive grasp of situations, where their performance is fluid and qualitatively different.

According to Cornford and Athanasou (1995, p. 12) the knowledge of experts contains fewer rigid classifications of areas of data, with mastery of understanding of the interrelationships and linking between the different areas of knowledge. Expert's store solutions and use them again, they learn from their mistakes, and tend to portray what they are solving in familiar elements. These elements describe the operations to be performed and allow the expert to find an optimal solution under conditions of uncertainty. Bussing and Herbig (2003, p. 145) suggest professional expertise includes the intuitive knowing how, and less the theoretical thus formalised knowing what.

Based on the available literature, according to Erricsson, Charness, Feltovich & Hoffman (2006, p. 3) an expert is defined as a person widely recognised as somebody with extensive knowledge or ability based on factors including; research, experience, occupation, or education and training within a specific area of focus (domain) beyond that of the average person, sufficiently that others may rely upon that individual's opinion. Cornford and Athanasou (1995, p. 10) add, domain experts are defined, in serious professional fields, by their reasonably skilled peers with whom they work. This study drew on this literature to establish its target sample of participants congruous with Bedard and Chi (1992, p. 136) as security decay is at present an ill defined problem. However, experts have an intuitive grasp of solutions, "intuitive knowing" stemming from their knowledge and experience (Cornford & Athanasou, 1995, p. 12).

5.3.2.1 Security Expertise

This study required an expert with domain specific episodic knowledge and experience within the security profession. However, in establishing a security expert Phinney and Smith (2009, p. 2) argue that the knowledge domains of security are relatively unknown. For example, Brooks (2007, p. 1) advices, "security is a multi-disciplined industry, constructed from knowledge stemming from a multitude of disciplines". That is, according to Brooks (2007, p. 2) security practitioners provide a wide range of services in areas including security management, human resources, risk management, crisis management, investigations, information technology and computing, physical security and security technology.

For example, towards defining security through the presentation of security knowledge categories Brooks (2007) conducted a study to establish:

- What are the knowledge categories of security;

- What are the subordinate concepts of security
- What is the expert knowledge structure and subordinate concepts of security as measured by expert interviews;
- Can security be defined through knowledge categorization and supporting concepts?

Brooks's (2007) study results presented security categories which included (N = 14) categories across many associated industries (Table 5.1), within many occupations.

Table: 5.1 Security knowledge categories

Security knowledge categories

Security category descriptors		
Criminology	Emergency/contingency planning	Fire science
Facility management	Industrial security	Information and Computer
Investigations	Physical security	Security principles
Risk management	Safety	Security law
Security management	Security technology	

Accordant with Delbecq, Van de Ven and Gustafson (1975, p. 88); Cornford & Athanasou, 1995, p. 10; Okoli and Pawlowski (2004, p. 22); Erricsson, Charness, Feltovich & Hoffman (2006, p. 3); and Brooks (2007) for this study, security experts were defined based on their biographical information relating to their qualifications, length of years of experience, and tenure in government positions, and advice they provide across the various security discipline categories established by Brooks (2007). In accordance with Cornford and Athanasou (1995, p. 10), security experts were selected through peer nomination based on their revered reputations across these categories and have been peer nominated (defined) as experts.

5.3.3 Interviews

This research enquiry adopted a qualitative approach, responding to this study's sub-questions and research question through the gathering of security expert's knowledge and experience by employing a semi-structured interview questionnaire. Interviews are a systematic means of discussing with people an area under investigation towards collecting data and constructing knowledge in research. The use of interviews in

research considers that knowledge is something generated between people, often through conversation. Interviews enable research participants in a study to discuss their interpretations of the world in which they live, and to express how they regard issues under investigation from their personal experience (Cohen, et al, 2005, p. 267).

Interviews differ in their openness of purpose, their degree of structure, and the extent to which they are exploratory or hypothesis testing, and whether they seek description and interpretation (Liamputtong & Ezzy, 2006). To respond to this study's questions semi-structured interviews were conducted to gather data from security experts via direct verbal interaction drawing on an interpretative analysis (Cohen, et al, 2005, p. 268). Semi-structured interviews can also be referred to as in-depth interviews, or focused interviews (Liamputtong & Ezzy, 2006, p. 56). Such interviews focus on participants' subjective responses to a known situation in which they have been involved, and which has been analysed by the researcher prior to the interview.

Based on the outcome of such interviews researchers are able to support or reject previously formulated ideas relating to their focus of inquiry (Cohen, et al, 2005, p. 273). Semi-structured interviews are very common in qualitative research. They draw on an interpretative theoretical framework emphasising a belief that meanings are continually constructed and reconstructed during interaction. In this research methodology, participants' become constructors of knowledge in collaboration with their interviewer (Liamputtong & Ezzy, 2006, p. 57). That is, the interview methodology facilitates for interviewers to bring in their own knowledge of an area under investigation, enabling them to probe for deeper views and opinions of the interviewee (Cohen, et al, 2005, p. 273). In drawing out security expert's intuitive knowledge relating to the concept of security decay, it was argued that such a process underpinned by the available literature was an excellent means of explaining such an ill defined problem.

5.3.3.1 Disadvantages of interviews

According to Liamputtong and Ezzy (2006, p. 72) interviews as a research methodology do have their disadvantages. First, interviews are resource intensive, that is, they take a great deal of time and expense to collect data. Second, in-depth interviewing is difficult to do well. However it is argued that these disadvantages were overcome by various advantages interviewing provides towards achieving research goals. These advantages

included the fact that semi-structured interviews are an excellent means of discovering a person's interpretations of their relevant experiences. In addition, they allow for new understandings and theories to be developed during the research process.

It was this strength of the interview technique which the study sought to draw on towards establishing whether security experts support the premises and principles underpinning the theory of entropic security decay. In addition, according to Liamputtong and Ezzy (2006, p. 72), participants generally find the interview process rewarding. Consistent with this view, during the interviews all participants reported that they did enjoy the process and found the subject matter under investigation very interesting. As such, it is argued that this research methodology enabled participants' (interviewer and interviewee) to discuss their point of view with regards to the concept of entropic security decay where concordant with the writings of Cohen, et al, (2005, p. 267) experts' were able to offer their deep thoughts and feelings either supporting or refuting the premises underpinning the theory of entropic security decay.

5.4 Potential alternative methodology

An alternative means of collecting data relating to the concept of security decay may have been facilitated through the use of a psychometric survey questionnaire (attitude test) in the form of a rating scale. There are three types of scales that have been utilized in the construction of such attitude tests, including Guttman Scaling, Thurnstone scales and Likert Scales (Kline, 2000, pp. 91-95). For example, a Likert scale is a survey rating scale which measures attitudes, opinions and motivations by asking study participants to indicate whether they agree or disagree with each statement in the questionnaire (Martin, 2000, pp. 223-224). In designing a scale Loewanthal (2001, p. 3) suggests a multi-item measure is needed where there is an underlying central conceptual entity with a number of facets which may not be tapped by a single question.

However, the variables and factors underpinning the theory are still under investigation at the conceptual stage. Until further research is carried out, factor analysis showing that specific constructs or factors are correlated with the phenomenon under investigation is limited in its validity. Nevertheless, according to Loewenthal (2001, p. 31) a good means of sourcing items to be included in psychometric measures is through qualitative interviews. This approach is based on the premise that in qualitative research, data analyses is carried out concurrently with data collection. That is, with qualitative

studies, a constant interplay exists between collection and analysis which produces a gradual growth in understanding of the phenomenon under investigation (Walliman, 2005, p. 188).

5.5 Participant sample

In determining a suitable research sample, Best (1989, p. 10) highlights that it is not possible to study an entire population. As such, according to Okoli and Pawlowski (2004, p. 19) many research methodologies are focused towards random statistical sampling of a population of interest, with the aim of generalizing their results to a larger population. In considering a valid research population Lin (1976, p. 146) explains that the total group of people (cases) who meet certain criteria of interest set by researchers is referred to as its research population. Such a focus requires researchers to select a sample size suitable for averaging and detecting statistically significant effects in a population (Okoli & Pawlowski, 2004, p. 19). In discussing the selection of a suitable participant sample for a research study Martin (2000, p. 219) suggests that a representative sample is one where the extent of the sample truly represents the population under investigation. Cohen, et al, (2005, p. 93) add, that such samples have a measure of randomness and therefore a degree of generalizability.

However, in considering the issue of a statistical sample representing the security industry, Brooks (2007, p.1) explains that security as a profession is a multi-disciplined industry. This eclectic mix has resulted in a profession which lacks clear definition, potentially the result of its diversity and inter-disciplinary structure, as security draws its breadth of knowledge from many disciplines. For example, as Brooks (2007) study; *mapping the knowledge structure of security*, highlighted fourteen (14) security knowledge categories including: criminology, emergency/contingency planning, facility management, fire science, industrial security, information and computer security, investigations, physical security, principles, risk management, security law, security management, technology and threats. In addition, Brooks (2007) reported a list of supporting subordinate security concepts (N=2001). Brook's (2007) views are supported by Borodzicz and Gibson (2006, p. 181) who adds that due to its diverse tasks, security is both difficult to define and practice. That is, security practitioners provide a significant range of professional services.

In addition to definitional concerns, Borodzicz and Gibson (2006, p. 191) highlight that researching in the security domain is tremendously difficult given that the industry often shrouds itself in secrecy. Many of the practitioners within the security industry often decline to be researched by academics even though they wish to draw on a body of knowledge towards stronger professional standing. This very aspect of the security industry was experienced during the study, where some security "expert" practitioners declined to participate irrespective of its research focus and abstract nature of the interview questionnaire. These combined issues impede the successful poling of a statistically representative security expert sample. Furthermore, when considering the suitable size of a research sample Cohen, et al, (2005, p. 93) explain that no clear answer exists, therefore consideration of statistical analysis, that is, the research methodology, is what drives the selection suitable sample size.

In considering the issues effecting a valid security industry statistical sample and the writings of Cohen, et al, (2005, p. 93), Okoli and Pawlowski (2004, p. 16) point out that the Delphi method does not attempt to be representative of any population through statistical sample. Rather it is a group decision tool to consider individual's opinions towards solving research problems utilizing a group of subject matter experts (Schmidt, 1997, p. 764), using several rounds of questionnaires or interviews (Sproull, 1995, p. 242). More specifically Rundblad (2006, p. 2) explains that a suitable participant sample size for qualitative research designs using interviews requires very few participants.

In addition, when considering an appropriate sample size for grounded theory Liamputtong and Ezzy (2006, p. 51) suggest that sample size is determined on theoretical as opposed to statistical grounds. It is the representativeness of concepts not of persons which is crucial. Such a view is faithful with Silverman (2002, pp. 138-250) writings who explains that participants for qualitative research generally stem from purposive sampling, as researchers seek out specific groups and individuals to evaluate the processes under investigation (Silverman, 2002, pp. 138-250).

Based on the available literature, participants' for this study consisted of peer nominated security experts (N=6) selected and solicited to participate who were employed to provide security category knowledge advice across the varied security related occupations. Their selection was based on their meeting such criteria, where based on their extensive knowledge or ability, their experience, occupation and/or education and

training others rely upon them for professional opinion within the multi-disciplined security industry and they were considered by their peers (peer revered) as experts. These experts formed a non-probability (purposive) sample, enabling the full scope of their professional experience and judgement of the issue to be explored. Purposive sampling is supported by Cohen, et al, (2005, p. 102) who state "such samples are selected when researchers target a particular group based on very specific research needs".

5.6 Materials

Accordant with the requirements of informed consent, an information letter was prepared (Appendix A). The letter presented the aims and benefits of the study. In addition, the letter briefly discussed the premises underpinning the theory of entropic security decay and explained the workings of a Delphi poll. In addition, potential risks and discomforts were presented to participants, where it was anticipated that there would be no foreseeable risks and discomforts within the study. The explanation letter also explained that there was no penalty for withdrawing from the study as participation was voluntary. Conforming to Edith Cowan University ethical requirements, an independent contact person was nominated and their contact details were provided to participants as part of the research letter. The last page of the research letter was an attached informed consent acknowledgement slip, where participant's informed consent was formally recorded.

A semi-structured interview questionnaire was prepared (Appendix's B & C) consisting of open ended questions supplemented with closed questions. The questionnaire sought to obtain participants' deep feelings, concerns and experience (Cohen, et al, 2005, p. 148) associated with decaying PPS. Questions were drawn from the conceptual benchmark (Chapters 2, 3 and 4). Participant's responses were written on the survey questionnaire using a pen, with additional writing pad materials provided to ensure answers were not limited to available space on the questionnaire. The interviews were transcribed into word documents (Appendix D) for validity checks and analysis.

5.7 Research procedure and ethics

5.7.1 Procedure

To achieve the research goals a sequential multiple phase methodology was applied (Lin, 1976, p. 5) incorporating a Delphic Poll, employing semi-structured interviews to gather data from security experts through direct verbal interaction (Cohen, et al, 2005, p. 268). This research process required the repeated individual interviewing of participating experts. Congruous with Eggers and Jones (1998) individuals identified/nominated as experts were contacted by telephone or email and solicited to participate in the study. Once contacted, potential participants were informed about the objectives of the study, the nature of the panels, the obligations of participants, the length of time the Delphi process was going to take (1-2 hours), and the information which would be shared among the study's other participants (Delbecq, et al, 1975, p. 88). Those who respond favourably were sent the research letter explaining the research methodology and premises formed. This study then followed a multiple sequential phase process towards achieving its desired outcomes. These steps and activities are outlined in Figure 5.1.

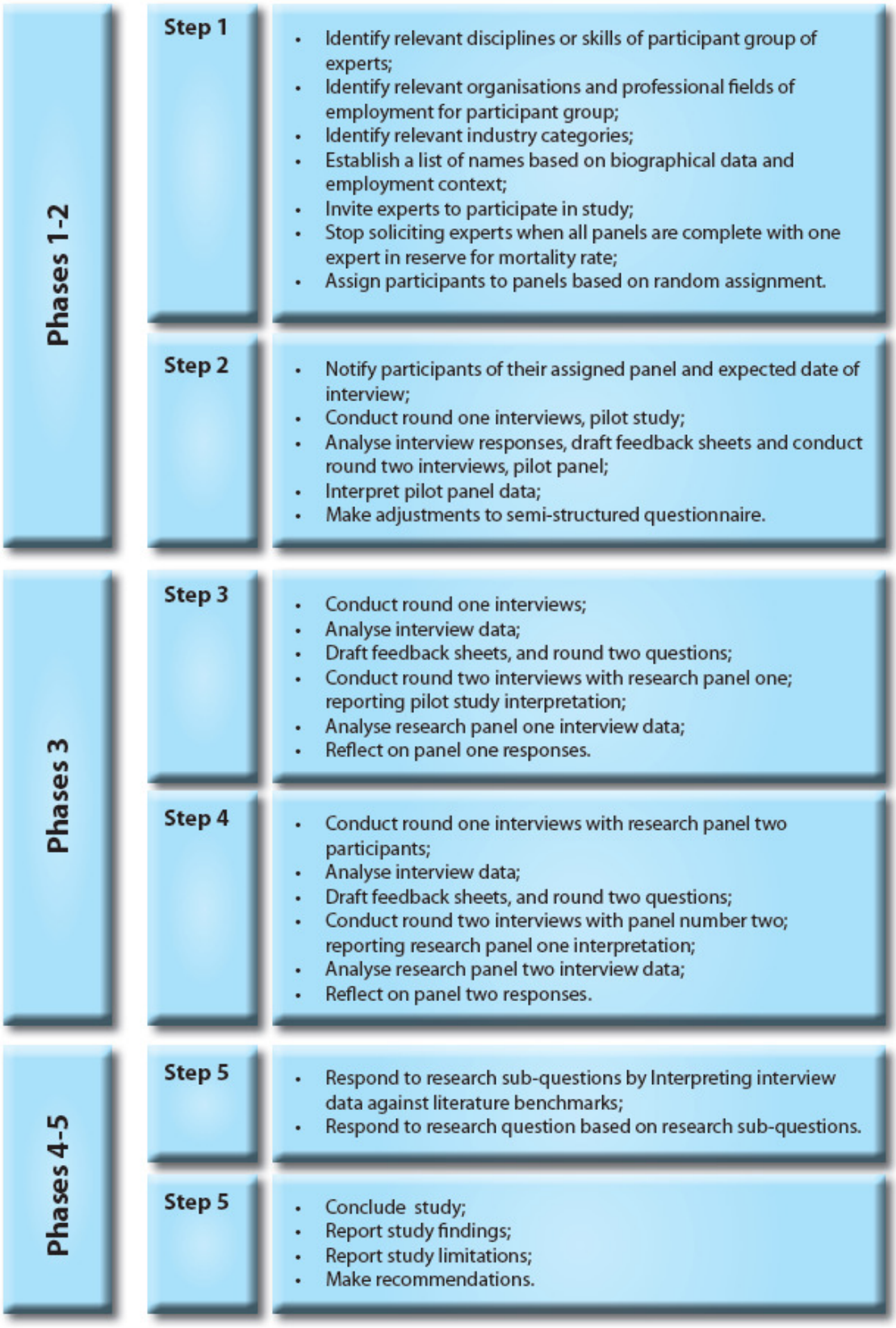


Figure 5.1 Study procedural steps.

Given the difficulty in conducting research in the security domain, research data was recorded manually by the interviewer during the interview process. This method is considered suitable when the potential exists for participants to constrain their answers when faced with mechanical means as manual recording appears less threatening to participants (Cohen, et al, 2005, p. 281). For answers where interpretation was subjective, clarification was asked during the interview to increase internal validity.

5.7.2 Ethics

In moving into the data collection phase of the study, it must be acknowledged that ethics are an essential aspect of scientific research. The concept of ethics stems beyond specific principles or abstract rules applied to a research design. They are about the issues or potential problems each research situation presents (Davies & Dodd, 2002, p. 281). According to Davies and Dodd (220, p. 281) within a research framework, ethics exist in researchers' actions, and in their ways of doing and practicing their research, they are always in progress, never to be taken for granted, flexible and responsive to change.

In the pursuit of an ethically robust study congruous with Forshaw (2004, p. 48) ethical approval for conducting the study was gained from Edith Cowan University's ethics committee. In addition, all participants solicited to take part in the study were given information pertaining to what they were agreeing to participate in to ensure the protocols of informed consent. All participants were informed that there was no penalty for refusal to participate (Forshaw, 2004, p. 47), and no undue pressure was placed on any participants if they declined to participate in the study (Forshaw, 2004, p. 45), as this did occur. In addition, all interviews were conducted without any time limits, and no financial or other material benefits were offered to individuals for their participation in this study.

For some participants there was a legal obligation to protect their identity and keep their data/personal information confidential. In-light of this to ensure the confidentiality of participant's data and identities, participants were not asked to supply their names or other identifying details outside of research data requirements. All participants who agreed to participate in the study were interviewed utilizing the pre-established semi-structured interview questionnaire which had been submitted to Edith Cowan University's ethics committee for prior approval.

5.8 Analysis

An essential part of research is data analysis to measure, make comparisons, and examine phenomena relationships towards generating explanations (Walliman, 2004, p. 301). In qualitative research data analysis is predominately interpretative (Cohen, et al, 2005, p. 282), where according to Patton (2002, pp. 453-454) qualitative analysis is typically inductive in the early stages, where the final, confirming stage is deductive. Conforming with Patton (2002, p. 453) and Liamputtong (2006, p. 265) the study was evaluated through the use of an interpretative analysis, where stage one of the analysis initially drew on an inductive methodology, where at the completion of all interviews, responses were analysed (Gillham, 2000, p. 69), inductively identifying themes (Krippendorff, 2004 cited in Liamputtong, 2006, p. 259) using line-by-line analysis of panel members responses. The inductive analysis was aimed towards generating natural units of meaning, looking for explanations and/or constructs which provide the data patterns and themes (Strauss & Corbin, 1990, p. 72). This analysis focused on the themes of important messages inherent in the participant's responses, such messages stems from the interviewee's perspective of research subject matter, being security decay (Liamputtong, 2006, p. 111).

Stage two of the study's analysis subjected the inductive analysis to a deductive analysis. This analysis was achieved using informed intuition to deductively connect the inductive data (participant's responses) with the literature benchmark, and interpreted by comparing participant's responses with the textual data, and considered in relation to this study's research sub-questions, establishing a chain of evidence towards making inferences in relation to responding to this study's research question.

The deductive analysis was achieved drawing from a benchmark (Chapters 2 and 3) conceived in phase one of the study from the literature stating that security is applied within a systems approach (Underwood, 1984, p. xi; Fennelly, 1997; Garcia, 2001, p. 6; Fisher & Green, 2003, p. 164), where such systems are only as good as their parts (Konicek & Little, 1997, p. 184: Fisher & Green, 2003, p. 164; Garcia, 2006; King, 2008, p. 1). This literature was combined with literature published from systems theory, specifically how the macro state of any system is directly related to the sum of its microstates (Bertalanffy, 1950; Churchman, 1968; Bittel, 1978; Checkland, 1981; Waldman, 2007). This literature is supported by research conducted by Lorenz

(Butterfly Effect, see, Lorenz, 1963; 1969; Peirce, 2000), and literature supporting the isomorphic application of entropy to discuss the irreversible processes suffered by a system without the appropriate feed-back mechanism (Bertalanffy, 1950; Bittel, 1978; Keren, 1979; Prigogine, 1987; Pidwriny, 2006; Morales- Matamoros, Tejeida-Padilla & Badillo-Pina, 2010, p. 75-76).

This synergy of literature brought together knowledge from laws, theories and concepts across multiple textual documents. This process identified major and minor themes towards developing a benchmark for framing the deductions in response to this study's research sub-questions and research question, by comparing the messages and themes stemming from the questionnaire with those stemming from the theory's document benchmark (Cohen, et al, 2005, p. 283). According to Silverman (2002, p. 229) such textual data are in principle reliable sources for analysis, where in-line with Patton (2002, p. 453) such a conceptual review provides a framework for data to be deductively analysed.

The aim of the analysis was to establish a level of theoretical validity for the study where, congruous with the literature from Sections 4.3.1 and Section 4.3.2 it was argued that by comparing the themes inherent in the security experts responses stemming from the semi-structured interview questions, to those inducted themes in the theory's embodying literature suitable evidence to respond to the study's research question could be drawn. To strengthen the reliability and validity of the deductive analysis closed questions were also employed to provide confirming data, establishing a chain of evidence of whether a consensus among the panels was achieved, aiding the interpretative analysis. The closed questions provided additional evidence supporting the interpretations and conclusions drawn for this study's research sub-questions, and provided the supporting data to enable an interpretation of consensus amongst the research panels, in-line with the methodological principles of the Delphi technique.

5.9 Reliability and Validity

Qualitative research, in its broad sense, embodies that research which produces findings not arrived at through statistical analysis or other means of quantification. Rather, qualitative research draws its findings through the use of analytical procedures utilized to interpret data stemming from observations and interviews (Strauss & Corbin, 1990, p. 18). That is, qualitative research does not seek to measure a phenomenon under

investigation, rather, it seeks to understand, represent or explain it (Pyett, 2003, p. 1170). However, faithful to the quantitative research philosophy, validity and reliability are two factors which must be considered when designing such studies, analysing results, and judging the quality of a study (Golafshani, 2003, p. 601). As Creswell and Miller (2000, p. 124) explain, a consensus exists amongst qualitative researchers that qualitative inquires' need to demonstrate their research studies are credible.

In quantitative research the terms reliability and validity are treated very separately, yet, these terms are not viewed so separately in qualitative research (Golafshani, 2003, p. 600). However, according to Bashir, Afzal and Azeem (2008, p. 35) both paradigms seek to find the same result, "the truth". For example, both qualitative and quantitative researchers need credibility in their research, where according to Bashir (2008, p. 35) validity and the norms of rigour which embody quantitative research are not fully applicable to qualitative research. Golafshani (2003, p. 604) explains that from a qualitative researcher's perspective, reliability and validity are entwined and conceptualised as trustworthiness, rigour and quality.

5.9.1 *Reliability*

Whilst the term reliability is a concept utilized when discussing the testing and evaluation of quantitative research (Bashir, et al, 2008, p. 39) it is also considered in qualitative research (Golafshani, 2003, p. 601). In quantitative research, reliability aims to ensure proposed research is creditable, dependable, consistent and trustworthy, where according to Cohen, et al, (2005, p148) it assumes research methods used can be employed to duplicate the sample with results being consistent. In applying the concept of reliability in qualitative research, Patton (2001 cited in Golafshani, 2003, p. 602) argues, in such a study, reliability is more a consequence of validity. Patton's (2001) view is supported by Silverman (2002) and Seale (1999, p.468) who state, reliability in qualitative research is framed around an examination of trustworthiness. As such Lincoln and Guba (1985 cited in Bashir, 2009, p. 39; Golafshani, 2003, p. 601) note, in qualitative research a demonstration of validity is sufficient to establish reliability.

5.9.2 *Validity*

The issue of validity has been an enduring issue in the debate relating to the legitimacy of qualitative research (Maxwell, 1992, p. 279). In a focused discussion on the topic Maxwell (1992, p. 279) highlights that if qualitative studies cannot consistently produce

valid results, the policies, programs or predictions based on such studies cannot be relied on.

In discussing the issue of validity in various research designs, Loewenthal (2001, p. 17) describes two specific types of validity which need to be considered when employing questionnaires, these are face and content validity. Face validity is suggested to be present when questionnaire items appear to measure what they are intended to measure, and can be gained by asking the questions to judges who are members of a target population and agree that the questions intuitively represent what they are purported to measure. Accordant with Loewenthal (2001, p. 17) to establish a measure of face validity within the study's research questionnaire, a professional security academic reviewed the semi-structured interview questions prior to their being tested in a pilot study (Face validity).

Once face validity was established, a level of content validity was pursued. Content validity is said to be present when particular test items actually represent what they are intended to measure (Loewenthal, 2001, p. 17). Content validity can be assessed by conducting a pilot study, which will enable actual observations of typical responses to researcher's questions (Cohen, et al, 2005, p. 121). Furthermore, congruous with Cohen, et al, (2005, p. 121) open-ended questions were supplemented with closed questions to enhance the reliability of the research design.

In addition to face and content validity, the available literature argues that to ensure reliability and validity in qualitative research an examination of truth is crucial (Golafshani, 2003, p. 601). Maxwell (1992, p. 284) explains, validity is not a sole product of a particular methodology rather validity pertains to the data, accounts, or conclusions drawn by employing a particular method in a particular context for a particular purpose. That is, validity in qualitative research is defined as how accurately an account represents participants' realities of the phenomenon under investigation, "truth" (Creswell & Miller, 2000, p. 1). In the pursuit of truth in qualitative research two specific types of qualitative validity are descriptive and interpretative validity (Maxwell, 1992, pp. 285-291).

5.9.2.1 Descriptive validity

Descriptive validity according to Maxwell (1992, pp. 285-286) relates to the factual accuracy in which participants responses to a situation or question are presented. For example, if a researcher reports that a participant made a particular statement during an interview, is this report correct? That is, did the participant really make that statement, or did the researcher miss-hear, miss-transcribe, or miss-remember their words? These issues of descriptive accuracy relate to what the researcher reports to have heard or seen.

5.9.2.2 Interpretative validity

Interpretative validity refers to the accounts of meaning drawn from an interview or observation. That is, interpretative accounts are grounded in the language and words of the participants studied and rely as much as possible on participants own words and concepts. Interpretative validity in qualitative research seeks to ensure inferences made from statements stems from the participants' perspective and not the researcher's perspective (Maxwell, 1992, pp. 288-291). Maxwell's (1992) views on validity are supported by Creswell and Miller (2000, p. 125) who explain that for qualitative research validity refers to both the data and the inferences drawn from it.

5.9.2.3 Truth

In qualitative research methodologies, descriptive and interpretative validity aim to establish truth. Truth is established through judgements in quality, where according to Seale (1999, p. 472) such judgements involve the objective establishment of trust, which is provided through the application of certain methodological procedures. According to Creswell and Miller (2000, p. 1) these methodological procedures include the application of one or more of the following techniques: triangulation, peer-review, external audit and thick description. This study through the Delphi methodology employed a number of these methodological procedures providing multiple layers of validity and reliability (truth) into the research design.

5.9.2.4 Triangulation

Throughout the study the principle of triangulation was employed, a methodology aimed towards establishing a level of validity and reliability in research findings (Golafshani, 2003, p. 603) through linking concepts and indicators which are checked by recourse of other indicators (Atkinson cited in Seale, 1999, p. 473). According to Patton (2002, p. 247) the term triangulation works in a metaphorical sense, drawing into conscious the world's strongest shape-the triangle, and is used as an analogy with

surveying and navigation where different bearings give a correct position (Silverman, 2002, p. 233). That is, a position on a map is discovered by taking bearings as two landmarks, creating lines which will intersect at an observers' position. In a research context, triangulation used from this analogy purports a single fixed reality can be known objectively through the use of multiple social research methodologies, increasing a study's validity (Blaikie cited in Seale, 1999, p. 473).

Triangulation aims to cancel out biases from any one research method by employing other, additional methodological measures (Seale, 1999, p. 473), drawing confirming data from multiple forms of evidence rather than a single incident or data point. These data points include theories, observations, documents and interviews (research participants) to locate major and minor themes towards establishing objective findings (Creswell & Miller, 2000, p. 3). Patton (2002, p. 247) explains that triangulation can occur in several forms. For this study, both theory and data triangulation was achieved drawing on a variety of textual sources to establish a benchmark (Chapters 2 and 3) within the conceptual review of literature which was drawn on to frame stage two of the study's analysis. In addition, investigator triangulation was established utilizing three participants per interview panel, where inferences were drawn based on the sum of each participant's responses, underpinned by the Delphi methodology. Furthermore, triangulation was achieved across the study by utilizing three panels, including the pilot panel, providing confirming data from multiple participants (researchers) and across multiple panels.

5.9.2.5 Audit trail technique

Triangulation was also pursued by means of the audit trail technique, where researcher/s provide clear documentation relating to all research decisions and activities enabling collected data to be externally evaluated for truthfulness. In achieving an audit trail, member checking was also employed within this study, where research data and their interpretations are shown to participants towards strengthening the credibility of data and narrative accounts. In this methodology participants add to the study's credibility (truthfulness) by having the chance to react to both the data representations, and the final interpretations. Finally, collaboration was included in this study's design between research participants and researcher during data collection and analysis phases, actively involving participants as co-researchers. Collaboration is closely entwined with member

checking, and occurs in many forms, such as building participant's views into the study design.

5.9.2.6 Validity lens

These combined procedures shift the validity lens from researchers to persons external from a study answering questions such as, are the findings grounded in the data or are inferences logical (Creswell & Miller, 2000, pp. 3-5)? In addition, for this study both audit trail and member checking was conducted by research supervisors from Edith Cowan University as part of this thesis's formal requirements.

In final consideration of the debate encompassing reliability and validity in qualitative research, Seale (1999, p. 465) warns a variety of conceptions exist, with competing claims determining what counts as good quality research. However, this debate has limitations to practicing social researchers, who are, in reality pursuing a craft occupation which is learned "on the job" through apprenticeship like conditions, encompassing trial and error. Therefore, this ongoing debate should encourage a degree of methodological awareness, which, should be employed at a level below where it would create anxieties that ultimately would hinder practice. Rather this debate should attempt to guard against obvious errors. Conforming to Seale (1999, p. 465) the study employed a number of techniques towards establishing a level of trustworthiness to satisfy concerns of reliability and validity in its design and research findings.

5.10 Conclusion

This chapter presented the methodology and supporting literature drawn on to achieve this research design and its outcomes. Section 5.2 presented the study design, where Section 5.3 presented the supporting theories providing the scientific frame of the study. This included a description of the Delphi method used for conducting social research, and the literature describing and supporting the use of interviews in qualitative research. Furthermore, Section 5.4 presented an alternative methodology and the reasoning supporting a qualitative approach. Section 5.5 presented the study's target population (N=6) and how participants were selected for participation.

This chapter also presented Section 5.6 materials, explaining the informed consent process and interview questionnaire. Section 5.7 discussed the research procedure and ethics considerations, and a discussion on the safe guards within qualitative research.

Section 5.8 explained the study's data analysis process, underpinning the study's interpretative design. In considering the study's research design, Section 5.9 discussed the concepts of reliability and validity in qualitative research and the various tools which will be applied across the study to ensure the study produces reliable and valid results.

CHAPTER 6

PILOT STUDY

6.0 Introduction

This chapter presents the initial participant based research data analysis and interpretation in responding to the study's research questions. The pilot study consisted of security experts (N=3) solicited as part of a purposive sample. This chapter presents the analysis of the pilot study's panel member's interview questionnaire data. Based on this analysis, responses are then compared against the reviewed literature (Chapters 2, 3 and 4) towards interpreting the results in relation to the various research sub-questions and this study's overarching research question. The aim was to establish whether the pilot panel support the premises underpinning entropic decay theory. In addition, this chapter identifies and explains recommended changes to the semi-structured questionnaire to increase both the depth of data collection and validity of this study.

6.1 Pilot study

In their pre-pilot work researchers identify specific topics central to the area or phenomenon under their investigation (Gillham, 2004, p. 25). These topics are then subjected to a pilot study, which is a small scale version of the researchers proposed research methodology (Martin, 2000, p. 136). The aim of such a process is to conduct a complete trial of the proposed methodology, and to iron out potential problems prior to commencing the resource intensive formal study (Martin, 2000, p. 136). As Martin (2000, p. 136) explains, when conducting a pilot study researchers' sometimes find that what previously looked good on paper just did not work. That is, a pilot study becomes the guide for the future research methodology.

6.2 Participants

Participants' for the pilot study consisted of peer nominated security experts (N=3) (see Section 5.5). These experts were selected and solicited to participate in this study based on the criteria that they are employed to provide security category knowledge advice across the varied security related occupations. Their selection was based on their extensive knowledge or ability, their experience, occupation and/or education and training others rely upon them for professional opinion within the multi-disciplined security industry and they were considered by their peers (peer revered) as experts, forming a non-probability (purposive) sample.

Participant one has worked within the security industry and specifically around Physical Protection Systems (PPS) for approximately twenty (20) years within the corrections environment. He holds a Bachelors Degree in Security Science from Edith Cowan University (ECU). This participant provides advice on the operational effectiveness of PPS and facilitates training in the operating of such systems, including all components within the system which contribute to achieving the overall design goals of specific systems.

Participant two has worked within the security industry and specifically around PPS for fifteen (15) years within the corrections environment. This participant holds a Bachelors Degree in Security Science from Edith Cowan University (ECU) and in his professional capacity, provides advice on the operational effectiveness of PPS and on a daily basis monitors for effectiveness.

Participant three has worked within the security industry and specifically around PPS for over twenty (20) years with both customs and within the corrections environment. This participant holds a Bachelors Degree in Business Management and in his professional capacity provides supervision and advice relating to the daily management of both staff operating PPS and the management of the maintenance reporting of PPS.

6.3 Pilot Panel interview questionnaire analysis

The theory of entropic security decay is framed around a functional, operational definition of security where security is defined as "*A stable condition stemming from a systematic process which effectively combines people, equipment and procedures, within a security context, to restrict unauthorised access to either people, information or physical assets through their ability to deter, detect, delay and respond to attacks which may lead to loss of, or, harm to protected assets manifested by a malevolent human adversary/s who seek/s to gain a level of unauthorised access"*. This definition is focused towards the integration of all heterogeneous security centred measures towards the establishment of a "systems" approach in implementing effective security controls. In-line with Patton (2002, p. 454), (Section 5.8), this analysis was achieved by drawing on an inductive process, discovering themes categories which emerge from the collected interview data.

To achieve the pilot study each panel member was met individually. The aims and benefits of the study were discussed with each participant, and their voluntary status established. Conforming with Section 5.7.2 Ethics, each panel member was asked to complete the informed consent documentation (Appendix A). After informed consent was established in writing, the interviews took place, taking approximately 1 hour and 30 minutes each for the first round, and approximately 30-40 minutes for the feedback interview. For some panel members the feedback process was achieved utilizing e-mail and telephone interview due to their professional commitments.

6.4 Interview Questionnaire Analysis

6.4.1. Question One: Security's organisational role

Questions one of the semi-structured interview questionnaire (Appendix B) asked panel members to state what, from their experience, the role of security is within an organisation, that is, the systems purpose. This question related to the functional approach towards security, discussed in Section 2.1.3 Security defined, and sought to consider the validity of this thesis's functional, focused approach to security. This approach sought to validate the removal of attached disciplines such as safety from the security function at the tactical level of management to enable a concentrated approach towards discussing, explaining and defining security decay functionally and across all three levels of organisational management (strategic, tactical and operational).

In response to this question, member one stated that security relates to the protection of assets, including procedural controls, physical components and electronic aids. The aim is to implement measures to deter, detect, delay, and respond to organisation specific threats. Panel member two responded with a similar theme stating "security's role is the protection of assets", adding, "Security is the practice of ensuring the protection of: human, physical or proprietor (information) assets, in a holistic manner to minimize the gaps in the protection of assets". This holistic approach is achieved by physical means, technologies and procedural controls. This theme was also reported by panel member three, who responded "to safe guard resources including: people, property and information.

For this panel a consensus was reached that security at the "tactical level" of management, relates to the holistic implementation of procedural, physical and electronic measures which aim to protect an organisation's assets which includes people, information and physical property through their ability to deter, detect, delay and respond against organisation specific threats.

6.4.2 Question two: Security's organisational purpose

Question two sought to establish whether the pilot panel viewed security's role as a risk reduction role, in-line with Section 3.4, Security and Risk Management. This question considered the strategic role of the system, where it is argued that as the operational and tactical aspects decay, so does its strategic aspect.

To this question all panel members agreed that security is a risk reduction role, where panel member one stated "without effective controls people would conduct acts against the organisation". In addition, panel member two added that security's role is also a deterrent role. A consensus was reached amongst the pilot panel that security is a risk reduction role and a deterrence factor towards preventing security related incidents.

6.4.3 Question Three: Security's body of knowledge

Question three asked panel members how they apply security's body of knowledge including theories, principles and specifically Defence in Depth. Panel member one responded that the theory of defence in depth is how he employs security's body of knowledge, stating "all elements need to be holistically implemented utilizing technology, physical components, people and procedures". Panel member two added, regardless of context, that is, the protection of people, information and assets, defence in depth is the salient strategy. In addition, panel member three stated that Defence in Depth within a cost benefit process where the benefits must achieve a prescribed value, is how he employs security's body of knowledge. A consensus was reached amongst the pilot panel that Defence in Depth, applied holistically in a manner which includes all elements is the salient and consistent strategy/means of employing the security body of knowledge.

6.4.4 Question Four: The systems approach to security

Question four asked panel members if they supported a systems approach to implementing effective security. All panel members provided an affirmative response to this question, achieving a consensus, with all panel members reporting that they support

a systems approach towards achieving security risk reduction. This consensus is consistent with the literature reviewed in Section 3.1 (Chapter 3), an open Systems Approach to physical protection. The systems approach was recommended by many published security professionals. It is the systems approach to security risk reduction which frames this research's approach to understanding security decay.

6.4.5 Question Five: Defining systems

Question five explored panel members understanding of a system in relation to Sections 2.2.9, the systems approach to physical protection, Section 3.1, an open systems approach to physical security, and Section 3.2 defining a Physical Protection System (PPS). This question asked panel members to explain their understanding of a system. To this question panel member one stated "a systems approach relates to how risks can be holistically reduced through the interrelation of all security controls, together". For this question panel member two responded, a system relates to how separate components are combined together to achieve an overall goal. Panel member two suggested that for security, this relates to the separate security components and theories combined to create a more robust security strategy. However, panel member three considered that a system considers the combination of people, processes and resources to achieve a purpose.

A consensus was achieved amongst the pilot panel that, a systems approach to security relates to how risks can be reduced through a holistic approach, interrelating the separate components which combine together to achieve an overall goal. A common theme in panel member's responses was how separate components combine and interrelate to achieve a goal. The panel member's views' pertaining to this question are accordant with Sections 2.2.9, 3.1 and 3.2 (Chapters 2 and 3) of the study and indicates that consistent with this literature the panel have a good understanding of what constitutes a system.

6.4.6 Question Six: A micro-macro relationship

Question six asked panel members if they consider the relationships between a system's micro state and its macro state. This question aimed to establish whether it could be interpreted that panel members, accordant with Sections 4.3.1, System sensitivity, support the argument that security systems effectiveness can be become degraded through the reduction in effectiveness of individual components (microstates). In addition, Section 4.3.3, Entropic decay defined, specifically considers such interrelationships between the systems microstates and its macro-state.

Panel members one and three both stated that they do consider this relationship; however, member two expanded on this response, stating "yes", there exists a serious relationship between all components of a defence in depth system, where each component is useless without its interrelations". A consensus was reached amongst the pilot panel that in considering a system, a serious relationship exists between the systems microstates and macro-state, and that this serious relationship does exist within a Defence in Depth system, where each component within the Defence in Depth system is useless without its interrelationships.

6.4.7 Question Seven: System interrelationships

In considering the systems approach in detail, specifically the various relations between the microstates and macro-state question seven asked panel members what they think this involved. Panel member one stated that he considered the relationships between the systems *micro states and its macro-state* involves the interrelations between the various individual components which make up a security program towards the achievement of the systems overall output goal. For this question panel member two stated "this involves specifically the interrelationships within the system". In addition, panel member three stated "this involves the breaking of the system down into its micro component parts to evaluate it with regards to the systems macro purpose".

This question relates to the literature discussed in Sections 2.2.5, Different Types of Systems, and Section 3.1.3, Systems Performance. A consensus was reached amongst the panel that this involves the interrelationships between the various individual components within the system, where it was reported that such consideration requires the system to be broken down into its component parts (microstates) for evaluation

(analysis), then combined (subjected to a synthesis process) for purpose evaluation (macro-state).

6.4.8 Question Eight: The Butterfly metaphor

A concept termed the "Butterfly Effect" is a significant principle within systems literature (Lorenz, 1963; 1968; Peirce, 2000, p. 5), and is used in this research to explain how decay propagates through a Defence in Depth System. As such, question eight asked panel members if they agree with the principle that small changes within a specific part of a system can lead to a large change at the output of the system.

Panel member one responded "yes", that he does agree with the principles underpinning the "Butterfly Effect". Panel member two also supported the application of this principle to security, and stated "There was a nexus between every single component within a defence in depth system, and if there is a small change, this changes the whole system". Panel member number three also supported the use of the "Butterfly" metaphor, stating "A small bit of change in any system has an overall change down the track through the system". A consensus was achieved amongst the pilot supporting this premise of systems theory relating to the principle of the "Butterfly Effect".

6.4.9 Question Nine: Physical security and key performance indicators

In considering the systems approach towards security risk reduction it is argued within the systems literature that "the ultimate aim is to discover those components whose measures of performance truly relate to the measures of performance of the whole system". As such, question nine asked panel members that, based on their understanding of a systems approach and their industry experience, what they believed the key performance indicators are within a Physical Protection System (PPS).

In response to this question panel member one responded that the initial focus for the systems key performance indicators is the detection system, specifically, the probability of detection is a key performance indicator. In considering this key performance indicator, panel member one states "the system must be set to minimize false alarms". In addition, after detection panel member one considered the delay aspects of the system are the next key performance indicators, where this overall key performance indicator must be linked to your response time and capabilities over all key performance

indicator. Panel member one considered that response times across the facility must be tested for both their time of arrival and efficacy against the systems defined threat.

For this question panel member two responded that a system's key performance indicators relates to the security time line, which starts at the commencement of the attack. As such, the first system key performance indicator is the detection function of the system. According to panel member two, after detection the next key performance indicator is the accurate assessment of the alarm source, then a key performance indicator relating to the communication of a genuine alarm event to a response force must be included. Once successful communication has occurred, panel member two considered the next key performance indicator is the systems delay time, followed by the response forces arrival time. Panel member two stated "in establishing these two key performance indicators the delay time must exceed the response forces arrival time key performance indicator".

In his response to this question, panel member three responded that the systems key performance indicators relate to the percentage of error in the system. The key performance indicators start with the detection function, then accurate alarm assessment, then successful communication followed by physical barrier delay time in relation to actual response time.

A consensus amongst the pilot panel was achieved listing the PPS key performance indicators in sequential order as: The initial detection of an unauthorised intrusion, the accurate assessment of such an alarm event, then communication of an intruder at a location to a responding person/group. Following the detection sub-system, the next key performance indicators are the sum delay time impeding the progression of the intruder, and the responding forces arrival time to interrupt the intruder, and where required the response forces ability to neutralize the threat based on the systems defined threat.

6.4.10 Question Ten: Key performance indicators and system effectiveness

Question ten asked panel members if, based on their experience, they believe the key performance indicators of a PPS are related to the systems overall effectiveness. Panel member one responded that he did believe the key performance indicators of a PPS are related to the PPS's overall effectiveness. Panel member one stated, "Each component

of the system is given score, and then, the overall system is given a score. Once this overall system score has been achieved it provides a benchmark of the system for future audits". For this question both panel members two and three agreed that the key performance indicators of a PPS are related to the PPS's overall effectiveness. All panel members responded positively to this question, providing a consensus amongst the pilot panel, that they believe the key performance indicators of a PPS are related to the systems overall effectiveness.

6.4.11 Question Eleven: Security decay

Question eleven asked panel members if, based on their experience, do they believe that security systems decay. This question related to Section 4.1, Physical System degradation, which postulates that, based on the available literature, all physical systems, if left to themselves', move towards a state of decay. That is, maximize their entropy. All panel members responded yes to this question, providing a consensus within the panel that, based on their experience, the panel believe, in-line with this research's literature review, security systems suffer from decay.

6*.4.12 Question Twelve: Understanding security decay*

Question twelve explored each panel members understanding of Security Decay in relation to the literature review and asked panel members what their understanding of Security Decay is. For this question panel member one stated that decay relates to many facets of the PPS. These facets include a failure to maintain systems at their operational level in order to deliver the required output for the system. This includes failures towards engineering controls maintenance, where failures to maintain these controls to a standard and monitor the systems maintenance to such standards causes technical based system decay.

Furthermore, panel member one considered that a lack of system spare parts and adequate redundancy processes for spares triggers extended time lags between systems faults being reported and proper repairs being carried out; to re-instate commissioning levels of operation, leading to decay. Panel member one considered that such time lags leave the security system vulnerable to technical attack during these periods. In addition, panel member one considers decay to be related to the people component of the systems as well, stating that a failure to maintain system commissioning levels of

training over time, beyond initial contractual obligations, leads to decay throughout the PPS overall effectiveness.

Panel members two and three were asked whether they agree with panel member one's views relating to the concept of Security Decay, where a consensus was achieved with panel members two and three supporting panel member one's views relating to Security Decay. Furthermore, Panel member two responded that Security Decay relates to the slow continuing degradation of components of a security strategy, which ultimately makes redundant that specific component as it relates to the system as a "whole". During the feedback process panel members' one and three reported that they supported panel member two's view towards the concept of security decay. A consensus was reached amongst the panel with regards to panel member two's views, with panel members' one and three agreeing with panel member two's views relating to these aspects of security decay.

Furthermore, panel member three stated that any specific single part of the system can decay, where this decay affects the rest of the "system". During the feedback process panel members one and two reported that they agree with panel member three's views relating towards security decay. A consensus amongst the pilot was achieved, that in-line with the heterogeneous aspect of a PPS, any specific single part of the system can decay, and based on the systems interrelationships, this decay affects the rest of the system.

6.4.13 Question Thirteen: An experience approach to Security decay

Question thirteen sought to achieve an evidence based approach, exploring real world examples of a time when panel members' had experienced security controls degrading. This question asked panel members to provide an example of a time when they experienced security decay.

For this question both panel members one and two responded that they had experienced system degradation, which had impeded the key performance indicator relating to the probability of accurate assessment. According to panel member one, he experienced a time when decay, manifested in the security systems lighting sub-system, had lead to a diminished ability to reliably assess (discriminate) alarm events initiated by the systems intrusion detection system. Panel member one reported that this specific decay

ultimately impacted on their ability to guarantee an effective interruption based on the theory of Defence in Depth.

Panel member two reported that he had experienced a time when specific sub-system degradation had also impeded the key performance indicator relating to the probability of accurate assessment (discriminate). According to panel member two, system degradation within the detection sub-system's performance resulted in a very high nuisance alarm rate. This high nuisance alarm rate lead to control room operators assuming that all incoming system alarm inputs were false alarms, ignoring them. This ultimately diminished the probability of accurate assessment key performance indicator through procedural breakdown, meaning the remaining system was worthless.

During the feed-back process panel member three was asked if he had experienced such decay manifestation and whether he identifies with panel member's one and two's experience. Panel member three identified with this experience, establishing a consensus that specific component decay can negatively impact on one of the systems key performance indicators. This provides a consensus amongst the panel that decay does occur, and can manifest in individual components, affecting specific key performance indicators, which, based on the PPS interrelations, affects the systems macro-state output product.

Furthermore, during the feedback process panel member one stated that if the key performance indicators are not maintained then the overall PPS is vulnerable, and in some cases worthless. This view is compatible to Section 4.5, Security decay and risk management, where the result of decay interlinked with Section 3.4.2, Defining risk, is the direct change in vulnerability state, purporting that Vulnerability = 1 – Pi, indicating a systems framed mathematical link between system effectiveness and system vulnerability. Panel member one's statement supports such a mathematical relationship, stating that as system performance decreases, vulnerability increases.

6.4.14 Question Fourteen: A systems approach to security decay

Question fourteen related to the systems approach to implementing effective security controls and asked participants how security controls degrade within a systems approach. According to panel member one, if one component fails, its key performance indicator is reduced and such individual component failure reduces the effectiveness of

the response force key performance indicator, ultimately reducing the overall protection process. Panel member two stated “the systems approach relies on all components working correctly where component change due to decay changes the whole system”. Furthermore, panel member three responded that consistent with the systems approach which combines people, procedures, technology and physical components into a system, the effects of the environment on the system contributes to decay, where changes in aspects such as the degradation of components, routines and procedures due to environmental influence contributes to decay.

A consensus was achieved with regards to how decay occurs in a system from a causation focus. According to panel member three, decay is the result of whole system pressure on the various heterogeneous components, stating that environmental effects on systems contributes to their decay at the component level. In addition, total system degradation can occur when people change their procedures affecting the human-technology coupling. This view of decay may explain how from a systems approach, how various influences on different aspects of the system can manifest and impact on the systems macro-state output.

6.4.15 Question Fifteen: Error propagation in Physical Protection Systems

Question fifteen related to the interrelationship aspect of systems thinking, and asked participants if they agree with a premise within the theory of entropic security decay that the concept of decay within a PPS occurs within the individual constituents, within the PPS, and its effects propagate through the system from this point. This aspect of security decay was discussed in Section 4.3.2, the effects of entropic decay on PPS. Panel member one supported this aspect, stating “if one process was not working properly this degradation affects the overall process down the line”. In addition, panel member one stated “such degradation also affects the deterrence aspect of the system”. For this question both panel members two and three responded that they agree with this premise, within the theory of entropic security decay, that decay within a PPS occurs within the individual constituents, within the PPS, and its effects propagate through the system from this point.

During the feedback process, a consensus was reached amongst the panel, supporting the argument that decay does occur within a PPS at the component level, within the

system individual constituents, which then propagates through the remainder of the system from this entry point, or point disturbance.

6.4.16 Question Sixteen: The Butterfly effect

Question sixteen related to aspects of systems decay discussed in Sections 2.2.4, Butterfly Effect, and 4.3.1, System Sensitivity, specifically an effect referred to as the "Butterfly Effect". This effect considers how small changes within a system can result in large changes at its macro output.

To this question, panel member one responded that he agreed with this premise within a systems approach to implementing effective security controls. For example, according to panel member one, he had encountered the result of this effect during a security audit. According to panel member one, he had inspected a high risk work place, where to reduce specific risks the organisation had installed staff emergency duress buttons to be activated if staff felt threatened. However, during the audit he discovered that individuals on staff, in the locations the duress buttons had been installed, did not know either about them or how to use them. Panel member one reported that for him, this experience supports the application of the butterfly effect to PPS. Since staff did not know about the system or how to use it, there would not have been any response to assist them should the need have arisen. Panel member one stated this experience supports his earlier statement that decay in security training ultimately leads to more holistic security decay.

Panel member two responded that he agrees with the premise that small changes within a system, specifically a security system, can result in large changes at the system's macro output. According to panel member two, he experienced a time where individual staffs reduced alertness levels and vigilance stemming from ongoing boredom had resulted in the systems key performance indicators becoming reduced in their effectiveness, specifically reducing the capacity and effectiveness of the system's response force.

Panel member three also reported that he agrees with this principle within systems theory. Panel member three reported experiencing a time where high numbers of system faults resulted in staff losing their confidence in the system. This lost confidence resulted in the overall system becoming vulnerable, weakening the overall protection

system. Panel member three provides the example of PTZ camera faults diminishing the capability for staff to accurately assess alarm causes, leading to decay in this area of the system (probability of assessment). Based on these responses, a consensus was achieved amongst the pilot panel that this aspect within the systems literature does relate to PPS.

6.4.17 Question Seventeen: The effects of security decay

Question seventeen asked panel members, what they consider the effects of decay are. To this question panel member one responded that decay is similar to an apple rotting, where its effects result in whole system not working properly, directly impacting on individual sub-system key performance indicators. However, panel member two focused on the strategic goals of the system, stating "decay ultimately diminishes the security objective". According to panel member two, security decay increases the vulnerability of the asset being guarded/secured. This increased vulnerability modifies the risk equation, where likelihood ratings become elevated and risk factors become increased.

Panel member two's views were supported in panel member three's response. According to panel member three, decay degrades the effectiveness of the "system"; therefore the risks associated with the asset being protected are increasing rather than being decreased. A consensus was reached amongst panel members that, in-line with previous responses, decay at the component level results in the gradual degradation of systems individual key performance indicators, reducing individual subsystem's commissioning key performance indicator scores. This aspect of security decay was discussed in Section 4.4, The Measurement of Security Decay. Furthermore, a consensus was reached amongst the panel that decay at the macro-level results in a diminished security objective, where the risks being treated/reduced are increased due to the effects of decay which force changes to the facilities risk equation where likelihood and vulnerability ratings become elevated diminishing risk reduction.

6.4.18 Question Eighteen: Correcting security decay

Question eighteen related to security systems management and asked panel members if they believed that once decay had set in, whether its effects, both at its point of manifestation and throughout the remainder of the system are reversible. Panel member one responded that he believed the effects of decay could be reversed; however,

qualified this with the belief that this process of reversal was dependant on the availability of resources and how far the system had decayed. For this question panel member two agreed with panel member one, reporting that he did believe the effects of decay could be reversed, however, according to panel member two, this would require a full systems audit to facilitate locating the point of decay within the system. For this question panel member three responded that he did believe the effects of decay could be reversed through proper maintenance of the systems components. All panel members responded yes providing a consensus within the panel that the effects of decay can be reversed, once decay was located.

6.4.19 Question Nineteen: Avoiding security decay

In considering the ability to reverse the effects of security decay, question nineteen explored whether panel members' opinions whether decay could be avoided. All panel members agreed that decay could be avoided through active monitoring of the system. For example, panel member one stated "decay could be avoided through proper maintenance, with systems components maintained at agreed operating levels in a timely manner".

In addition, panel member one considered that decay could be avoided through proper planned maintenance, scheduled redundancy management, ongoing education and awareness training relating to the system holistically, so that individuals understand the system fully. For this question panel member two considered that decay can be avoided at the initial stage (design stage) of the security project through the implementation of an effective system, which is actively monitored and reviewed utilizing a systems based auditing process. However, panel member three considered that security decay is inevitable to a point, as a system has a life span. Therefore after a period of time processes must be put in place to reduce decay.

Furthermore, it was established that decay, to a point, can be avoided through full systems based audits which focus on individual system aspects/components and their interrelationships. In addition, it was agreed that decay up to a point, could be reduced through the designing of an effective and suitable system from the beginning, where factors such as environmental and budgetary influence can be considered when systems would be designed to minimize decay.

6.4.20 Question Twenty: Security decay and risk management

It is argued in the literature that security is a risk reduction role and a consensus amongst the pilot panel was achieved supporting that security is a risk reduction role. As such, question twenty asked panel members if they believed the concept of decay has a place in the risk management formula.

All panel members responded affirmatively, stating that the concept of security decay has a place in the risk management formula, specifically in the monitor and review stage of the risk management formula. These responses provide a consensus that the concept of security decay should be considered in the monitor and review process of the risk management formula. This finding is in-line with the discussion from Section 4.6 Avoiding and countering entropic security decay, where Standards Australia HB 167 (2006, p. 87) incorporates a monitor and review stage in the security risk management process.

6.5 Interpretation

Security is a multi-disciplinary industry (Brooks, 2007, p. 1) and Physical Protection Systems (PPS) are heterogeneous, where such parts are brought together to achieve an output goal. To achieve this output goal a PPS aims to (A) deter, (B) detect, (C) delay and (D) respond to security events. Congruous with Section 4.3, the theory of entropic security decay, the sum of detect, delay and response (BCD) leads to A. In addition, for an adversary, Detect (B) (Action) and Delay (C) (Interaction) leads to Response (D) (Consequence). These interrelations are achieved utilizing people, procedures, and technology and physical properties. These combined phenomena draw on many heterogeneous categories with varying domain specific specialization, achieved by putting resources through a process to achieve an output function. Figure 2.6, Section 2.2.6.2, Open systems, and Figure 3.6 Section 3.2 Defining a physical protection system, indicate this process. Such a process is accordant with the principles of General Systems Theory (GST) which provided the scientific systems frame for the study.

6.5.1 Research sub-question one.

General Systems Theory (GST) is a meta-disciplinary approach towards understanding systems of all types, regardless of purpose or make up, and provides the skeletal frame of enquiry towards discussing, explaining and defining the phenomenon of security decay. As such, based on the heterogeneous nature of Physical Protection Systems

(PPS) research question one stems from GST's approach and seeks to investigate whether security experts support such a systems framed approach to implementing effective security controls accordant to the principles of GST.

In responding to the study's research question, sub-question one asks: *Do security experts support the systems approach to implementing effective security controls?*

The aim is to interpret whether panel members support a General Systems Theory (GST) approach, as it applies to physical security, to implementing effective security controls. Congruous with Patton (2002, p. 454) (Section 5.8) this interpretation will be achieved by drawing on the conceptual review of literature as an existing benchmark to deductively test and affirm the research data in response to the sub-questions. This interpretation will be framed around the core principles underpinning GST as they apply to physical security, and will involve comparing the inductive analysis from panel interviews with the literature drawn from the study's benchmark (Chapters 2, 3 and 4).

6.5.1.2 Research sub-question one Interpretation

All panel members responded "*yes*" that they support a "systems approach" to implementing effective security. Their response is accordant with the writings of Underwood (1984, p. xi; Fennelly, 1997, p. 59; Garcia, 2001, p. 6; Fisher & Green, 2003, p. 164). For example, according to Fisher and Green (2003, p. 147) every security program must be an integrated "whole", where Underwood (1984, p. xi) adds, and seen as a "whole". In exploring the panel's understanding of a systems approach, the pilot panel reported that a systems approach to physical security relates to how risks can be reduced through a holistic approach, interrelating the separate security components which combine together to achieve an overall design goal. For example, member two stated "*a system relates to how separate components are combined together to achieve an overall goal*". Furthermore, according to member three, it includes people, processes and resources which combine to achieve a purpose. Such a viewpoints are congruous with Bertalanffy (1968, p. 19) who considers a system to be "a set of elements standing in interaction".

Congruous with the writings of Bertalanffy (1950; 1968) the pilot panel reported that within a systems approach, a serious relationship exists between the systems micro-states and its macro state. Uniform with the systems literature the panel considered that

each component within a system is useless without its interrelationships, where all panel members responded "*yes*" when asked if they consider the relations within a system. For example, member two stated, "*A serious relationship exists between all components of a defence in depth system, where each component is useless without its interrelations*. This viewpoint is consistent with Midgley's (2003) who states "the systems approach is focused strongly towards the interrelationships within, where, it is these interrelationships which tie the system together".

Consistent with Midgley's (2003) viewpoint the panel reported that a systems interrelations involve the relations between the various individual components which collectively make up a security program towards the achievement of the systems overall output goal. For example, members two and three stated;

> "*this relates to the interrelationships between the carious individual components which make up the whole security program and the achievement of the system's overall goal or output function*". Where member three stated, "*such interrelations involve breaking the system down into its micro component parts to evaluate it with regards to the systems macro purpose*".

Such viewpoints are congruous with the writings of Bittel (1978, p. 1130) who considers the systems approach to be "sets of interrelated components that function together within constraints towards a common purpose".

In considering the panel's support towards a systems approach, Checkland (1980) stated that all physical systems are created for a specific purpose. In determining the systems purpose within a physical security context, the pilot panel agreed that from a functional perspective, security, therefore the "security system's" purpose, relates to the reduction of an organisation's risk. It was argued that such reduction is achieved through the holistic implementation of procedural, physical and electronic measures which combine to protect an organisation's assets which includes people, information and physical property through their ability to deter, detect, delay and respond to adversary threats. For example, member one stated "*I employ the theory of Defence in Depth where I consider that all elements need to be implemented within a holistic approach including procedures, barriers and electronic systems*". Member one's view was supported by member two who stated "*I see Defence in Depth as the salient strategy towards protecting any asset including information, physical or people*". Consistent with this

consensus, the panel reported that the salient approach to reducing security risk concerns was the employment of the theory of Defence in Depth, as a "system".

The panel's consensus conforms to the writings of Smith (2003, p. 8) and Standards Australia (HB 167: 2006), Security Risk Management, which states, "In addressing security risk concerns, the key elements of organisational, community and individual security controls are those components which contribute to the management of risk through their ability to deter, detect, delay, respond to and recover from adversary attack". In addition, member two stated that "*as well as a risk reduction role, security (the system) has a deterrent role*". A view supported by panel member one who stated "*without the controls people would conduct acts against the organisation*". Furthermore, in applying security's body of knowledge towards achieving an effective security state, all panel members supported the view that the parameters achieving defence in depth (levels of detect, delay and response) must be based on a defined threat, that is, based on risk.

In responding to sub-question one, one of the underpinning principles of systems thinking is found in the writings of Chruchman (1968, p. 43) who stated "within a systems thinking approach, the ultimate aim is to discover those components whose measures of performance are related to the measure of performance of the whole system, where a systems performance is proven by providing objective evidence of its effectiveness". Accordant with this principle the pilot panel reported that they believe the key performance indicators within a PPS are related to the systems overall effectiveness. For example, members three and one stated;

> "*the systems key performance indicators relate to the percentage of error in the system*", where according to member one "*each component of the system is given a score*". "*Once the overall systems score has been established, it provides a benchmark of the system for future audits*".

This approach indicates support towards the quantitative aspect of systems theory and specifically the quantitative approach to security decay, where the panel reported that within a systems approach to physical security the key performance indicators for a PPS in their sequential order are: the initial detection of an unauthorised intrusion, the accurate assessment of such an alarm event, the communication of the event to a responding force/group. Following the detection sub-system, the remaining key

performance indicators are the sum of delay time impeding then adversary's progression, and the responding forces arrival time to interrupt the intruder, and where necessary, the response forces ability to neutralize the threat, based on the systems defined threat. The panel's views relating to PPS key performance indicators are compatible to the writings of Garcia (2001, p. 6) who states "the performance measures of a PPS, within a systems approach, are a complex configuration of detection, delay and response elements, where the best effectiveness measure (macro state) for a PPS is one which combines these functional elements into a "whole" (Garcia, 2001, pp. 242-249).

The panels viewpoint towards the systems key performance indicators is compatible with the writings of Barton and Haslet (2007, p. 145) and Holton (cited in Barton and Haslet, 2007, p. 145) who state, "in science, analysis must precede synthesis, based on the argument that without a previous analysis, attempting synthesis does not lead to truth", where Ritchy (1991, p. 10) considered that every synthesis is built upon the results of a proceeding analysis, where every analysis requires a subsequent synthesis in order to verify and correct results. To this aspect of science Barton and Haslet (2007, pp. 147-148) explain that systems thinking involves, and provides a distinct means of framing this dialectic where systems thinkers recognize that individual (analysis) events are part of a pattern (synthesis) of events.

Congruous with the writings within the study's documentary analysis the pilot panel agreed that based on the interrelationships within PPS which achieve its macro-state output, small changes within a specific part of a system can lead to a large change at their output. For example, member two stated that "*I believe there is a serious nexus between every single component within a defence in depth system, and if there is a small change, this changes the "whole" system"*. Such a viewpoint is uniform to Waldman's (2007, p. 272) who stated, "as part of a system changes, the nature of the overall system changes". Waldman's (2007, p. 272) standpoint was depicted by member three who stated "*a small bit of change in any system has an overall change down the track through the systems*". This aspect of systems interrelations is what Lorenz (1968, p. 306) referred to as the "Butterfly Effect", which describes how error propagation occurs within a system.

It is argued that the panels support towards applying the "Butterfly" principle to physical security is considered in the writings of Konicek and Little (1997, p. 18; Garcia, 2006, p. 26; and Standards Australia HB167, 2006, p. 62). For example, Konicek and Little (1997, p. 18) state, "a security systems is only as good as its parts, when a single part fails, this failure can cause degradation of the total system. In addition, Garcia (2006, p. 26) states, "System effectiveness can become degraded through the reduction in effectiveness of individual components", where according to Standards Australia HB167 (2006, p. 62) a small change in control effectiveness may have a substantially magnified effect on vulnerability. In considering the Butterfly principle, according to Churchman (1968, pp.42-43) Lorenz's (1963; 1968) works are considered in many variations of systems theory, where the systems approach is based on the premise that as individual measures of performance of constituent components increase, so does the holistic measure of performance of the total system.

6.5.1.3 Research sub-question one deductions

The panel reported that they support a systems approach to implementing effective security. For example, all panel members responded "yes" to this question. Analysis of the interview process indicates that the pilot panel's views relating to the implementation of effective security controls are congruous with the underpinning principles of General Systems Theory (GST) applied to the theory of Defence in Depth. That is, the panel recognise the systems purpose, its functions and its architecture within a GST frame. In addition, accordant with the GST approach the panel comprehends the various interrelations, organisation and orderly aspects which achieve the systems output goal. Furthermore, the panel understand how, based on the systems interrelating aspects, small changes in one area of a system are associated with changes throughout the remainder of the system, and how these changes directly affect the various sub-systems and "whole" systems macro-state (key performance indicators). Based the available data, it is argued that the evidence supports an interpretation that the pilot panel do support a systems approach within a GST frame to implementing effective security controls.

6.5.2 Research sub-question Two

Research sub-question two directly relates to the premises of Underwood (1984) and McClure's (1997) writings, where according to Underwood (1984, p. xi) "security decay" is the most serious threat to a security systems, and "security decay" must be

expected. Research question two asks, "Do security experts support the argument that security systems can suffer from decay"?

In response to research sub-question two, the aim is to interpret whether panel members support the argument that "security systems" suffer from decay. Congruous with Patton (2002, p. 454) (Section 5.8) this interpretation was achieved by drawing on the conceptual review of literature as an existing benchmark to deductively test and affirm the research data in response to this research question. The interpretation was framed around the panel's understanding of, and real world experience (evidence) relating to decay within Physical Protection Systems (PPS). This interpretation will be achieved by comparing the data analysis of the panel interviews to the embodying literature presented in the conceptual review of literature (chapters' two and three).

6.*5.2.1 Research sub-question Two Interpretation*

Congruous with the works of Underwood (1984, p. xi; Howlet, 1995, p. 222; McClure, 1997; King, 2008, p. 1) the panel reported that they believe "security systems" suffer from decay, with all panel members responding "*yes*", where member three emphasized "*yes definitely*". The results of this question are accordant with King (2008, p. 1) who applied Lovey and Manohar's (2007, p. 99) and Styer's (2000, p. 1) views to explain the decay of physical protection systems, stating that security controls inevitably degrade over time as a result of natural entropy.

In responding to sub-question two, the pilot panel provided their understanding of security decay. For example, member one stated;

> "*security decay relates to a failure to maintain security systems at an operational level required to deliver their commissioned output capabilities*". This depiction was supported by member two who stated "*decay relates to degradation, that is, the slow continuing degradation of components of a security strategy which ultimately makes redundant that specific component as it relates to the system as a whole*".

These combined views towards security decay are uniform to the Australian Pocket Dictionary of English Language (1994) which defines decay as "a gradual decline" in; health, prosperity or excellence, a process of decline or deterioration, and the New Oxford Dictionary (1991) which defines decay as being less good or less strong.

Furthermore, within a General Systems Theory (GST) frame, the pilot panel spelt out that security decay relates to the *slow, continuing degradation* of, or decline in effectiveness of individual components which, based on their interrelations, affects the system as a whole, reducing its macro-state (Pi). That is, the systems approach to physical security relies of the effectiveness of each component interrelated with the effectiveness of other interrelated components to achieve a macro-state output goal (Pi). For example, according to panel member three "*any specific part of the system can decay, where this decay affects the rest of the system*". This viewpoint is consistent with Konicek and Little (1997), Garcia (2006) and Standards Australia HB 167, 2206).

In discussing their understanding of security decay, the pilot panel considered that security decay was as heterogeneous as the Physical Protection System's makeup. That is, a PPS combines and integrates as a "whole" people, procedures, physical measures and technologies to protect an organisation's assets, where decay relates to a failure to maintain such systems at their operational levels of effectiveness to deliver the required output goal. The pilot panel reported a number of real world examples where, based on their understanding, they have experienced aspects of security decay. For example, the pilot panel reported that security systems suffer from decaying training standards. This aspect of security decay relates to the systems approach which interrelates the categories of detect, delay and response to achieve the systems desired output goal through the utilization of people, procedures, technology and physical properties into a collective "whole". That is, a systems approach relies on an effective coupling of people, procedures and technology and this aspect of decay focuses on a gradual degradation in the effectiveness of this coupling impeding the achievement of the systems output goal.

Furthermore, panel member three suggested that either environmental effects, or changes to security operating procedures within PPS contributes to their decay. According to member three, changes in aspects such as component degradation, routines and procedures contributes to "total system decay". This response is uniform to an example offered by Broder (2006, p. 30) who states that he observed procedural decay to bypass perceived excessive access control strategies. According to Broder (2006, p. 30) to overcome perceived excessive access controls at a computer department of an airline, staff took to propping doors open for simplicity of movement during working hours.

In addition, the pilot panel reported that within a systems approach, if one component fails, its key performance indicator is reduced, and such component failure reduces the effectiveness of the response force key performance indicator, ultimately reducing the overall protection process. Panel member two stated,

> "*the systems approach relies on all components working correctly, where component change, due to decay changes the whole system".*

The panel's responses and views are congruous with the systems literature stemming from Waldman (2007, p. 272) who stated, "If a part of a system is changed, the nature of the overall system is often changed as well", where Midgley (2003, p. xxvii) points out, even the tiniest influence may have a major affect on the future of the system.

6.5.2.2 Research sub-question two deductions

In response to research sub-question two, the evidence indicates that a consensus amongst the expert panel supporting the argument that security systems do suffer from decay was reached. It is indicated that such decay relates to a failure to maintain security "systems" at their "operational levels of effectiveness" to deliver the required output goal (risk reduction).

6.5.3 Research sub-question Three

Research question three directly related to the premises of Coole and Brooks (2009), and focused on the heterogeneous aspects of the Physical Protection "System" (PPS) in response to writings of Lovey and Manohar (2007, p. 99) and Styer (2000, p. 1). Lovey and Manohar (2007, p. 99) and Styer (2000, p. 1) stated "all physical systems, if left to themselves, tend to maximise their entropy, in-line with the laws of thermodynamics", where according to Pitzer (1995, p. 30) entropy is an extensive property, where the entropy of a system is equal to the sum of the entropies of its parts. That is, the entropy of as system is a macro-state, where according to Konicek and Little (1997, p. 184) when a single part of a security system fails, such failure can cause degradation within the total system. As such, research question three asks "Do security experts support that security decay lies within the systems elements, constituents and their interrelationship"?

Conforming to Patton (2002, p. 454) (Section 5.8) this interpretation was achieved by drawing on the conceptual review of literature as an existing frame work to deductively test and affirm the research data in response to this question. This interpretation was

framed around the panel's understanding of how security decay occurs and the effects of its occurrence manifest, within a General Systems Theory (GST) frame.

6.5.3.1 Research sub-question Three Interpretation

A consensus was reached congruous with the conceptual review of literature indicating that security decay occurs at the component level (constituent) and that this affects specific sub-system key performance indicators. For example, member three stated "*any specific single part of the system can decay, where this decay affects the rest of the system*". Member two identified that "*Security Decay relates to the slow continuing degradation of components of a security strategy, which ultimately makes redundant that specific component as it relates to the system as a whole*". Such a viewpoint was also offered by member one who stated "*one subsystem process not working properly affects the overall process down the line*"

Furthermore, member one explained that decay relates to many facets of the PPS, which includes failures towards engineering controls maintenance, where failures to maintain these controls to a standard and monitor the systems maintenance to such standards causes technical based system decay. Member one states,

> *"a lack of system spare parts and adequate redundancy processes for spares triggers extended time lags between systems faults being reported and proper repairs being carried out to re-instate commissioning levels of operation, leading to decay".*

Panel member one considered that such time lags leave the security system vulnerable to technical attack during these periods. Member one's views are consistent with the writings of Howlet (1995, p. 220) who stated "a poorly maintained system will have numerous unexplained alarms and the guard force may lose confidence in it and eventually ignore it". In such a case according to Howlet (1995, p. 220) they may treat a genuine alarm as just another false alarm. This view was expressed by member three, stating "*eventually staff will lose confidence in that specific system*". In addition, Howlet's (1995, p. 220) writings support panel member three's example of CCTV decay, where panel member three gave an example of such decay within the mechanical aspects of a PTZ camera, where such degradation means that specific cameras cannot be used for assisting with alarm assessment purposes. According to Howlet (1995, p. 220) slow degradation of a CCTV monitor is not normally self evident.

The pilot panel reported that they believe the phenomenon of decay occurs within a PPS's individual constituents, and that such degradation at the constituent level, based on the orderliness interrelations, propagates throughout the remainder of the system. As member one stated "*with one sub-system process not working properly it affects the overall process down the line, where it also affects the deterrence aspect of the systems as well*". These responses are congruous with the literature stemming from Bertalanffy (1950; 1968; Konicek & Little, 1997; Waldman, 2007, and Garcia 2006, Mosely and Coleman, 2000, p. 101, and Broder, 2006). Such a view point is also congruous with the Gestalt approach to deterrence discussed in Section 3.1.1(Chapter 3). For example, member three reported that he agrees with the application of the "Butterfly Effect" to a PPS, member three states;

> "*high faults in one system affects the whole system where eventually staff will lose confidence in that specific system. This results in that specific aspect of the system becoming vulnerable within the system, weakening the overall system"*.

These collective views are true to the early works of Isaac Newton who stated, "The extension, hardness, impenetrability, mobility and inertia of every object, depends on, the extension, hardness, impenetrability, mobility and inertia of its component parts" (The Open University, 1976, p. 68).

The "Butterfly" metaphor has been used to articulate the interrelated aspects of specific systems. For physical security within a systems approach to security decay, it is argued that however decay is manifested in one component, its effects expand to affect that components effectiveness within the specific sub-system, and that this component degradation propagates throughout the remainder of the system, from its point of entry, based on the systems interrelationships. This view was supported by panel member two who explained that during a security review that he had conducted, he observed the capacity of the response force had degraded stemming from decayed training processes, and a lack of alertness and vigilance due to boredom, adding to the response forces arrival time and ultimately reducing the probability of interruption key performance indicator.

Panel member one supported member two's views, who considers decay to be related to the people component of the systems as well. Member two stated,

"*a failure to maintain system commissioning levels of training over time, beyond initial contractual obligations, leads to decay throughout the PPS overall effectiveness*".

For example, according to member one system degradation in security training leads to decay at the systems macro output level. Member one stated "*during security auditing in a high risk work place I found that individuals in the work place did not know of the existence of, or understand, how to use the staff duress system*". As such, should the requirement for external assistance eventuate, the response would be negatively impacted against, as staff may have to use alternative means for notifying the requirement for a security response, ultimately adding to the overall response time.

These views relating to security decay are compatible to Section 4.3.2, the effects of entropic decay on PPS. Section 4.3.2 purports the original decay within a PPS expands to the boundaries of that specific subsystem component, resulting in a failure within this specific part of the system. Based on the system interrelationships between the Defence in Depth elements individual failure results in the system becoming disordered, ultimately resulting in this point disturbance propagating through the remainder of the defence in depth system. In considering this aspect of security decay, all panel members supported the application of the "Butterfly" metaphor to PPS, where according to member one "*decay is like an apple rotting, with its effects resulting in the whole system not operating properly as per their individual key performance indicators commissioning scores, ultimately resulting in operators losing confidence with the system*". The loss in system confidence by operators was an outcome reported by Howlet (1995, p. 220).

According to member two decay results in a diminished security objective, ultimately increasing the vulnerability of the asset being guarded/secured. Member two stated, "*decay alters the risk equation, where likelihood becomes elevated and the risk factors become increased*". Such a view was also reported by member three, who stated "*decay degrades the effectiveness of the system, increasing the risks associated with the asset being protected rather than decreasing them*". These views are congruous with equation 28 (Section 4.5).

In addition, member one stated, "*one sub-system process not working properly affects the overall process down the line, where it also affects the systems deterrence aspect as*

well". The affects on the system's deterrence aspect was presented in Figure 4.2 (Section 4.5), where according to Walker (1988, p. 11) the psychological aspects governing offenders needs to persuade them that it is not worth trying an attempt against an asset because if they try, they will fail or be caught, in-line with Winoto's (2003, p. 2) rational choice formula. Whilst the pilot panel reported that they believe security system decay is inevitable to a point, they argued its affects could be countered or avoided through full system based audits which focus on individual system aspects/components and their interrelationships.

6.5.3.2 Research sub-question three deductions

It is argued that the available evidence indicates the pilot panel support the argument that security decay lies within the systems elements, constituents and their interrelationships. That is, all pilot study members supported that decay occurs at the constituent level, manifests, then expands to incorporate and affect specific sub-system key performance indicators, then expands to the specific defence in depth element for which it is located, then propagates throughout the remainder of the defence in depth system from that point, ultimately affecting the systems macro-state key performance indicator (Pi) based on the systems interrelations congruous with the writings of Bertalanffy (1950; 1968).

6.6 Pilot study Security decay preliminary item bank

Consistent with the writings of Loewanthal (2001, p. 3) Table 6.1 presents the pilot panel's preliminary pool of variables and factors associated with the concept of security decay. This item bank is underpinned by the panel's thoughts feelings and experience with degradation within Physical Protections Systems (PPS). Table 6.1 highlights the pilot panel participant's real world experiences and explanations relating to security decay.

Table 6.1 Pilot study Security decay preliminary item bank

Decay Categories	PPPS Components		
	Conditions	Phenomenon	Consequence
Technical	Poor maintenance, failing to maintain systems technical components at operational levels. This includes both scheduling and fault repairs.	Decay manifests in individual key performance indicators.	Specific element interrelations not achieved, significantly reducing the macro-state output key performance indicator.
	Specific sub-system key performance indicators not maintained.	Decay manifests in individual key performance indicators.	
People	Poor system management/supervision.	Poor monitoring leads to small changes in work practices.	Various sub-system KPI's are reduced due to lack of conscientiousness which propagates through the remainder of the system.
	People changing their procedures.	This decays the human-technology coupling as personnel don't fulfil their duties based on the desired KPI's.	
	Failure to maintain training standards overtime.	Decay relating to the technology-human coupling which is required in a complex system.	Total system effectiveness degraded.
Physical	Slow continuing degradation which contuse as it remains undetected.	This decay propagates through the remainder of the system.	Degradation of specific sub-system key performance indicators.
	Individual components decay.		
	Environmental effects on individual components.	Decays individual components, impacting on their sub-systems KPI's.	Degradation of whole system performance based on system interrelationships.

(Adjusted from Gillham, 2000, p. 68).

6.7 Adjustments to semi-structured survey questionnaire

Pilot studies enable researchers' to ascertain what worked well and what changes could be made to enhance the effectiveness, and depth to the study. The semi-structured interview questionnaire relating to the theory of entropic security decay was subjected to a pilot study to ensure that prior to engaging in the formal research component of this study the questionnaire was subject to test conditions congruent with those which the formal study would be subjected. As a result of this pilot study, in-line with Martin (2000), and (Gillham, 2004), a number of changes were recommended and implemented to enhance the semi-structured interview questionnaire effectiveness in drawing out responses which would contribute towards answering this study's sub- research questions and overarching research question.

The following changes were made to the research questionnaire:

The first change to the research questionnaire was the removal of the alphabetical sequencing and bulleted sub-questions to incorporate a simpler numerically sequenced interview questionnaire. It was considered that this change would facilitate a simpler interview questionnaire to administer and report findings. Based on the numerical sequencing of the interview questionnaire, question three's (3) wording was slightly changed to: Can you tell me how you apply security's body of knowledge, including security methodologies and concepts? If participants do not mention the application of the theory of defence in depth, then the question; do you use the theory of defence in depth will be asked. Table 6.2 displays the remaining changes that were incorporated into the semi-structured interview questionnaire:

Table: 6.2 Semi-structured interview questionnaire changes

Question No.	Question wording changes
4	Can you please explain to me your understanding of a system? Do you consider the relationships between the components and the goal of the system?
5	Do you support a systems approach towards security? Yes/No.
6	What do you think the systems approach towards security involves?
7	According to the principles of systems theory small changes within a specific component can lead to a large change at the output of the systems. Do you agree with this premise? Yes/No Can you explain why?
9	Based on your experience, do you believe the key performance indicators of the systems are related to the systems effectiveness? Can you explain how?
11	What is your understanding of security decay;
13	In considering the argument that security controls decay, how do you think this occurs within a systems approach to security?
14	The concept of security decay argues that decay within a PPS occurs within the individual constituents, within the PPS, and its effects propagate through the system from this point. Based on your experience, do you support this premise Yes/No, why, why not?
15	Do you feel this applies to a PPS? Yes/No. Can you give me an example where you have come across this?
16	Based on your experience, what do you consider the effects of decay are?
17	Once decay has set in, do you think its effects, both at the point of manifestation and throughout the remainder of the system are reversible? Yes/No. How do you think so? Or, why don't you think so?
20	Based on your experience, is there any facet of security decay which you can add to the research enquiry? This may include factors associated with either the cause of decay or impacts from it.

6.8 Conclusion

This chapter presented the Pilot study with the aim of conducting a complete trial of the proposed methodology to both establish the feasibility of continuing into the main study

phase and to identify and rectify potential problems prior to commencing the resource intensive formal study. The findings from the pilot study were that the pilot panel reported support towards the three sub-research questions, where it could be interpreted that the panel support the argument that Physical Protection Systems (PPS) suffer from decay, and that such decay is manifested at the component level which then expands to that components specific sub-system, affecting this sub-systems key performance indicator. Then, based on the interrelationships within the system, propagates throughout the remainder of the system, therefore negatively impacting on the "whole" systems key performance indicator, and ultimately decreasing the implemented level of risk treatment.

The pilot study demonstrated the viability of the study, supporting the progression into the main study with minor changes to the semi-structured questionnaire. As such, this chapter presented a number of changes which were made to the semi-structured interview questionnaire towards enhancing data collection practices and processes, and towards drawing out deeper research data framing the concept of security decay.

CHAPTER 7

ANALYSIS: PANEL ONE

7.0 Introduction

This chapter presents the first stage of phase three of the study, research panel one (n=3) interview questionnaire analysis. The aim of this chapter was to produce a gradual growth in experienced based knowledge towards developing a deeper understanding of entropic security decay. To achieve a successful outcome, an inductive analysis was conducted with research participant responses providing an analysis suitable for deductive evaluation in Chapter 9 (Phase 4). As previously stated, to-date there is dearth of knowledge relating to the gradual degradation of security systems. The variables and factors underpinning the theory of entropic security decay are still under investigation, at the conceptual stage.

This chapter is broken into a number of sections, providing participant responses to the interview questions (N=20). Section 7.1 presents this study's research panel one participant's biographical information, establishing each participant as a security expert within their respective security domains. Section 7.2 presents the interview data inductive analysis which will be drawn on in phase four of the study to achieve the required deductive analysis enabling responses to the study's research question. Section 7.3 provides a reflection of themes and core principles which evolved from this panel interview data that will be taken forward to research panel two (Chapter 8). Section 7.4 concludes the chapter, presenting a summary of achievements.

6.1 Participants

Participants' for this research, in-line with Section 4.4 participant sample, consisted of peer nominated security experts (N=6) divided into two research panels, research panel one (n=3) (this chapter) and research panel two (n=3) (Chapter 8). These experts were selected and solicited to participate in this study based on the criterion that they are employed to provide security category knowledge advice across the varied security related occupations. Their selection was based on their extensive knowledge or ability, their experience, occupation and/or education and training others rely upon them for professional opinion within the multi-disciplined security industry and they were considered by their peers (peer revered) as experts, forming a non-probability (purposive) sample.

7.1.1 Research Panel One

Panel member one

Panel member one is a client relationship manager for a large security engineering organization. Panel member one holds an electrician's qualification, electrical technician's qualification and a Diploma of Applied Science. His area expertise and duties include security risk management and the design of technical, physical and procedural security controls to reduce various organisation identified risks. Once strategies have been identified, panel member number one leads the implementation of large scale security engineering projects to achieve client's risk reduction needs. Panel member one has over twenty (20) years experience in security risk management, and the technical design and implementation of capital works security projects.

Panel member two

Panel member two is the coordinator capital works projects for a correctional department. His duties and focus is the security aspects of capital works project management within the justice portfolio. He provides advice and project management services towards building, refitting and maintaining effective security infrastructure to ensure his organisation can meet its business needs. Panel member two served in the Australian Defence Forces for nine (9) years, has worked in customs in the area of strategic assessments (one year) and has been with the corrections department for approximately eleven (11) years. Panel member two holds a Bachelors Degree in Security with a minor study area in Management from Edith Cowan University in Western Australia.

Panel member three

Panel member three is the state-wide security manager for a correctional Department, whose region covers 2.5 million squared kilometres. This position provides security services advice towards maintaining the Department's Security Directorates business component. The position means that panel member three is required to implement and coordinate both physical security audits and procedural audits. In addition, the manager reports on security practices and emerging technologies and is required to ensure ongoing development of security risk management processes. Panel member three has been in this role for five (5) years, prior to this he worked in the security and emergency unit within the Corrective Services for approximately twenty (20) years.

7.2 Research Panel one interview questionnaire analysis

The theory of entropic security decay is framed around a functional, operational definition of security where security is defined as "*A stable condition stemming from a systematic process which effectively combines people, equipment and procedures, within a security context, to restrict unauthorised access to either people, information or physical assets through their ability to deter, detect, delay and respond to attacks which may lead to loss of, or, harm to protected assets manifested by a malevolent human adversary/s who seek/s to gain a level of unauthorised access"*. This definition is focused towards the integration of all heterogeneous security centred measures in the establishment of a "systems" approach in implementing effective security controls. In-line with Patton (2002, p. 454) this analysis will be achieved by drawing on an inductive process (Section 4.7), discovering themes categories which emerge from the collected interview data.

To achieve the data collection phase of the study each panel member was met individually. At the beginning of the interview the study's aims and benefits were explained to each participant, and their voluntary status was established. Concordant with Section 5.7.2 Ethics, each panel member was asked to complete an informed consent form. After informed consent was established in writing, the interviews took place, taking approximately 1 hour and 30 minutes each for the first round, and approximately 30-40 minutes for the feedback interview. As with the pilot panel, due to some panel member's professional commitments, some second round interviews were conducted utilizing e-mail and telephone interviews. However, where possible second round interviews took place in a face-to-face exchange.

7.2.1 Question One: Security's organisational role

Question one of the semi-structured interview questionnaire (Appendix C) asked panel members to state what, from their experience, the role of security is within an organisation, that is, the systems purpose. This question related to the functional approach towards security, discussed in Section 2.1.3 Security defined, and sought to consider the validity of this thesis's functional, focused approach to security. This approach sought to validate the removal of attached disciplines such as safety from the security function at the tactical level of management to enable a concentrated approach towards discussing, explaining and defining security decay functionally and across all three levels of organisational management (strategic, tactical and operational).

In response to this question, panel member one stated that security depends on context; however, for him security primarily relates to the protection of people, not occupational safety and health, although this does come into it, rather the safety of people from malicious people. In addition, it also encompasses asset protection, secure containment and incident management. Panel member one stated that security is embodied within a triangle (Figure 7.1), interlinking management, technology with the built environment.

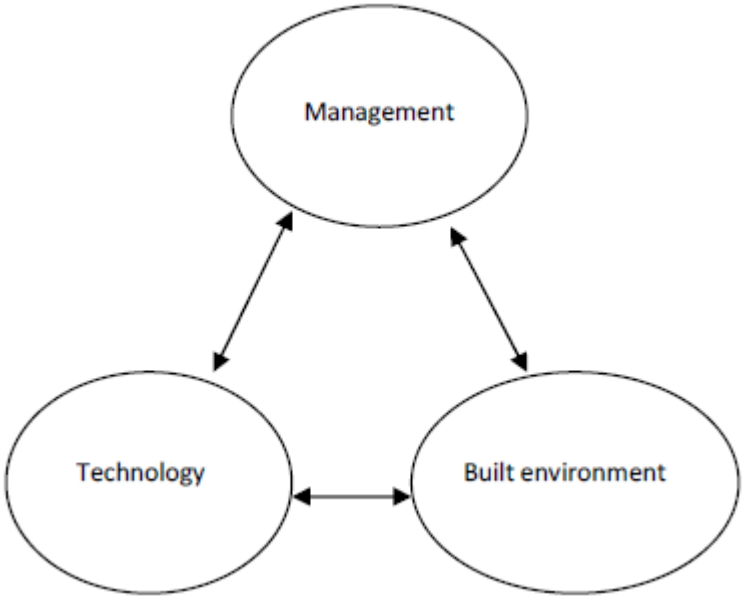


Figure 7.1 Panel member one's security management diagram.

To this question, panel member two stated that security relates to the protection of assets, including people, information and physical, integrated to assist the organisation achieve its specific business objectives. In considering this approach, panel member three stated that security for him is about the secure containment of offenders (institutional approach), approaching security from an organisational context, and states this is achieved through the provision of physical, procedural and dynamic (intelligence) security measures in a balanced and holistic manner.

During the feedback process (round two) panel members supported each other's responses. Therefore, for this panel, a consensus was achieved that security relates to the protection of an organisations assets, including people, information and property to achieve organisational specific business objectives, that is, context specific. For this question within the research panel a consensus was also achieved, supporting the pilot panel's results. The research panel supported that security at the tactical level of

management, relates to the holistic implementation of procedural, physical and electronic measures which aim to protect an organisation's assets which includes people, information and physical property through their ability to deter, detect, delay and respond against organisation specific threats in order for an organisation to achieve its business objectives.

7.2.2 Question two: Security's organisational purpose

Question two sought to establish whether research panel one viewed security's role as a risk reduction role in-line with Section 3.4 Security and risk management. All panel members responded "yes" to this question. Panel member one stated "without knowledge of risk there is no baseline for security". In addition, panel member two stated "security's role is to mitigate known or perceived risks". During the feedback process the panel supported the interpretation that a consensus was reached within the panel that security is a risk reduction role. The research panel supported the pilot panel's views that security is a risk reduction role at the strategic level of management. Furthermore, the research panel supported the pilot panel's view that security also has a deterrent role for any organisation towards preventing security related incidents.

7.2.3 Question three: Security's body of knowledge

Question three asked panel members how they apply security's body of knowledge including theories, principles and specifically Defence in Depth. Panel member number one responded that it does depend on the security context; however, Defence in Depth is an absolute underpinned by security risk management, that is, you need to understand the context. Furthermore, panel member one stated that security must be very functional. To this question, panel member two stated that he employs Defence in Depth along with crime prevention through environmental design (CPTED) and risk management. According to panel member two, all these aspects need to be interrelated. Panel member two stated that security intelligence (SYNT) needs to be integrated with risk management to ascertain how Defence in Depth will be achieved. In addition, panel member two states that Defence in Depth is achieved across a site based on the access control requirements, considering different zoning contexts. Panel member three also reported that he employs Defence in Depth and CPTED, stating "security incorporates procedural, physical, technical, intelligence and risk management in a balanced approach".

For this question a consensus was achieved, in-line with the results from the pilot study, that Defence in Depth coupled with CPTED and risk management applied holistically, based on a hierarchical system of access control is the salient and consistent strategy/means of employing security's body of knowledge, and that the employment of such a body of knowledge must be very functional.

7.2.4 Question Four: Defining systems

Question four explored panel members' understanding of a system in relation to Section 2.2.2 Defining systems and Section 2.2.3 the systems approach, and asked panel members to explain their understanding of a system. To this question panel member one stated a system approach is a "top down process". A systems approach considers strong interrelations between the components in achieving their and the system's objective, and the interrelationship between the design stage and the operator interface. According to panel member one, a systems approach requires a structure with good interactions between components (highly interrelated) which is seen as a "whole". Panel member two responded that a system ties together a group of elements and constituents which maintain a role towards an overall outcome, where all aspects are interrelated. Panel member three's views were similar, stating that systems are components linked, that is physical and procedures linked to achieve a goal.

In addition, the research panel supported the pilot panel's consensus that a systems approach to security relates to how risks can be reduced through a holistic approach, interrelating the separate components which combine to achieve an overall goal. For this panel a consensus was reached that a systems approach is a top down process (systems purpose) which ties together the separate components/constituents that have a defined role, which are interrelated with other aspects to facilitate the achievement of the systems overall goal. The panel's views and understanding were accordant with Sections 2.2.2 and 2.2.3 (Chapter 2) and indicates that accordant with this literature, the panel have a good understanding of what constitutes a system.

7.2.5 Question Five: The systems approach to security

Question five asked panel members if they supported a systems approach to implementing effective security. All panel members provided an affirmative response to this question, achieving a consensus, with all panel members reporting that they support a systems approach towards achieving security risk reduction. However, panel member

one stated “as long as systems are designed properly to manage the security risks they are intended to manage”. This consensus is consistent with the literature reviewed in Section 3.1 (Chapter 3), an open systems approach to physical security, where such an approach was recommended by many published security professionals. It is the systems approach to security risk reduction which frames this research’s approach to understanding security decay. It is therefore interpreted that a consensus exists amongst the panel supporting the systems approach to security and specifically, security risk management.

7.2.6 Question Six: Defining the systems approach to security

Question six asked panel members what they believed the systems approach to security involves. Panel member one responded the systems approach is a holistic approach that recognises the main contributions to the security solution. This approach includes the built environment, the technology, physical security aspects, procedures and management processes, and how each of these elements are implemented, recognising the importance of each other and how the interactions compliment and influence each other (Figure 7.1). According to panel member one, each element is configured or implemented to support each other, recognising the Swiss cheese approach (Figure 7.2) towards achieving holistic security. The Swiss cheese model proposes that under normal circumstances the holes in each slice of cheese will be covered up by subsequent layers of controls, where the summation of these controls represents the effectiveness of the system in managing an attack against the system.

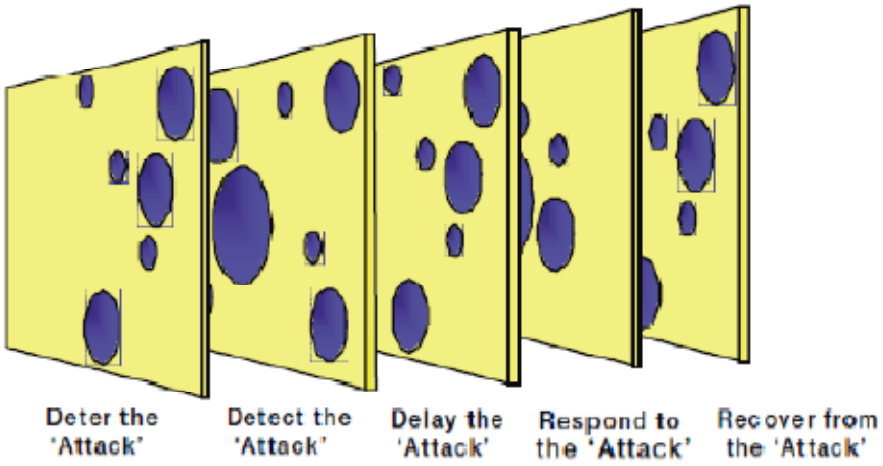


Figure 7.2 The Swiss cheese approach to security (Standards Australia; HB 167, 2006, p. 60).

Panel member one's views were supported by panel member two, who stated "the systems approach to security is the same as the systems approach with any organisation aiming to achieve business objectives". According to panel member two, the Physical Protection System (PPS) broken down into its component parts relies on the other components within the system, where if one component is broken, or removed, this changes the whole system. For example, Defence in Depth relies on all its elements to be integrated and at their measure of effectiveness. To this question, panel member three focused on the design aspects of a systems approach, stating for him, the systems approach is about having sound security practices in place before an event occurs, across all body of knowledge domains.

The panel reached a consensus that the systems approach to security is a holistic approach, which achieves its objective through the integration of separate security components/ constituents, being physical, technical and procedural, each with a defined role, that are implemented in a manner where their interrelations compliment and influence each other to reduce security related risks in a preventative manner. Specifically, panel member one utilized the Swiss cheese analogy to emphasise the systems approach to achieving holistic security. During the feedback process both panel members two and three supported this analogy, with panel member three stating "this model was a good example".

7.2.7 Question Seven: System sensitivity

Question seven related to a premise within systems theory that small changes within a specific component can lead to a large change at the output of systems, and asked panel members whether they agree with this premise and explain their reasons.

Panel member one responded to this question stating that he does agree with this principle. According to panel member one, due to the reliance on each element, small changes can have a domino effect on each of the other elements that combines to the systems base structure. These changes may be small, but if not considered in a holistic manner or without clear understanding of why an element was implemented or structured in the first place, you can change the basic premise of why and how it supported other elements within the system. Once again, panel member one drew on the Swiss cheese model, stating that you can actually move the "holes" so that it now aligns

with another hole (Figure 7.3). If you do this with several or many small changes you can create a weakness that is substantial, yet difficult to recognise.

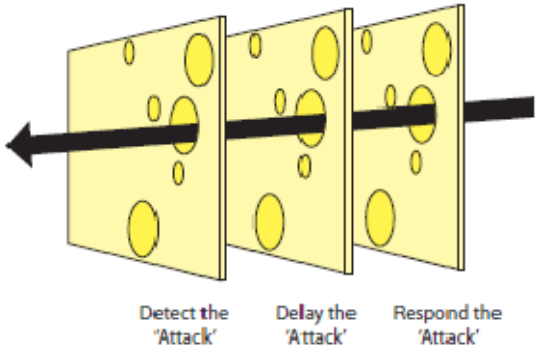


Figure 7.3 The Swiss cheese model where the holes line up, creating a system weakness.

To this question panel member two stated, “It comes down to a cause and effect”. By one small element changing, results in a larger-more-macro change, stimulating a chain reaction through the system. A consensus was reached within the research panel supporting both this principle within systems theory, and that it applies to PPS. In addition, a consensus was reached supporting panel member one’s Swiss cheese analogy of how small changes in a PPS can lead to a weakness within the “system”, based on the interrelations, which can be difficult to recognise.

7.2.8 Question Eight: Physical security and key performance indicators

Question eight related to an aspect of systems theory which focuses on those key performance indicators that are directly related to the “whole systems” key performance indicator, where it is argued within the systems literature that “the ultimate aim is to discover those components whose measures of performance truly relates to the measures of performance of the whole system” (Churchman, 1968, p. 43). As such, this question asked panel members within their understanding of a systems approach, what they believe the key performance indicators are within PPS.

Panel member one responded that key performance indicators are those items that you can use to monitor the effectiveness of the ongoing performance of each element of a system. Panel member two stated that key performance indicators give you a measure,

where you set the goals in an organisation to ensure you are achieving what the system is designed for, it is a monitoring process. According to panel member one, if the key performance indicators are not being met, this could strongly suggest that a specific element is not delivering the full capacity of the outcomes for which it was specifically designed. Panel member one stated "if an element is not delivering required performance it may not be supporting other elements within the total system in the manner for which it was intended to, designed and implemented". According to panel member one, shortfalls in elemental performance is very likely to have an impact on the whole of the systems performance, therefore if "whole of system key performance indicators" are correctly identified, structured and monitored, these will be directly influenced by elemental key performance indicators.

In considering this approach, panel member three stated "the key performance indicators for a PPS are the core elements of Defence in Depth", where according to panel member two "the elements of PPS become the key performance indicators". For this panel, a consensus was achieved that the key performance indicators for a PPS at the tactical level of management, were based on the Defence in Depth elements, starting with detection as an element, that is, the systems probability of detection, then the probability of successfully transmitting the alarm actuation, followed by a measure of accurate assessment (discrimination) of the alarm cause, then a probability of communicating that alarm source (probability of communication) to the appropriate response component of the system. Once detection has been achieved the next key performance indictors include delay aspects measured against the response capability, based on the mean averages, become the systems measures.

In his initial response panel member one provided a list of key performance indicators which he believed related to "whole of system effectiveness". However, a consensus was reached within the research panel that these represented operational key performance indicators which make up, and achieve the tactical level key performance indicators. That is, they contribute to ensuring and achieving the elements of Defence in Depth tactical level key performance indicators. The pilot panel responded through consensus that constituent performance measures across the built environment, management processes, and technology provide the operational level key performance indicators, for example, key performance indicators such as probability of detection,

nuisance and false alarm rate, vulnerability to defeat provide detection system key performance indicators.

7.2.9 Question Nine: Key performance indicators and system effectiveness

Question nine asked panel members, in relation to their responses to question eight, do they believe the key performance indicators of systems are related to the systems effectiveness, and explain their answer. In answering this question, panel member one responded "yes", stating the key performance indicators should be related to system effectiveness. The key performance indicators are a measure of whether an element and therefore a "system", is delivering the outcomes and functionality for which it was designed. Panel member two supported this approach, stating "this is your means of ensuring elements are achieving your design goals".

To this question panel member two added that key performance indicator reduction at the micro-level reduces key performance indicator reduction at the macro-level. "As panel member two stated "The overall key performance indicator provides a strategic level of monitoring effectiveness". Panel member one supported this approach, stating "this directly determines or impacts on the elements effectiveness as a single element performing its required function and effectiveness in supporting other elements in its functions within the total system". These responses were also supported by panel member three, who stated "I do believe the systems performance indicators are related to the systems overall key performance indicator". We select individual components from their individual key performance indicators, then, combine them together into a "designed whole". It is interpreted, in-line with the responses from the pilot panel, that the panel support that the key performance indicators of the systems are related to the systems effectiveness.

7.2.10 Question Ten: Security decay

Question ten asked panel members if, based on their experience, do they believe that security systems decay. This question related to Section 4.1 (Chapter 4), which postulates that all physical systems, if left to themselves (become closed) move towards a state of decay, that is, maximize their entropy. All panel members responded positively to this question, providing a consensus that based on their experience, they believe, consistent with this research's literature review, security systems decay.

7.2.11 Question Eleven: Understanding security decay

Question eleven asked panel members what their understanding of security decay was. For this question, panel member one responded "security system decay is the degradation in the performance of an element of the security solution ... Both as a single element performing a specific function, and the elements role in supporting other elements in their function within the total system". To this question panel member three responded that security decay goes right across all aspects of a security program, across dynamic (intelligence), physical, technology and procedural security. For example, according to panel member three, all technology decays, as technology decays it constantly false alarms, then staff ignore them, where ultimately they lose confidence in it (the system) and their work practices decay.

In explaining his understanding of security decay, panel member one states "decay may not be a major failure of this system, but more incremental decrease in performance that occurs over time". To this point, panel member two believed that decay could be gradual or rapid over time. For example, procedural decay can occur rapidly. Panel member one added, "decay may however occur incrementally and continue over an extended period to the point it has a significant impact on performance and effectiveness". This aspect may be compounded further where this decay occurs over many or all elements within a system, which can lead to major failure. However, panel member two states that decay is something you can have an element of control over, that is, the rate of decay. There are elements of decay you can have control over such as training and awareness, whilst some things decay, they can be brought back up to commissioning levels. Nevertheless, for engineering or built environment there is a life span.

According to panel member one, decay may be the degradation of a detection technology "probability of detection" (lack of testing and maintenance), degradation of the alarm gathering notification communication systems reliability, that is, increase communications alarm failures (lack of routine maintenance), degradation of daily testing procedures, degradation of control room operator's knowledge of correct procedures, and the degradation of the physical environment.

A consensus was achieved within the research panel that decay embodies all aspects, constituents and elements within PPS. That is, consistent with the pilot panel's results,

any single part of the system can decay, and based on the systems interrelationships, this decay affects the rest of the system.

7.2.12 Question Twelve: An experience approach to security decay

Question twelve sought to achieve an experienced based approach, exploring real world examples of a time when panel members had experienced security decay. This question asked panel members to provide an example of a time when they experience security decay. Panel member one responded that there are many practical examples where he has come across security decay as a security consultant, both elemental and/or systems decay. For example, panel member one experienced a lack of maintenance in perimeter detection systems sterile zones (weeds and other feral growth), triggering increased nuisance alarm rates, causing lack of confidence and increasing operator's complacency. According to panel member one, a lack in electronic system maintenance causes these same outcomes. Furthermore, panel member one stated "poor or total lack of daily testing procedures resulted in a failure to identify systems not working". In addition, a lack in ongoing formal training where new training in how to operate systems occurs for new staff by handed down experience rather than from formal training processes, meaning incorrect procedures or bad habits are passed on. Also, a lack of ongoing training for qualified staff leads to decay.

Panel member one also reported having experienced physical deterioration of physical elements, which are not maintained, reducing their effectiveness of the element as a barrier, or what-ever function it performs. Furthermore, changes to the built environment, or adjacent areas without considering the perimeter detection and surveillance systems, and changes to systems aspects to suit personal preference, without consideration to, or reference to, initial design considerations and integrated response requirements. Panel member two also reported experience with fluctuations in staff competencies leading to security decay. According to panel member two, staff competency's fluctuations alters key performance indicators, where decay occurs in relation to the reduction in competencies and capabilities of the people component within PPS. Panel member two states that most agencies work at the lowest common denominator where system key performance indicators are based on the lowest standard, this includes training. Panel member two states "system key performance indicators

increase with competency increase, and of course decrease as those competencies decrease".

Both panel member one and two's responses relating to staff competencies was also reported by panel member three, who provided a situation involving staff's lack of familiarization/awareness with procedural security during perimeter alarm checks as an example of security decay. This very aspect was also reported by panel member one. According to panel member three a system they had commissioned incorporated a microphonic detection technology into the cowling on top of a barrier. Often staffs do-not test this system properly, where decay relates to improper testing around its designed requirement, in-line with their procedures, resulting in technical decay as it is not known if the system is working based on its design configuration. Also, during staff testing, they do not test all aspects such as alarm preset positions and field of view objectives for closed circuit television cameras.

According to panel member three, he has experienced environmental impact on physical structures leading to security decay, for example, a high security fence (barrier) they had installed. The plinth was not designed to move water; therefore water sat at the base of the fence and due to high salt content within the environment, premature physical decay of the barrier occurred. According to panel member three, such decay needs to be considered at the design stage of a security project.

Each participant's examples were put to the other panel members during the second round interviews. A consensus was reached with all aspects of the each participant's examples of security decay, showing that decay occurs within each aspect of the PPS. For example, Figure 7.4 indicates the interrelated aspects of people, technology and physical engineering which combine to achieve a PPS, where decay can occur in each aspect, and based on the systems interrelations, affect another aspect of the system.

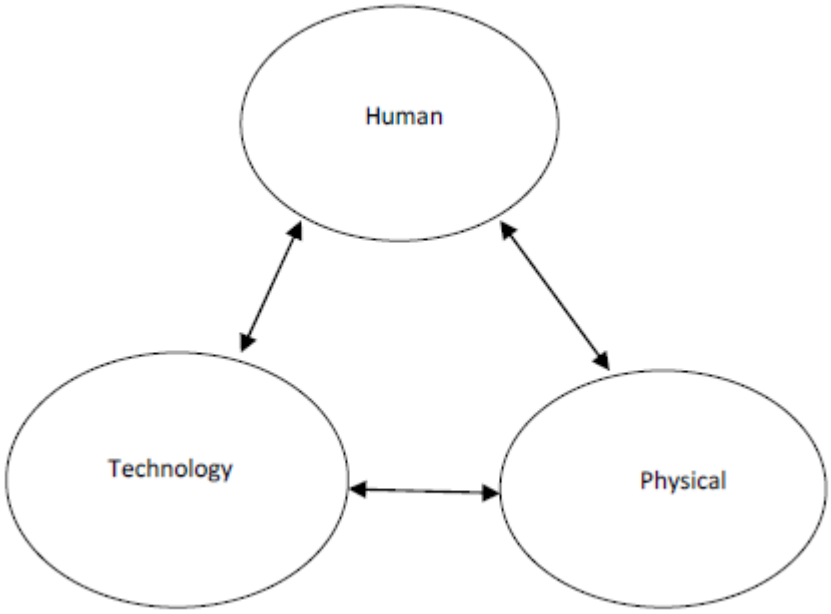


Figure 7.4 The interrelated aspects of a Physical Protection System.

7.2.13 Question thirteen: A systems approach to security decay

Question thirteen asked panel members that in considering the argument that security controls decay: how did they think this occurs within a systems approach to security. To this question panel member one stated "decay within a Physical protection System (PPS) occurs within its individual elements and propagates through the system". According to panel member one, decay occurs at the base element level over time. This decay at element level occurs through many causes and the effect can result in major system breakdown. Once again panel member one draws on the Swiss cheese model of Defence in Depth, where failure can occur across the "system" if not planned, implemented and individual elements integrated correctly.

Panel member one's views were also reported by panel member two, who stated "decay occurs at the elemental level". According to panel member two, the efficacy of the system decays as small changes occur, changes start small, however, spread when not detected and managed. Panel member two stated that systems are delivered (commissioned) based on a desired benchmark and are commissioned against this benchmark including physical, procedural and electronic aspects. According to panel member two, what changes initially is procedural security, where decay occurs when staff no longer maintain initial personnel based key performance indicators, where this initial decay propagates throughout the remainder of the system. Panel member three

also reported similar views stating “as one component decays, this affects other aspects of the security system; and its deterrence aspect as well”. For example, according to panel member three, multiple false alarms can propagate through the rest of the system, then complacency sets in, alarm inputs are not discriminated (assessed) or reported, ultimately affecting the response aspect of the system. Any aspect of decay affects the rest of the system.

A consensus was reached within the panel, that within a systems approach to security, decay starts in one aspect of the system; however, this can manifest simultaneously across several constituents, then based on the systems interrelationships propagates throughout the remainder of the system, ultimately affecting the systems response element and its output goal.

7.2.14 Question fourteen: Error propagation in Physical Protection Systems

Question fourteen asked panel members whether they support the premise that security decay within a PPS occurs within individual constituents, and its effects propagate through the system from this point. To this question a consensus was achieved, with all panel members supporting this premise, where this occurs based on the systems interrelations. In addition, panel member one stated that consistent with his previous answer, a “system” is a combination of elemental inputs, the system is very much dependant on the correct operation of the effectiveness of each of these elements in performing their function and supporting functions of other elements. Therefore, small decay/changes in the elements, particularly where it occurs across many/all elements can have a major impact on “system” output at the macro level.

7.2.15 Question fifteen: The Butterfly effect

Question fifteen asked panel members if they feel an effect referred to as the “Butterfly” effect, which suggest that small input changes within a system can result in large changes at the macro output, applies to a PPS, and could they provide an example. All panel members responded affirmatively, agreeing that the “Butterfly” effect does apply to PPS. For example, panel member one provided a substantial list of examples where he had experienced the “Butterfly” effect within PPS. Panel member one stated “I have seen a PPS that was reviewed that had contribution degradation in:

1. High nuisance alarm rates due to poor performance in detection technologies due to lack of maintenance in perimeter zone.

2. Incorrect technical maintenance causing high false alarm rates
3. Poor or complete lack of maintenance of physical elements, leading to decline in this reliability of physical barriers.
4. Changes in CCR, adding technology, moving equipment etc, degrading their operational effectiveness of this area.
5. Poor physical attribute (lighting and air conditioning) providing inappropriate outputs conditions for maintaining concentration and focus, degrading this operational efficiency in the CCR.
6. Standard operating procedures (SOP), other procedures being modified without reference to holistic system requirements (To address minor elemental issues), degrading the performance of the operational system.
7. Poor communications structures between CCR staff, security management and operational staff contributing to degradation of overall "system".
8. Poor or lack of formal CCR operational training specific to the subject, (training by operators handing down through word of mouth) leading to a lack of true understanding of how to use the "systems" effectively.
9. Incorrect incompletion of both daily tests of PPS zones.
10. Degradation in support systems functional operational or technical performance, affecting ability to discriminate alarms, this includes operation of lighting system controls, maintenance of lighting-lamp failure affects the performance of CCTV surveillance cameras".

Each of the above may have only minor degradation or degradation that is not significant in its own sphere, the accumulated impact of this above, however, presented significant risk. In this instance, it was clear that the input changes or performance degradation with each element had this potential to result in large change or performance degradation without evaluation in consideration of the total PPS.

For his example, panel member two stated that he has seen how procedural decay stimulated through poor operator training has lead to the "Butterfly" effect. According to panel member two, system training has a macro level output throughout the system, however, over time, the training level set at the systems commissioning is allowed to decline, then the level of staff competency declines, affecting the remainder of the system. Furthermore, panel member three stated "small system changes can have a significant impact at a much higher level and change the strategic direction of an agency".

7.2.16 Question sixteen: The effects of security decay

Question sixteen asked panel members what, based on their experience, did they think the effects of decay were. To this question panel member one stated "the effects of decay were as heterogeneous as the system itself". Panel member two stated that decay

disrupts an organisation's ability to achieve set goals and objectives as it disrupts each component or element within the system. Such views were supported by panel member three, who added that decay leads to a breakdown in system reliability, increases the risks of significant events occurring and can impact on the strategic and operational direction of agencies due to political encumbrance if events are realized. In addition, for this question the research panel supported the pilot panel's findings that decay at the component level results in gradual degradation of a system's individual key performance indicators, reducing sub-system key performance indicators.

It is therefore suggested that a consensus exists that decay occurs at the component/constituent level, then, degrades system key performance indicators, reducing sub-system key performance indicators. Such decay ultimately affects the risk reduction aspects of the system, bearing a strategic impact on an organisation.

7.2.17 Question seventeen: Correcting security decay

This question asked panel members if, once decay has set in, did they think its effects, both at the point of manifestation and throughout the remainder of the system are reversible. The consensus within the group for this question was that reversing the effects of decay depended on what the decay related to. The panel agreed that procedural decay could be prevented and reversed through management, that is, ongoing monitoring and reviewing of the people component. However, physical and technical decay can only be controlled/delayed, through processes. The research panel agreed that all physical and technology components have a life cycle, where eventually they will decay beyond a repairable state. It was considered that with proper maintenance decay can be slowed and managed. Nevertheless, panel member two stated "decay can only be countered if it is understood". In response to the pilot panel's findings that decay could be reversed once located within the system, the response from the research panel were that as previously stated it depends on what type of decay it is, where you can reverse some aspects of decay.

7*.2.18 Question eighteen: Avoiding security decay*

Question eighteen asked panel members if they believed decay within a PPS could be avoided. In response to this question panel member one stated that the majority of decay can be avoided; however, decay is like risk, you can mitigate some decay, and you can accept some decay and you can reduce the impact. The responses to panel member

one's views were in-line with previous responses, that is, procedural decay can be avoided, through intense management strategies with regular audits and implementing the necessary corrections. Nevertheless, for technical and physical decay, the consensus was that it can be managed and its effects delayed through proper monitored maintenance.

7.2.19 Question nineteen: Security decay and risk management

Question nineteen asked panel members if they believed the concept of decay had a place in the risk management process. For this question panel member one responded that it belongs in the monitor and review process; however, there was a danger in not considering decay outside this sphere. Panel members two and three responded that security decay needs to be considered in your security context planning, where according to panel member three, consideration of decay should start at the assessment of risk stage, where decay is considered at the design stage and considered as a risk. A consensus was reached amongst the research panel that security decay should be considered as a "system", at the design stage, against its consequences, with a view to countering it where practicable as a risk treatment, towards designing out decay, then continually assessed for in the monitor and review stage. Such views supporting the consideration of security decay in the monitor and review stage are congruous with the pilot panel's findings and consistent with Standards Australia HB 167 (2006, p. 87), which incorporates a monitor and review stage in the security and risk management process.

7.2.20 Question twenty: Exploring security decay

Question twenty asked panel members if, based on their experience, is there any facet of security decay which they could add to the research enquiry. To this question panel member two stated that decay relates to the "whole" system and its interrelations, linked into your planning processes where, in-line with question nineteen, you should as best as practicable, consider future proofing within the system to minimize decay onset. Panel member three added that he believed security decay will always be managed against the level of recurrent funding available.

To this point, during the feedback process, panel member two responded that panel member three's views relate to the initial security project scope, stating "when you put your capital submission forward, you must, at a strategic level, indentify whether the

system you are putting in is achievable, and that you can maintain the system you are putting in". According to panel member two, panel member three's recurrent funding submission is required at the design stage. Panel member two's views suggest that decay should be planned for at the design stage of PPS. This view is consistent with all panel members' responses to question nineteen, where it was agreed that security decay should be considered as a risk, and countered, prior to system implementation. That is, decay should be budgeted for as an ongoing aspect of the security project.

7.3 Reliability and validity

Congruous with Section 5.9 this chapter incorporated reliability and validity controls. These controls included the principle of triangulation where three participants were used to construct the research panel. This provided data inputs from multiple participant sources where in-line with the underpinning principles of triangulation it is argued where consistent views were reflected and where consensus was achieved a higher level of confidence can be inferred towards supporting the core themes and principles evolving from the panel. Triangulation was also used to establish consensus support to each panel member's thoughts and feelings relating to security decay. In addition, member checking was incorporated into the panel design, where during the second round feed-back process each panel member was presented with a transcript of their interview responses. Furthermore, each panel member was asked whether they supported the interpretations drawn from the data, and were provided with the opportunity to respond to these interpretations. This aimed to establish a level of trust towards the inductive analysis prior to moving forward to the deductive analysis phase.

7.4 Reflection

Reflecting back over research panel one's interview data a number of themes and core principles have evolved towards developing an understanding of security decay within an open systems frame. According to this research panel, security starts at the strategic level of management incorporating a top down process, where the systems purpose is established based on an organisation's risk reduction requirement, establishing a systems base line. Risk management then steers the establishment of a systems parameters at a tactical level of management, holistically integrating: technology, physical controls, the built environment, and procedural risk control aspects, which all have a defined role that are combined into an integrated "whole", where each

component: functions, interacts, compliments and influences other functions towards achieving organisational goals. These controls are selected based on the theory of Defence in Depth and Crime Prevention through Environmental Control, where these security controls are summative, that is, their combination based on planning and design specifications provides the measure of risk reduction.

Physical Protection Systems (PPS) are commissioned against a benchmark, based on the risk reduction requirements. A consensus response from research panel one was that this summative, integrated "whole" suffers from decay across all constituent aspects, including: technological controls, the built environment, physical environment, physical controls, procedural and management aspects within Physical Protection Systems (PPS). This decay is caused by many factors relating to the management of the PPS. Research panel one agreed that procedural decay within PPS can be reversed or avoided through professional management strategies, whilst physical and technical decay aspects can be controlled/delayed through processes where some decay can be accepted, whilst other decay aspects can be mitigated, such as its impact. Research panel one concluded that decay starts small, but spreads if not detected and managed, propagating through the rest of the PPS based on the interrelated aspects of systems in general, ultimately affecting the organisations ability to achieve its goals therefore having a strategic impact. These core themes will be presented to research panel two, where not initially revealed, during their round two interview process towards evaluating their robustness as explanations of security decay within a systems approach to security risk reduction.

7.5 Conclusion

This chapter presented phase three, research panel one (N=3) interview analysis. The analysis provided a detailed account of participant's thoughts, feelings and understanding relating to the phenomenon of security decay, where in-line with Cohen, et al, (2005, p. 24) such research designs enable the gathering of information which is considered common sense, taken for granted, assumptions from lived experience. The research questionnaire required panel members to reflect back on their experiences within their respective security domains, inputting meaning retrospectively. This reflection (Section 7.4) produced a number of core themes to be taken to research panel two towards developing a consensus model of entropic security decay. These themes include the argument that security starts with a top down approach at the strategic level.

Risk management then steers the establishment of a systems parameters at the tactical level of management, holistically integrating: technology, physical controls, the built environment, and procedural risk control aspects which all have a defined role and are combined into an integrated "whole". Based on these themes Physical Protection Systems (PPS) are commissioned against a benchmark as a summative integrated "whole" where all constituent aspects suffer from decay. Decay within these constituents is caused by many factors relating to the management of PPS.

This chapter also presented measures of reliability and validity (Section 5.9) in-line with this study's methodology. Reliability and validity was achieved by employing the principle of participant triangulation, drawing on multiple participant information sources relating to security decay underpinned by member checking, where during the second round interviews, panel members were provided written transcripts of their interview responses towards establishing a measure of truthfulness in this study's research analysis.

CHAPTER 8

RESEARCH PANEL TWO

8.0 Introduction

This chapter presents the second stage of phase three, research panel two (n=3) of the study. The chapter aims to produce a further growth in experienced based knowledge towards developing an enhanced understanding of entropic security decay. To achieve a successful outcome for this chapter an inductive analysis was conducted with research participant responses to the interview questions (N=20), providing an analysis suitable for deductive evaluation in Chapter 9 (Phase 4).

This chapter is broken into a number of sections providing participant responses to the interview questions (N=20). Sections 8.1 presents research panel two's participant's biographical information, establishing each participant as a security expert within their respective security domains. Section 8.2 presents the interview data, which will be drawn on in phase four of the study to achieve the required deductive analysis enabling responses to this study's research sub-questions and research question. Section 8.3 provides a reflection of themes and core principles which evolved across this study. Section 8.4 concludes this chapter presenting, a summary of achievement and measures of reliability and validity.

8.1 Participants

Participants' for this panel consisted of peer nominated security experts (n=3). These experts were selected and solicited to participate in this study based on the criterion that they are employed to provide security category knowledge advice across the varied security related occupations. As per panel one's participants (Chapter 7), they were selected based on their peer revere stemming from such criterion, as experience, occupation and/or education and training so that others rely upon them for professional opinion within the multi-disciplined security industry. These participants formed a non-probability security expert sample.

Participant number one

Panel member one has worked in the Oil and Gas industry for approximately five (5) years as a senior security adviser. He has over twenty (20) years military experience within the Special Forces fraternity, and holds a Bachelor of Science (Security) and a Graduate Certificate in Operations Management. Panel member one provides security compliance advice relating to Australia's Maritime Transport and Offshore Facilities Security Act 2003 in the pursuit of organisational goals. In addition, the panel member provides security advice relating to major capital works projects, prepares security plans and procedures and has responsibilities in the area of emergency management.

Participant number two

Panel member two is a principle security consultant for a Perth based consultancy in Western Australia. He has a combined twenty (20) years experience in criminal and civil investigations, conducts corporate risk assessments, security audits and specialist investigations for government and industry. Panel member two has lectured in Security Risk and Physical Security at Edith Cowan University (ECU) and holds a Bachelor of Science (Security) Honours, an Advanced Diploma in Business Management, and a Diploma in Criminal Investigations.

Participant number three

Panel member three is a senior security consultant with over thirty three (33) years experience consulting in high level security projects. Panel member three has professional qualifications as an electrical engineer and building services engineer, along with formal qualifications in security including Certified Protection Professional (CPP) designation. He has presented over 60 papers on security issues at both national and international conferences, and has lectured for sixteen (16) years in general security and facility counter-terrorism at Edith Cowan University (ECU), holding a post as Associate Professor of Security Science at ECU.

8.2 Panel study two interview questionnaire analysis

8.2.1Question one: Security's organisational role

Questions one of the semi-structured interview questionnaire (Appendix C) asked panel members to state what, from their experience, the role of security is within an organisation, that is, the systems purpose. This question related to the functional

approach towards security, discussed in Section 2.1.3 Security defined, and sought to consider the validity of this study's functional, focused approach to security. This approach sought to validate the removal of attached disciplines such as safety from the security function at the tactical level of management to enable a concentrated approach towards discussing, explaining and defining security decay functionally and across all three levels of organisational management (strategic, tactical and operational).

To this question, panel member one responded that for him, security's role relates to the protection of assets, and especially company personnel to enable work/business objectives to continue in a safe and secure environment. This approach was consistent with the pilot study's responses and research panel's one's views. However, panel member two responded that security's role is to manage the various security related risks for specific organisations. An approach also taken by panel member three, who stated "the role is to manage the threats that pose a risk to either: institutional, commercial and industrial organisations to mitigate risks". During the feedback process (Round two) a consensus was achieved that security's role at the tactical level of management relates to the holistic implementation of procedural, physical and electronic measures which aims to protect an organisation's assets, including people, information and property, through their ability to deter, detect, delay and respond against organisation specific threats.

8.2.2 Question two: Security's organisational purpose

Question two sought to establish whether the panel viewed security's role as a risk reduction role, consistent with Section 3.4, Security and risk management. This view was an important question, as an underlying premise framing the theory of entropic security decay is that when security controls decay they are in actuality still in place; however, their efficacy degrades as decay sets in, reducing their intended commissioning levels of effectiveness. It is this reduced level of effectiveness which may lead to an adversary determining that the balance of probabilities of success are on their side and it is worth attempting a penetration, ultimately leading to a security event. That is, the risks for an attacker are reducing therefore the strategic role of security is decaying as well as its tactical and operational roles.

For this question panel members' one and two stated "yes it is", where according to panel member three, the reason you have security is the mitigation role against those risks (Question one). In addition, for question one both panel member two and panel member three responded that security's role is to manage security related risks. The pilot panel and research panel one agreed through consensus that risk reduction relates to security's role at the strategic level of management. During the feedback process (round two) this aspect was put to the panel, where a consensus was achieved supporting that security's role at the strategic level of management is the reduction of security related organisational risks to facilitate the achievement of organisational objectives.

8.2.3 Question three: Security's body of knowledge

Question three asked panel members how they apply security's body of knowledge including theories, principles and specifically Defence in Depth. Panel member one responded to this question explaining that within his organisation they work of a prevention, preparedness, response and recovery model, stating, "I do employ Defence in Depth, but Defence in Depth can be hard to implement in our environment, on the ground because of environmental pressures". According to panel member one, Defence in Depth does work in some contexts, and he utilizes Crime Prevention through Environmental Design (CPTED). However, panel member two responded that he employs CPTED and Defence in Depth, in-line with organisation's management systems. Panel member three responded "I absolutely use Defence in Depth, with multiple rings of protection. During the feedback process (round two) panel member one supported that in applying the prevention, preparedness, response and recovery aspects of this model relate to the functions of Defence in Depth interrelated with CPTED principles to achieve prevention, preparedness and initial response aspects of their model.

In addition, to this question member three responded that he utilizes a philosophy incorporating a Triangle model (Figure 8.1). Member three refers to this as: The Campbell Triangle, stating "this provides the means of interrelating the multiple rings of protection". These rings stem from the integration of Defence in Depth and CPTED with the systems planning and development, the technological solution and the management aspects of the holistic solution. According to member three, once you define the multiple rings of protection, all elements of the triangle (Figure 8.1) must be

completed. Furthermore, for this question member two responded that he sees risk management, which underpins the implementation of security controls, to be part of the body of knowledge employed. This view was also stated by panel member three, research panel one.

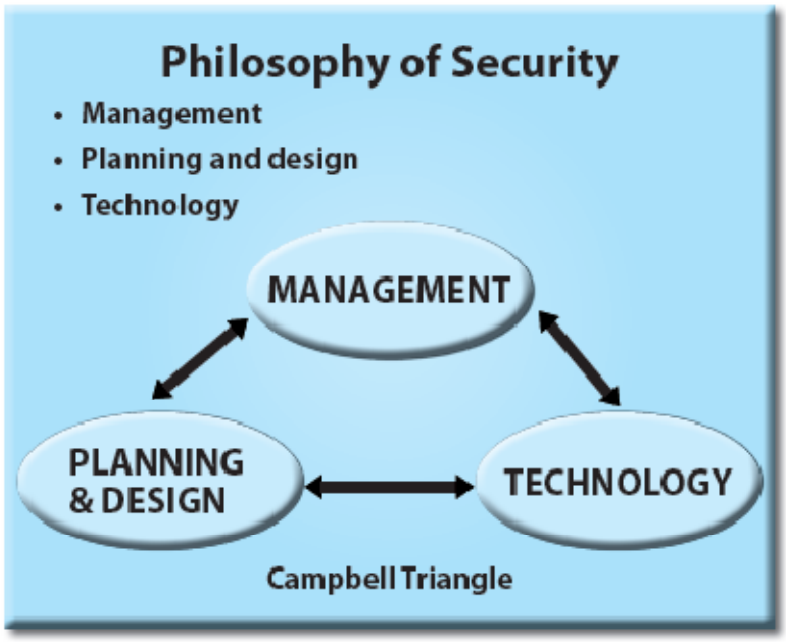


Figure 8.1 The Campbell Triangle.

For this question a consensus was achieved, consistent with the results from the pilot panel and research panel one. This consensus agreed that Defence in Depth coupled with CPTED and risk management applied holistically, with all aspects integrated, based on multiple rigs of protection, depending on risk, is the salient and consistent strategy/means of employing security's body of knowledge. The panel's agreed that the employment of such a body of knowledge, in-line with member one, research panel one, must be very functional.

8.2.4 Question four: Defining systems

Question four explored all panel members' understanding of a system in relation to Section 2.2.2 Defining systems and Section 2.2.3 the systems approach, and asked panel members to explain their understanding of a system. To this question panel member one responded that a system is something logical in sequence, with a start and an end point, which has a designated and predicted outcome. Panel member two responded similarly, stating "systems are processes working towards an output or goal. Their key factor is that their components are interrelated and interdependent". According to panel member

two, he considers the interrelationships. Panel member three expanded this explanation, adding, “Each system in itself is a system of systems. Each system has to be integrated into other systems, where each must play its part underpinned by mission critical infrastructure”. In addition to this question, member one, research panel one, stated that “a systems approach is a top down process”; however it should be seen as a whole. During the feedback process all panel members supported this additional view point, with panel member three responding, “Yes he is right. A security system is aggregating a number of systems to achieve the solution”.

For this question all panel members considered that a system embodies something purposely designed to achieve a designated goal or outcome, where a consensus was achieved supporting the responses that each component must be integrated and play its part in supporting other systems aspects. For this panel a consensus was reached that a systems approach is a top down process (systems purpose) which ties or brings together the separate components which have a defined role. These components are interrelated with other aspects to facilitate the achievement of the systems overall design goal.

8.2.5 Question five: The systems approach to security

Question five asked panel members if they support a systems approach to implementing effective security. In response to this question panel member one stated “as much as practically possible”, where panel member two responded “yes”. In his response to this question, panel member three stated “yes, any security solution is based on an organisation’s physical and technical needs, all of which must be compatible, homogeneous, and completely supporting the risk mitigation process”. A consensus was reached within panel two, consistent with the pilot panel and panel one, with all panel members supporting the systems approach to implementing effective security.

Consistent with research panel one, this consensus is congruent with the literature reviewed in Chapters 2 and 3, establishing an open systems approach to Defence in Depth, where such an approach was recommended by many published security professionals. It is the systems approach to security risk reduction which frames this research’s approach to understanding security decay. Therefore it is interpreted that a consensus exists amongst the panel supporting the systems approach to security and specifically, security risk management.

8.2.6 Question six: Defining the systems approach to security

Question six asked panel members what they believed the systems approach to security involves. Panel member one responded that the systems approach incorporates prevention, response and recovery, and all aspects which fall in place to minimize the occurrence of an event, and the processes in place to respond and recover. Panel member two suggested a systems approach provides a holistic approach from beginning to end, starting with policy, then infrastructure, and how this infrastructure relates to the threats where the gap is the vulnerability. Panel member three responded stating "in-line with my previous response", refers back to the Campbell Triangle (Figure 8.1), "where each system is a system within a system".

During the feed back process panel member two participants were presented panel one member one's response, where according to this panel member a system approach is a holistic approach that recognises the main contributions to the security solution, be they management processes, procedures, technology, physical barriers, built environment and people, and how each of these components are implemented to complement and support each other. In his explanation of a systems approach panel one member one drew on the Swiss cheese analogy presented in Standards Australia (HB 167: 2006, p. 59), where many security controls will exist in a "layered" or Defence in Depth structure, under normal circumstances the holes in each layer are covered up by subsequent layers of controls (Figure 8.2).

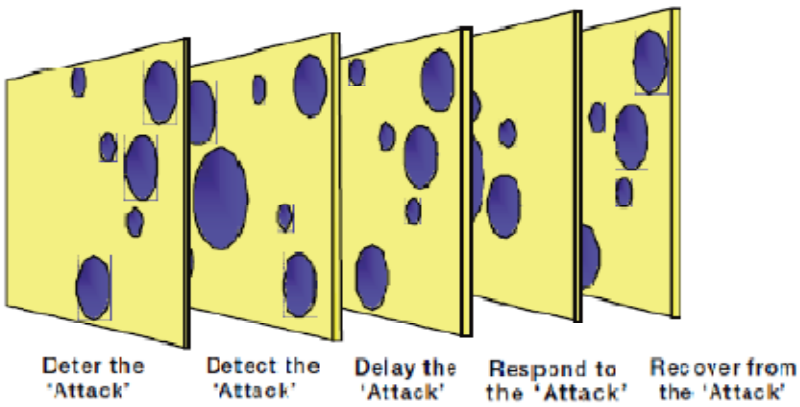


Figure 8.2 The systems approach to Defence in Depth (Standards Australia, HB 167: 2006, p. 59).

Consistent with this approach, panel one member two, responded that the systems approach to security is the same as the systems approach to any other organisational aspect. That is, the Physical Protection System (PPS) broken down into its component parts relies on the other components within the system, where if one component within the system is broken or removed, this changes the whole system. For example, Defence in Depth relies on all its elements to be interrelated and at their measure of effectiveness. For this question, research panel two reached a consensus consistent with research panel one, that the systems approach to security is a holistic approach, which starts with a policy (systems purpose) and achieves its objective through the integration of separate security components/ constituents, being physical, technical and procedural, each with a defined role, that are implemented in a manner where their interrelations compliment and influence each other to reduce security related risks in a preventative manner. Where accordant with panel member two, the gap is the system's vulnerability. During the feedback process all panel members supported panel one member one's explanation, drawing on the Swiss cheese analogy to emphasise the systems approach to achieving holistic security.

8.2.7 *Question seven: System sensitivity*

Question seven related to a premise within systems theory that small changes within a specific component can lead to a large change at the output of systems, and asked panel members wether they agree with this premise and explain their reasons.

To this question panel member one responded that it goes back to a disproportional effect, one small aspect of change on a system can change the output significantly. This view was also reported by panel member two, who stated "variable inputs can have significant ramifications that can become confounded. Small changes in something like Defence in Depth, such as a passive infrared detection sensor not detecting renders the remainder of the system useless". Such a view was also reported by panel member three, who responded "absolutely". Panel member three referred back to the Campbell Triangle, stating "there is an interrelationship between the management, planning and design and the technology aspects of the system, any changes in one area affects the other interrelated areas.

A consensus was reached within the research panel supporting both this principle within systems theory and that it applies to PPS. In addition, a consensus was reached

supporting panel one member one's Swiss cheese analogy of how small changes in a PPS can lead to a weakness within the "system" based on the interrelations, where according to panel one member one, due to the reliance on each element, small changes can have a domino effect on each other elements that combines to the systems base structure. These changes may be small, but if not considered in a holistic manner or without clear understanding of why an element was implemented or structured in the first place, you can change the basic premise of why and how it supported other elements within the system.

According to panel one member one you can actually move the "holes" so that the holes in the Swiss cheese now align (Figure 8.3), where if you do this with several or many small changes, you can create a weakness that is substantial, yet difficult to recognise. In response to this, during the feedback process, panel member three stated "the holes may not be in a direct line, but align for a specific threat agent (defined threat) across the layers, where decay may only occur in one aspect of the Swiss cheese, where the specific capabilities across the other two layers means they now can exploit this vulnerability, creating for themselves 'opportunity".

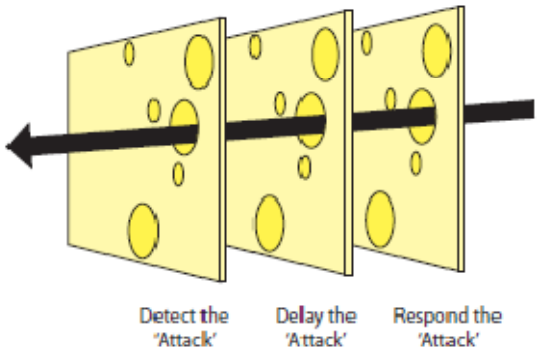


Figure 8.3 The Swiss cheese model where the holes line up, creating a system weakness.

8.2.8 Question eight: Physical security and key performance indicators

Question eight related to an aspect of systems theory which focuses on those key performance indicators that are directly related to the "whole systems" indicator. It is argued within the systems literature that "the ultimate aim is to discover those components whose measures of performance truly relates to the measures of

performance of the whole system" (Churchman, 1968, p. 43). As such, this question asked panel members within their understanding of a systems approach, what they believed the key performance indicators are within PPS.

To this question panel member one responded that these relate to the amount of who can enter a restricted area, the identification that something has occurred, the assessment of the situation, the communication of an event, plus the response to the event. This theme was also followed by panel member two who responded that these (it) come back to Defence in Depth and the SANDIA EASI model. That is, the EASI key performance indicators linked into the operational key performance indicators that achieve a Defence in Depth key performance indicator. According to panel member two, whilst each set of measurements will be different, the structure will be the same. However, panel member three responded that at present there is no standard and that he does not like the term key performance indicator, as this potentially degrades the significance of their performance of ensuring ongoing performance. Panel member three stated "what concerns me is that you could end up with a tick in the box approach". However, what we need is some quantifiable measure to ascertain the system is performing what it is designed for, that is, the holes in the Swiss cheese are not getting bigger or aligning over time.

For this question, research panel one stated that key performance indicators are those items that you can use to monitor the effectiveness of the ongoing performance of each element of a system. If the key performance indicators are not being met, this could strongly suggest that a specific element is not delivering the full capacity of outcomes for which it was specifically designed. In applying panel member three's views that we require some quantifiable measure, research panel one reached a consensus that the key performance indicators for a PPS at the tactical level of management were based on the Defence in Depth elements. These measures commence with detection as an element, that is, the systems probability of detection, then the probability of successfully transmitting the alarm actuation, followed by a measure of accurate assessment (discrimination) of the alarm cause, then a probability of communicating that alarm source (probability of communication) to the appropriate response component of the system. Once detection has been achieved the next key performance indictors include delay aspects measured against the response capability, based on the mean averages, becomes the systems measures. During the feedback process all panel members

supported this approach, providing a consensus in-line with the pilot panel's and research panel one.

Consistent with panel member two, who responded that EASI key performance indicators are linked into the operational key performance indicators that achieve a Defence in Depth, the pilot panel and research panel one reported through consensus that constituent performance measures across the built environment, management processes and technology provide the operational level key performance indicators, which link in to the tactical level key performance indicators to achieve the system's macro state. For example, according to panel one member three's probability of detection "we look at the selection of components from their individual key performance indicators, then combine them together into a designed whole".

During the feedback process all panel members supported this approach to articulating the Defence in Depth key performance indicators. Although panel member three still does not like the label key performance indicator, he states "I don't disagree with this aspect; you need some methodology to evaluate the system. However, a significant cause of decay is a lack in professional management of the systems and what we don't want is a tick box process where it is perceived anybody can manage the system based on the boxes. It still requires professional knowledge".

8.2.9 Question nine: Key performance indicators and system effectiveness

Question nine asked panel members' in relation to their responses to question eight, do they believe the key performance indicators of systems are related to the systems effectiveness and how?

To this question panel member one responded "yes" and "no". According to panel member one, quantitatively the only way to get an indication or answer of how the system is doing is to look at the key performance indicators. However, with security there are so many variables and the key performance indicators are not so clear. In-line with this approach, panel member two responded "yes", as long as they are selected appropriately. They must show efficacy, achieving what they are designed to achieve as the key performance indicators aim to measure and monitor the systems level of efficacy. Panel member three responded that whatever you call them (the measures of

performance) they are related to the system's output. During the feedback process a consensus was achieved, in-line with research panel one that the panel support that the key performance indicators of the systems are related to the systems effectiveness.

8.2.10 Question ten: Security decay

Question ten asked panel members if, based on their experience, do they believe that security systems decay. This question related to Section 4.1 (Chapter 4), which postulates that all physical systems, if left to themselves (become closed) move towards a state of decay, that is, maximize their entropy. To this question panel member one responded "yes" they do, if they are not maintained, where panel member two responded "yes of course". Furthermore, panel member three stated "I believe security systems categorically decay". For example, Figure 8.4 indicates how decay is considered in engineering aspects, where for a lighting system, within the systems life cycle, maintenance considerations are programmed in to mitigate natural decay.

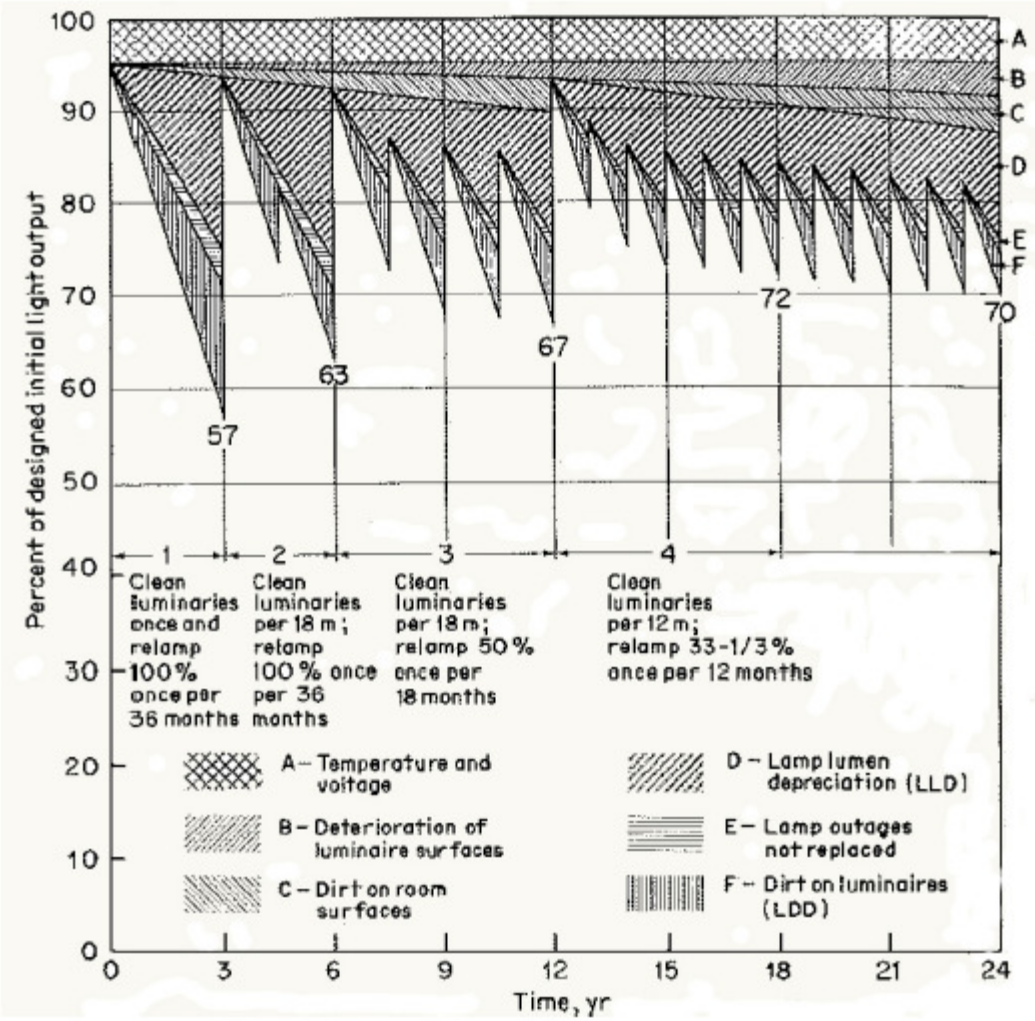


Figure 8.4 Panel member three's lighting system decay cycle. (Fink & Beaty, 1978, pp. 22-42).

However, panel member three stated "there is no reason in the world why you cannot keep the system working properly; however, to achieve this over time maintenance costs will increase". All panel members responded "yes" to this question, providing a consensus that based on their experience, they believe, congruous with this study's reviewed literature, security systems decay.

8.2.11 Question eleven: Understanding security decay

Question eleven asked panel members what their understanding of security decay was. Panel member one responded stating "the degradation of security systems, processes and hardware (security) arrangements, and personnel procedures". Panel member two expanded on this response, reporting that security decay is the decline in the efficacy (effectiveness) and efficiency of the security function, and correlating increase in risk. Also, the inappropriate response to security events which causes a new or updated security function which has no impact in altering or managing the risk, decay leads to adhoc security.

In response to this question, panel member three stated "people install systems that do not understand what underpins them". "We do design in parameters to facilitate for decay, however, the lack of knowledge and management of these parameters leads to security decay". That is, a number of factors leads to security decay, these include: lack of professional management; lack of continuity in educating management on how the system works; lack of formal training; where training is handed down rather than through formal processes; physical aspects decay through lack of maintenance; and technology gets old and decays. To this question panel member three, referred back to the Campbell Triangle (Figure 8.1); where according to panel member three, decay occurs in all three aspects: management, technology and physical engineering. Panel member three states, "You can build in quality that will maintain the system over time, for its life cycle, at the design stage".

During the feedback process research panel two were provided panel one member one's explanation, who stated;

> *Security system decay is the degradation in the performance of an element of the security solution, both as a single element performing a specific function and its role in supporting other elements in their function within the total system. This may not be a major failure of the system, but mere incremental decrease in performance that occurs over time. This decay may however occur incrementally and continue over an extended period to the point it has a significant impact on performance and effectiveness. Furthermore, this may be compounded further where this decay occurs over many or all of the elements within a system.*

All research panel two members supported this explanation. Consistent with research panel one to this question a consensus was achieved within research panel two supporting that decay embodies all aspects, constituents and elements within PPS. That is, all aspects of PPS decay, where decay occurs when performance falls below preset parameters, where a lack of knowledge and professional management of these parameters leads to decay, where based on the systems interrelationships, this decay affects the rest of the system.

8.2.12 Question twelve: An experience approach to security decay

Question twelve sought an evidence based approach, exploring real world examples of a time when panel members had experienced security decay. This question asked panel members to provide an example of a time when they experienced security decay. Panel member one reported experiencing security decay stemming from people's apathy. According to panel member one, for them, one day they give individuals an induction awareness lecture relating to security, and they walk out and forget it immediately. Then security processes decay over time when nothing happens, for example, people do not report security incidents, even though they have been told and trained to report them. This human failure breaks down the knowledge (intelligence) of what is occurring in the field.

To this question panel member two responded that decay is often why he, as a consultant, is called in to review security after an incident. According to panel member two, security decay is often found in non-systems arranged approaches to security, where isolated security measures are failing. As an example, panel member two explains that during a cash handling audit he conducted for local government, where he

found that whilst staff were of the belief they were protected by a duress alarm, the alarm had been disconnected for two years. In addition, the built environment maintenance had decreased due to leasing issues, where complete lack of security management lead to security decay. However, the operational environment had also changed, where cash movements had increased dramatically. In one of the cash handling facilities a successful robbery occurred, where in response to the robbery the security improvements were excessive after the fact.

Panel member three's response to this question was

> *I cannot name specific organisations", however, an audit I did was on an old system, where I had the privilege of speaking to the people who set it, when I conduct a security audit I look at: management; physical and technical systems aspects. The system I was auditing had clearly suffered decay because no-body wrote down in the first place what the system was meant to achieve (no measures of performance). I found that a lack of education and awareness existed in how the system is meant to operate.*

According to member three, to overcome such systemic decay the systems purpose and aspects needs to be written down, as a document. What occurs is that changes based on wants are implemented; however such changes are made to satisfy people; not to maintain the efficacy of the security plan. The system needs a defined security plan otherwise changes occur which lead to decay.

A consensus was reached within research panel two, supporting Figure 8.5, which highlights that consistent with each panel member's experience all aspects of PPS decay, where decay can occur in each aspect and based on the systems interrelations, affect another aspect of the system.

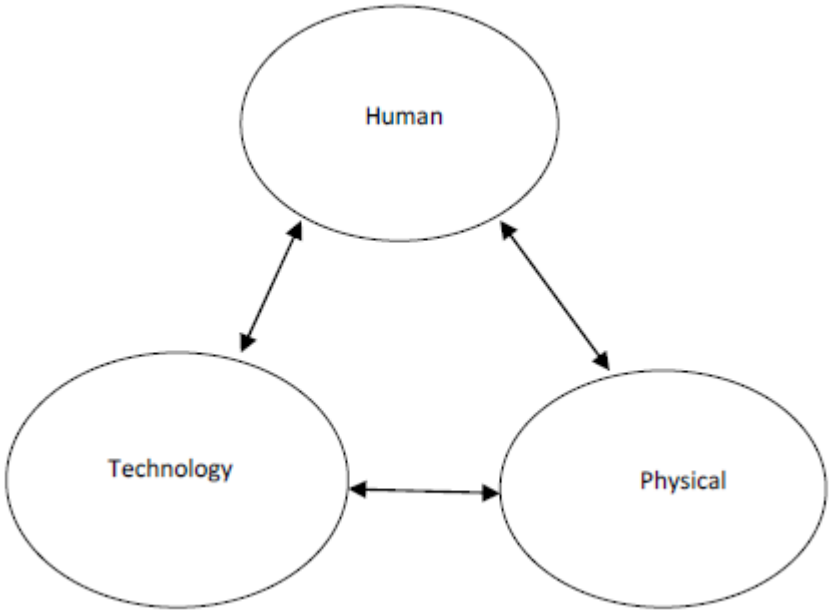


Figure 8.5 The interrelated aspects of a Physical protection System.

8.2.13 Question thirteen: A systems approach to security decay

Question thirteen asked panel members that in considering the argument that security controls decay, how did they think this occurs within a systems approach to security? Panel member one responded that normally a benign security environment leads to a reduction in the security program, that is, small changes. These changes eventually leave the system vulnerable so when something does happen, everybody's guard is down. This view was also considered by panel member two, who stated "systems require efficiencies, where spending cuts within the system occur which can lead to a large change within the system. However, panel member three once again referred to the Campbell Triangle, stating "decay occurs in each or all aspects of the triangle (Figure 8.1), when based on what a system is and how the system operates, decay occurs according to what underpins the system".

Panel member three's views are consistent with panel one member one's, who stated "I believe that security decay within a PPS occurs within its individual elements, them propagates through the system. Decay occurs at the base elemental level over time". To support this view, panel one member three, stated, "Any aspect of decay affects the rest of the system". For example, multiple false alarms can propagate through the rest of the system, when complacency sets in alarm inputs are not discriminated or reported, ultimately affecting the response aspect of the system. In addition, the pilot panel

responded that decay also affects the systems deterrence aspect as well. During the feedback process all panel member two participants responded that they support this articulation of how decay occurs within a systems approach to security, where panel member three states “yes it can, that’s a fact”.

A consensus was reached within this panel consistent with research panel one, that within a systems approach to security, decay starts in one aspect of the system; however, this can manifest simultaneously across several constituents. Then based on the systems interrelationships such decay propagates throughout the remainder of the system, ultimately affecting the systems response element and its deterrence aspects as well.

8.2.14 Question fourteen: Error propagation in Physical Protection Systems

Question fourteen asked panel members whether they support the premise that security decay within a PPS occurs within individual constituents, within the PPS and its effects propagate through the system from this point. Panel member one responded “yes”, stating; “something serious would have a knock on effect”. In addition, panel member two responded “yes”, small changes can lead to large security implications, much like a chain. A chain is only as good as its weakest link or point. When the weakest point breaks the result can be larger. In response to this question, panel member three once again refers to the Campbell Triangle (Figure 8.1), stating “yes, decay can occur in all three elements, based on the triangle”.

During the feedback process all panel members were asked if they support that a consensus was reached supporting this premise, based on the summary that “a system is a combination of various inputs, where each of these inputs has a function in performing a specific function and supporting functions of others (interrelationships) therefore small changes across many/all elements can have a major impact on the system at the macro level”, with all panel members supporting this interpretation.

8.2.15 Question fifteen: The Butterfly effect

Question fifteen asked panel members if they feel an effect referred to as the “Butterfly” effect, which suggests small input changes within a system can result in large changes at the macro output, applies to PPS. In his response to this question panel member one stated, “Yes it does”, where in his organisation, if they did not conduct drug and alcohol

testing, then this deficiency would lead to a security or safety event. Panel member two responded, “yes”, as discussed earlier, “one small change leads to larger chain reactions”. Panel member three responded every security system has two mission critical aspects. First, the context is established, where the system is analysed for single point failure. Second, you need to apply tools to look for the single point factor, which leads to the “Butterfly” effect, to overcome it. According to panel member three, compatibility of design considers inbuilt redundancy as key. If these aspects of system design do not occur, yes you will have the “Butterfly” effect.

For this question both the pilot panel and research panel one supported the application of the “Butterfly” principle to PPS. As such, a consensus was achieved across this study, supporting the argument that the “Butterfly” effect, certain conditions considered, does apply to a PPS.

8.2.16 Question sixteen: The effects of security decay

Question sixteen asked panel members what, based on their experience, did they think the effects of decay were. To this question panel member one responded that decay results in a more apathetic work force, where degradation may affect assets, personnel and service delivery of your product. Panel member two responded, “Invariably it will lead to a security related incident, a degree of loss, then in response, excessive spending, and potentially re-justification of the system itself”. Consistent with member two’s approach, member three responded that the effects of decay are directly proportional to the loss of risk management. This outcome was also mentioned by panel member two for question eleven, where according to panel member two, “decay relates to the decline in the efficacy and efficiency of the security function, and its correlating increase in risk”.

This outcome was also reported by member two of the pilot panel who stated “decay ultimately diminishes the security objective, increases the vulnerability of the asset, where this increase in vulnerability modifies the risk equation, where likelihood ratings become elevated and risk factors become increased”. Research panel one supported this aspect of decay where, through a consensus they supported that decay occurs at the component/constituent level, then degrades key performance indicators, reducing sub-system key performance indicators. Such decay ultimately affects the risk reduction aspects of the system, bearing a strategic impact on the organisation.

A consensus was achieved across this study, with all panel members supporting the argument that one of the salient effects of security decay is that risks increase as a direct result of decay within a security system. That is, where decay increases so does system vulnerability.

8.2.17 Question seventeen: Correcting security decay

This question asked panel members once decay has set in did they think its effects, both at the point of manifestation and throughout the remainder of the system are reversible. Panel member one responded "yes", but it does come down to leadership and management support, and of course the necessary resources. According to panel member one, "you need the will to turn decay around". This view was also reported by panel member two, who stated "yes they are reversible. Whether that happens comes down to management structure, through maintenance review, awareness recognition, and preventative maintenance". Panel member three also supported the argument that decay could be reversed, stating "absolutely". According to panel member three, as soon as decay has been recognised, through professional management of the problem, the decay can be overcome. However, panel member three states that usually independent audit is usually required to recognise decay.

During the feedback process (round two), panel members were provided with additional information from panel one which reported through consensus that procedural decay can be reversed and prevented through management, that is, ongoing monitoring and reviewing of the people component of the system. However, technical and decay can only be controlled and delayed through processes, where with proper maintenance decay can be slowed and managed. In response to this additional information, both panel members one and two supported this view.

However, panel member three provided an engineering clarification to this aspect, stating

> Technical aspects have a finite life, as do physical aspects (life cycle) between 8-12 years for technology, stating "and it should be 8-10 years but it is pushed to around 12". However, there is no reason why the system cannot be kept at its commissioned level of effectiveness, that is, at the original detection capabilities. Both physical and technology can be

maintained at that level over the cycle of the system. It can be maintained to ensure over the systems life cycle that it performs at the desired capabilities, commissioned level performance. This usually requires about 10% of its purchase prices per year over the life cycle.

A consensus was reached supporting research panel one's view that decay can only be countered if it is understood.

8.2.18 Question eighteen: Avoiding security decay

Question eighteen asked panel members if they believe decay within a PPS could be avoided. Panel member one responded "yes, possibly". However, according to panel member one, decay is a political concern rather than a technical aspect; it comes down to management's will. Panel member two also responded "yes", stating "through proper management, the monitoring and review of the systems key performance indicators, as the key performance indicators tell you what is going wrong". In addition, panel member two added, through a system driven by clear policy. Panel member three responded "absolutely, and unequivocally". It can be done (avoided) through professional management which looks after the technology, physical aspects and operational aspects. If you manage the triangle (Figure 8.1) you manage the system and avoid decay, that is, avoid the movement below the level of inbuilt redundancy (Figure 8.4).

During the feedback process (round two) panel members were provided research panel one's views, who argued that only procedural security decay can be avoided. However, technical and physical decay can only be managed and its effects delayed through proper monitored maintenance. In response to this information, panel member three stated "security decay is a quantifiable factor, decay must be managed so it does not fall below the inbuilt redundancy level". As such, it is argued that a consensus exists across the study that decay can be avoided or delayed through professional management, which focuses on the aspects of panel member three's triangle, where by focusing on the systems performance measures (key performance indicators) enables the professional management of the triangle, towards avoiding decay by ensuring the system does not fall below its levels of inbuilt redundancy.

8.2.19 Question nineteen: Security decay and risk management

Question nineteen asked panel members if they believe the concept of decay has a place in the risk management process. Panel member one responded "yes, the context section", decay is a risk. This view was also reported by panel member two who stated "yes, in establishing the context, security decay is a context, recognising it as a risk". Panel member three also responded yes, stating "you would have to assess for decay". To this question all panel members responded yes. In addition, a theme developed throughout this study, supported through consensus, that decay needs to be considered as a risk, recognised at the design stage, considered against its consequences, with a view to countering it where practicable as a risk treatment, towards designing out decay, then continually assessed for in the monitor and review stage.

8.2.20 Question twenty: Exploring security decay

Question twenty asked panel members if, based on their experience, is there any facet of security decay which they could add to the research enquiry. Panel member two responded that security decay is very common in various forms. However, according to panel member one, security decay will be constantly driven by organisational culture, then the resource prioritization, coupled with the threat landscape. This view was supported by panel member three, who stated;

> *Decay is caused by a lack in professional management, security management, that is: a lack of education, a lack of system awareness, and employing the wrong people to manage it, this goes back to quantifiable performance measures of the system". "I have come across systems in Asia where there is absolutely no decay. That is, there is no procedural decay, and the technological and physical aspects of the system are professionally managed in-line with the systems commissioning security management plan.*

For this question research panel one reported that the ongoing professional management of the system needs to be considered at the design stage, as part of the capital works submission, at a strategic level of management, where you need to identify whether the system you are putting in is achievable, and you can maintain the installed systems. This response was supported by panel member three, who responded saying "decay can be designed out, to a point, however, the system will cost around 10% of its purchase

price annually to maintain it over its life cycle, and yes this should be considered at the design stage.

8.3 Reflection

Reflecting over research panel two's interview data, based on the principle of triangulation, a measure of robustness has developed pertaining to the consistent themes and core aspects associated with security decay within a systems approach to security. Consistent with research panel one, research panel two supported that security commences at the strategic level of management, where a security systems purpose is established based on organisational risk reduction requirements. These requirements direct the tactical level of security controls towards managing the threats that pose a risk against organisational objectives. These controls are selected based on the Theory of Defence in Depth and Crime Prevention through Environmental Control (CPTED) achieved through the holistic integration of technology, physical controls and the built environment, all with a specified role, combined with procedures and management principles to achieve a pre-determined output goal. The aim is to implement a Physical Protection System (PPS) which is commission against a defined benchmark, being the defined risk reduction requirements "system's purpose".

Congruous with both the pilot panel and research panel one, research panel two agreed through consensus that PPS suffer from decay. Such decay relates to the degradation in effectiveness of individual constituents/components across all aspects of the built and natural environments (CPTED), physical components, technological controls, security procedures and management aspects within PPS. Due to the interrelated aspects of systems in general and specifically PPS, decay in one aspect of the system, if undetected or not treated/managed can propagate through the system from its point of manifestation, impeding the efficacy of higher order aspect of within the system, ultimately reducing the systems output product.

Research panel two agreed that security decay can be professionally managed, where the system can, through professional knowledge, management support and the provision of resources, be maintained to ensure it maintains its commissioned output performance levels over its life cycle. Research panel two reported that the management of decay starts at the design stage, in-line with research panel two, where decay is considered as a risk, the system is designed to either avoid decay, or mitigate it from the beginning of a

security project, and that the system must be reviewed as a "system" to detect and correct decay before it leads to a security event.

8.4 Reliability and validity

Consistent with Chapter 7, this stage incorporated the reliability and validity controls of triangulation and member checking. Triangulation was achieved using data inputs from all three panel members. This principle is underpinned by the argument that where consistent views are reflected and where consensus is achieved a higher level of confidence can be inferred towards supporting the core themes and principles evolving from the panel. In addition, member checking was incorporated into this panel, where during the second round feed-back process each panel member was presented with a transcript of their interview responses. Furthermore, each panel member was asked whether they supported the interpretations drawn from the data, and were provided with the opportunity to respond to these interpretations. These methodologies aimed to establish a level of trust towards the inductive analysis prior to moving forward to the deductive analysis phase.

8.5 Conclusion

This chapter presented the second stage of phase three, research panel two (n=3) interview analysis. This analysis provided a detailed account of participant's thoughts, feelings and understanding relating to the phenomenon of security decay. As with Chapter 7, the research questionnaire required panel members to reflect back on their experiences within their respective security domains, inputting meaning retrospectively. In addition, this panel was required to reflect on research panel one's experience with security decay towards developing stronger support towards their thoughts and feelings relating to entropic security decay.

This reflection enhanced and strengthened support towards the core themes which have evolved during this research enquiry, developing a consensus model within the study of entropic security decay. These themes were consistent with research panel one and included support towards the argument that security starts with a top down approach at the strategic level of management. Risk reduction requirements then guides the establishment of a systems parameters at the tactical level of management. This includes holistically integrating: technology, physical controls, the built environment, and procedural risk control aspects, all with a defined role are combined into an integrated

"whole". Consistent with research panel one, panel two supported that based on these themes Physical Protection Systems (PPS) are commissioned against a risk management benchmark, where all constituent aspects suffer decay. Decay within these constituents is inevitable if not managed.

Congruous with Chapter 7, this chapter also presented measures of reliability and validity (see Section 5.9), employing the principle of participant triangulation, drawing on multiple participant information sources relating to security decay underpinned by member checking, where during the second round interviews, panel members were provided written transcripts of their interview responses towards establishing a measure of truthfulness in this study's research analysis. Such an approach allowed the primary themes to be put forward in response to the study's research question, considered in the following chapter.

CHAPTER 9

STUDY INTERPRETATION

9.0 Introduction

This chapter presents phase four of the study, the deductive analysis of security expert's thoughts, feelings and experience with decaying security systems. The chapter draws on the conceptual review of security literature (Chapters 2, 3 and 4) and system decay (Chapter 4) benchmarks. The initial deductive analysis facilitated a response to the study's research sub-questions. This analysis then facilitated a response to the study's research question: Do security experts support the argument that security decay is represented by "the gradual degradation of the microscopic quantities (constituents), and, or, the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system"?

In response to the study's various research questions the chapter is divided into a number of sections. Section 9.1 provides the interpretative context for this study, explaining the interrelated aspects of Physical Protection Systems (PPS). Sections 9.2, 9.3 and 9.4 provide responses to their relevant research sub-question, utilizing an interpretative analysis and linking the deductive analysis from the three sub-questions forming a response to the study's research question. Section 9.5 presents a response to the study's research question. This response is supported by Section 9.6 the study's Security Decay preliminary item bank (Table 9.1), which provides a tabulated analysis of participants thought, feelings and experience with security decay. This chapter is then summarised with a conclusion (9.7).

9.1 Interpretation: The theory of entropic security decay

Security is a multi-disciplinary industry (Brooks, 2007, p. 1) and Physical Protection Systems (PPS) are heterogeneous, where such parts are brought together to achieve an output goal. To achieve this output goal a PPS aims to (A) deter, (B) detect, (C) delay and (D) respond to security events. Accordant with Section 4.3, the theory of entropic security decay, the sum of detect, delay and response (BCD) leads to A. In addition, detect (B) (Action) and delay (C) (Interaction) leads to response (D) (Consequence). These interrelations are achieved utilizing people, procedures, technology, and physical properties. These combined phenomena draw on many heterogeneous categories with varying domain specific specializations and are achieved by putting resources through a

process to achieve an output function. Such a process, indicated by Figures 2.6 and 3.6, conforms to the underpinning principles of General Systems Theory (GST) which provides the scientific systems frame for the study.

In combining this diverse literature, the study's research question seeks to determine if security experts support the argument that security decay is represented by "the gradual degradation of the microscopic quantities (constituents), and, or, the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system", as reported by Coole and Brooks (2009). It is argued this research question can be responded to through the deductive analysis and synergy of the following research sub-questions:

1. Do security experts support the systems approach to implementing effective security controls?
2. Do security experts support the argument that security systems can and do suffer from decay?
3. Do security experts support that security decay lies within the systems elements, constituents and their interrelationship?

9.2 Research sub-question one.

In responding to this study's overall research question, research sub-question one asks: *Do security experts support the systems approach to implementing effective security controls?*

In response to research sub-question one the aim is to interpret whether the study's research sample support a General Systems Theory (GST) approach, as it applies to physical security, to implementing effective security controls. As with the pilot study, this interpretation will be framed around the core principles underpinning GST. Congruous with the writings of Patton (2002, p. 454) (Section 5.8) this interpretation was achieved through a deductive, interpretative analysis, responding to the sub-question by drawing on the inductive analysis from each research panel and the study's benchmarks (Chapters 2, 3 and 4).

9.2.1 Research sub-question one: the systems approach to physical security.

The systems approach towards implementing effective physical security is supported by many published security authors (Underwood (1984, p. xi; Fennelly, 1997, p. 59; Garcia, 2001, p. 6; Fisher & Green, 2003, p. 164). For example, according to Fisher and

Green (2003, p. 147) every security program must be an integrated "whole". A view depicted by Fennelly (1997, p. 59) who states "maximum security is a concept, whereas alarm systems, physical barriers, guard forces and other components of a security system do not individually (silo thinking) achieve this". Congruous with Fennelly's (1997) view Underwood (1984, p. xi) emphasises the Gestalt approach stating "this combined should be seen as a whole". Accordant with this combined literature, both research panels reported that they support such a systems approach to security risk reduction, with all panel members responding "*yes*" they support a systems approach towards security. Furthermore, panel one member one added, "*as long as the systems are properly designed tools for the management of the security risk*". To this point, panel two member three stated, "*any security solution is based on an organisation's physical and technical needs, all of which must be compatible, homogeneous and completely supporting the risk mitigation process*".

Research panel one reported that a systems approach to security relates to how organisational security risks can be reduced using a top "down process", tying together separate security components/constituents that have a defined role. According to panel one, these components are interrelated with other aspects to facilitate the achievement of the systems overall goal. Such a depiction conforms to the writings of Bertalanffy (1968, p. 19) who considers a system to be "a set of elements standing in interaction". For example, panel one member two stated "*a system ties together a group of elements and constituents which maintain a role towards an overall outcome, where all aspects are interrelated*". This view was supported by panel one member one, who stated:

> "*the systems approach is a holistic approach, "seen as a whole". It requires structure with good interactions between components (highly interrelated) interface between components, "it's a top down process*".

Panel one's viewpoint is compatible with Midgley's (2003, p. 64) standpoint who states "the systems approach is focused strongly towards the interrelationships within, where, it is these interrelationships which tie the system together".

Research panel two's responses were congruous with research panel one, where consistent with the GST literature, panel two reported that a systems approach is a logical sequential process with a start and end point, which has a designated predetermined outcome. Panel two reported that a key factor in supporting a system

approach is that the components of a PPS are interrelated and interdependent, with each sub-system being a system of systems. That is, based on an orderly relationship each constituent within a PPS is unable to achieve its output without the cooperation and/or interaction of other constituent parts. For example, according to member three, "*every system has to be integrated into other systems, where each must play its part underpinned by mission critical infrastructure*", where uniform with panel one's opinion, utilizing a top down process. Such a consensus is true to the writings of Bertalanffy (1968) and Midgley (2003) where according to Midegley (2003) the systems approach is focused strongly towards the interrelationships within, these interrelationships which tie the system together.

In responding to sub-question one, accordant with Checkland's (1980) view that all physical systems are created for a specific purpose, panel one agreed that from a functional perspective security, and therefore the "Physical Protection System's purpose", at the strategic level of management is to reduce an organisation's risk exposure, both functionally and through deterrence. For example, member one stated "*security's role is the protection of people"*, where member two added "*the protection of assets, including: people, information and physical property, integrated to assist the organisation to achieve its specific business objectives"*. However, member one added "*it needs to be very functional*". Panel one's viewpoints were supported by panel two, where they reported that security's role therefore that system's purpose, at the "strategic level" of management, relates to the reduction of an organisations risk. For example, panel two member two stated "*security's role is to manage the various security related risks for specific organisations*". A view supported by member three who stated "*the role is to manage the threats that pose to risk to either: institutional, commercial and industrial organisations to mitigate risks*".

In evaluating the evidence supporting the systems approach to implementing effective security, research panel one suggested that organisational risk reduction is achieved through the holistic implementation of security's body of knowledge. According to panel one this body of knowledge saliently employs the theory of Defence in Depth, integrated with Crime Prevention through Environmental Design (CPTED), as a "system". For example, member one stated "*Defence in Depth is an absolute*", where member two stated "*I combine all aspects of Defence in Depth and CPTED*". Panel one's standpoint was also reported by panel two, where panel members agreed that such

risk reduction is achieved through the holistic implementation of security's body of knowledge, including Defence in Depth, integrated with Crime Prevention though Environmental Control (CPTED) and underpinned by security risk management. For example, member three stated "*I absolutely use Defence in Depth, with multiple rings of protection*'. Such views are congruous with the writings of Smith (2003, p. 8) who explains that Defence in Depth as a functional strategy has been applied to the protection of assets for centuries.

In pursuing a chain of evidence to respond to sub-question one, research panel one reported that the systems approach to security is the same as the systems approach towards achieving any other business objective. Member two stated:

> "*the systems approach to security is the same as the systems approach with any organisation aiming to achieve business objectives*". *That is*, "*the system broken down into its component parts relies on the other components within the system, where if one component is broken, or removed, this changes the whole system*".

According to panel one, a functional physical security system is achieved through the combining of procedural, physical and technological measures to protect an organisation's assets, which includes people, information and physical property through their ability to deter, detect, delay and respond to adversary threats. Such views are supported by the writings of Bertalanffy (1968, p. 18) who considers the systems approach to be focused on forms of "wholeness", where wholeness relates to problems of organisation where phenomena are not observable by respective parts in isolation.

Uniform with panel one's views panel two reported that this involves "a holistic approach from beginning to end", with member two stating "*starting with policy, then infrastructure, and how this infrastructure relates to the threats*". According to panel two, each aspect of a security system has a defined role and implemented in a manner where their interrelationships compliment and influence each other to reduce security risks. Both research panel's perspectives are congruous with Standards Australia (HB 167: 2006), Security Risk Management, which states, "In addressing security risk concerns, the key elements of organisational, community and individual security controls are those components which contribute to the management of risk through their ability to deter, detect, delay, respond to and recover from adversary attack".

Further evidence indicating support towards the systems approach stems from both research panels agreement towards a systems principle stipulated by Churchman (1968, pp. 42-43). This principle purports that as individual measures of performance of a system's constituent components increases so does the holistic measure of performance of the total system. In considering this proposition, research panel one supported that the key performance indicators of the system are related to the systems effectiveness. For example, panel one members two and three stated:

> *"we select individual components from their individual key performance indicators, then, combine then together into a "designed whole". The overall key performance indicator provides a strategic level of monitoring effectiveness...this is your means of ensuring elements are achieving your design goals".*

Research panel one agreed that within a systems approach to physical security, the key performance indicators of a PPS at the "tactical level" of management were based on the Defence in Depth elements. For example, member three stated "*the key performance indicators for a PPS are the core elements of Defence in Depth,* where the panel agreed that these start with the probability of detection, then the probability of successfully transmitting an alarm actuation, followed by a measures of accurate assessment (discrimination), then a probability of communicating that alarm source (probability of communication) to the appropriate response component of the system. Once detection has been achieved, the next key performance indicators include delay aspects measured against the response capability, based on the mean averages.

Panel one's viewpoint relating to the writings of Churchman (1968) was supported by research panel two. For example, members one and three stated:

> *"key performance indicators are those items that you can use to monitor the effectiveness of the ongoing performance of each element of a system. If the key performance indicators are not being met, this could strongly suggest that a specific element is not delivering the full capacity of outcomes for which it was specifically designed*". Congruous with this viewpoint, member three stated, "*I don't like the term key performance indicator, however,* w*hatever you call them, we need some quantifiable*

measures to ascertain the system is performing what it was designed for, that is, the holes in the Swiss cheese are not getting bigger over time".

Panel two supported that the key performance indicators (measures) for a PPS at the "tactical level" of management were based on the Defence in Depth elements. Member two stated "*this comes back to the Defence in Depth and the SANDIA (EASI) model, that is, the EASI key performance indicators*". Research panel two agreed that the key performance indicators (measures) start with detection as an element, that is, the systems probability of detection, then the probability of successfully transmitting the alarm actuation, followed by a measure of accurate assessment (discrimination) of the alarm cause, then a probability of communicating that alarm source (probability of communication) to the appropriate response component of the system. Once detection has been achieved, the next key performance indicators include delay and response aspects measured against the response capability based on mean averages, become the systems measures.

Both research panels consensus is consistent with the works of Spencer (1998, p. 3) and Garcia (2001, p. 246), where according to Spencer (1998, p. 3) overall system performance measures are achieved through the combining of component subsystem performance measures. Spencer's (1998, p. 3) view is uniform to panel one member three, who stated "*We select individual components from their individual key performance indicators, then, combine them together into a designed whole*", where according to Garcia (2001, p. 246) the overall performance measures for a PPS is the integrated measure of the detection, delay and response functions.

Evidence indicating the research sample's support towards the systems approach to implementing effective security also stems from their support towards Waldman's (2007, p. 272) standpoint that as part of a system changes, the nature of the overall system changes. Research panel one provided consensus support towards the proposition that small changes within a specific component can lead to a large change at the output of systems. For example, panel one member one stated "*due to the reliance on each element, small changes can have a domino effect on each of the other elements that combines to the system's base structure*". In addition, consensus support towards this principle within the context of physical security was also reported by research panel two. For example, panel members three and two stated:

"*absolutely*, (referring back to the Campbell Triangle), "*there is an interrelationship between the management, planning and design and the technology aspects of the system, any changes in one area affects the other interrelated areas*", where member two stated "*small changes in something like Defence in Depth, such as a passive infrared detection sensor not detecting renders the remainder of the system useless*".

Panel member two's example is supported by Garcia (2006, p. 14) who explains that to be effective, a detection capability must ensure its sensors are correct for their application, installed correctly, have a low nuisance alarm rate and be difficult for the threat to defeat. Where according to Adams, et al, (2005, p. 2) factors such as corroded wires could impede this capability, as stated by King (2008, p. 1) "it is the erosion of seemingly minor security controls which eventually leads to a security incident, resulting in a loss event".

Waldman's (2007, p. 272) standpoint according to Peirce (2000, p. 5) is what Lorenz (1968, p. 306) referred to as the "Butterfly Effect", which describes the principles of error propagation within a system. Accordant with this underpinning principle of systems theory, research panel one supported the application of Lorenz's (1968) "Butterfly" metaphor to physical security. For example, panel one member one stated:

"*a system is a combination of elemental inputs, the system is very much dependant on the correct operation of the effectiveness of each of these elements performing their function and supporting functions of other elements. Therefore, small changes in the elements, particularly where it occurs across many/all elements can have a major impact on "system" output at the macro level*".

Such support towards the "Butterfly" effect was also reported by research panel two, with all members responding "*yes*" they feel this effect applies to PPS. To this aspect of systems theory member one stated "*Defence in Depth relies on all its elements to be integrated and at their measures of effectiveness*". In addition, member two stated *"one small change leads to a larger chain reaction"*, where member three reported that unless the system is designed and managed for single point failure, that is, the appropriate amount of inbuilt redundancy, "*yes, you will have the Butterfly effect*".

9.2.2 Research sub-question one deductions

In responding to sub-question one the available evidence indicates that both research panels' views relating to the implementation of effective security controls are accordant with the various underpinning principles of General Systems Theory (GST). It is argued that both research panels consensually agree to the systems purpose, its functions and its architecture, and comprehend the various interrelations, organisation and orderly aspects which achieve the systems output goal. Furthermore, both panels thoughts relating to how, based on the systems interrelating aspects, small changes in one area of a system are associated with changes throughout the remainder of the system, and how these changes directly affect the various sub-systems and "whole" systems macro-state (key performance indicators) are congruous with the literature underpinning GST. Based this analysis, it is put forward that in response to sub-question one, it can be argued that both research panels do support the systems approach to implementing effective security controls.

9.3 Research sub-question two: The phenomenon of security decay

Research question two directly relates to the premises of Underwood (1984) and McClure's (1997) writings, where according to Underwood (1984, p. xi) "security decay" is the most serious threat to a security systems and "security decay" must be expected. Research question two asks, "Do security experts support the argument that security systems can suffer from decay"? In response to research question two, the aim was to interpret whether panel members support the argument that "security systems" suffer from decay. Accordant with Patton (2002, p. 454) (Section 5.8) this interpretation was achieved by drawing on the conceptual review of literature as an existing benchmark to deductively test and affirm the research data in response to this research question. This interpretation was framed around the panel's understanding of their real world experience (evidence) relating to decay within Physical Protection Systems (PPS), achieved by comparing the data analysis of the panel interviews to the embodying literature presented in the conceptual review of literature (Chapters' 2, 3 and 4).

9.3.1 Research sub-question two Interpretation: security decay

Accordant with Underwood (1984, p. xi; Howlet, 1995, p. 222; McClure, 1997; King, 2008, p. 1) research panel one reported that they believe "security systems" suffer from decay. For example, all members responded "*yes*" they believe security systems suffer from decay, where member one stated "*I do believe that security systems can and do*

experience decay", with member two stating "*yes they do decay*". Such a consensus supporting the argument that security systems decay was also reported by research panel two. Again all panel members responded "*yes*", where member three stated "*I believe security systems categorically decay*". Member three's view was supported by member two, who stated "*security decay is common in various forms*".

The results of this question are uniform with King (2008, p. 1) who applies Lovey and Manohar's (2007, p. 99) and Styer's (2000, p. 1) views to explain the decay of physical protection systems, stating that security controls inevitably degrade over time as a result of natural entropy. For example, panel two member one responded, "*yes they do, if they are not maintained*". Member one's point is congruous with Howlet (1995, p. 220) who stated "without proper maintenance the system will not work". In explaining his understanding of security decay, panel one member one, stated:

> "*security decay is the degradation in the performance of an element of the security solution, both, as a single element performing a specific function, and the elements role in supporting other elements in their function within the total system*".

This approach was supported by panel one member three, who stated "*key performance indicator reduction at the micro-level reduces key performance indicator at the macro level*". Member three's viewpoint is compatible with Tables 4.1 and 4.2 (Section 4.4), and conforming to Pitzer's (1995, p. 30) sentiment that entropy is an extensive property, where the entropy of a system is equal to the sum of the entropies of its parts (see Equation 26). That is, the entropy of a system is a macro state. Such views were also reported by research panel two, where member two stated, "*decay relates to the decline in the efficacy and efficiency of the security function, and its correlating increase in risk*". Such a view was also reported by member three, who stated "*the effects of decay are directly proportional to the loss of risk management*". Members two and three's views indicates that as decay increases, risk reduction decreases and opportunity for a defined threat increases. These views are consistent with the propositions represented in Figure 4.2 and Equation 28.

Furthermore, panel one member one adds "*decay may not be a major failure of a system, but more incremental decrease in performance that occurs over time*". Nonetheless, panel member two added, "*decay may occur incrementally or rapidly*".

For example, procedural decay may occur rapidly. Furthermore, decay may continue over an extensive period, to the point where it has significant impact on performance and effectiveness. This view was supported by the pilot panel's findings, suggesting that if one component fails, its key performance indicator is reduced and such component failure reduces the effectiveness of the response force key performance indicator, ultimately reducing the overall protection process, (see Section 4.11, Tables 4.1 and 4.2). In addition, according to panel one member two, decay may be further compounded where it occurs over many or all elements within a system, which can lead to major failure.

The panel's views relating to security decay are congruous with the writings of Konicek and Little (1997, p. 18. For example, Konicek and Little (1997, p. 18) state, "a security systems is only as good as its parts, when a single part fails, this failure can cause degradation of the total system. A standpoint supported by Garcia (2006, p. 26) who states, "system effectiveness can become degraded through the reduction in effectiveness of individual components", where according to Standards Australia HB167 (2006, p. 62) a small change in control effectiveness may have a substantially magnified effect on vulnerability. It is these combined viewpoints which draw on the writings of Lorenz (1968, p. 306) who referred to this aspect of systems theory as the "Butterfly Effect", to describe how error propagation occurs within a system.

In examining the argument that security systems decay, research panel one considered that the effects of decay were as heterogeneous as the system itself, where according to panel one member three, "*decay leads to a breakdown in reliability, and increases the risk of significant events occurring*" (see Equation 28). Research panel one agreed that all Physical Protection Systems (PPS) decay, where all physical and technical aspects components have a life cycle. However, according to research panel one, the effects of decay can be managed, delaying its onset through processes, that is, with monitored maintenance. For example, member one stated "*decay is like risk, you can mitigate some decay, you can accept some decay, and you can reduce the impact*". This view is accordant with the writings of Byeon (1999, p. 287) who states "open frame systems are able to circumvent the effects of the second law of thermodynamics (entropy law) through their feedback processes".

Congruous with research panel one panel two, member three stated, "*decay occurs in all aspects: management, technology and physical engineering*". Panel two supported the argument that all PPS decay, stating "all physical and technical components have a life cycle", where congruous with member three, "decay occurs in each, or all, aspects of the triangle (see Figure 7.4), based on what a system is, and how the system operates, decay undermines the system". The research sample's views are congruous with the writings of Lovey and Manohar (2007, p. 99) and Styer (2000, p. 1) who argue that all physical systems, if left to themselves, tend to maximise their entropy true to the laws of thermodynamics. Within the context of physical security, this view is supported by Underwood (1984) and Howlet (1995), where according to Underwood (1984, p. 252) whatever security measures were established initially, they would not last forever, where according to Howlet (1995, p. 219) "that from the time of taking a system into use, it will start to deteriorate".

In response to sub-question two, panel two member three felt that a number of factors lead to security systems decaying. Member three stated:

> "*people who have systems installed that do not understand what underpins them, systems are designed with parameters to facilitate for decay, a lack in professional system management, that is, a lack of knowledge to manage these parameters, a lack in education, in formal training leads to decay within Physical Protection Systems*".

Member three's views are consistent with the writings of Garcia (2006, pp. 24-25) who states "systems engineering considers both business objectives and the technical needs of customers. This is an approach concerned with the integration of functional, technical and operational requirements, where integration includes physical, electrical, customer needs, technical performance, safety, reliability, procedures, personnel, training, testing and life cycle of the systems solution". Congruous with Garcia's (2001, pp. 24-25) writings, panel two, member three stated:

> "*there is no reason why the system cannot be kept at its commissioned level of effectiveness. That is, at the original detection capabilities, both physical and technology can be maintained at that level over the cycle of the system. It can be maintained to ensure over the systems life cycle, that it performs at the desired capabilities "commissioned level performance*".

Such a standpoint was supported by Howlet (1995, pp. 219-220) who states "no system, however well designed, can be completely reliable without proper maintenance. If left without attention (proper maintenance), it will become unserviceable, that is, not work. The operator may not be aware of it, but the system will now perform as intended". Congruous with Garcia's (2006) writings and according to member three, the avoidance of decay requires professional management of the system. Panel two member three further states, "*I have come across systems in Asia where there is absolutely no decay. That is, there is no procedural decay, and the technological and physical aspects of the system are professionally managed in-line with the systems commissioning security management plan*". This experience suggests a cultural aspect to security decay.

Nevertheless Underwood (1984, p. xi) wrote, *decay should be avoided and countered where possible, most of all, it must be expected*. In relation to countering decay panel two member one, responded "decay is reversible, however it comes down to leadership and management support, and of course the necessary resources, stating "*you need the will to turn decay around"*. This view was supported by member three, who considered security decay to be a phenomenon which could be both reversed and avoided, stating:

> "*as soon as decay has been recognised, through professional management of the problem, "decay" can be overcome*". "*Decay is a quantifiable factor; decay must be managed so it does not fall below the inbuilt redundancy level*".

These views are compatible with the writings of Byeon's (1999, p. 287) who explains that open frame systems are able to circumvent the effects of the second law of thermodynamics (entropy law) through their feedback processes (management and maintenance).

In responding to sub-question two, all panel one members reported real world examples of how they have experienced decay or degradation within PPS. For example, panel one member one provided a substantial list of examples where he has observed decay manifestation within PPS. member one states:

> *"poor maintenance of the environment in which PPS components are deployed leads to decay, based on the interrelated aspects of PPS elements. That is, weeds or feral growth in detection zones triggers high nuisance alarm rates, or poor electronic system maintenance having the same effect"*.

As Howlet (1995, p. 220) writes, without proper maintenance the system will not work, where he states "ideally maintenance should be considered at the design stage, and that maintenance costs are very closely tied to the original design specifications of the system. Furthermore, member one responded that a lack of ongoing operator training, or operator training through handed down experience rather than through formal training processes ultimately leads to decay in the system as a "whole". In addition, panel one member two provided similar views, stating:

> "*I have noticed that as staff competencies fluctuate, this fluctuation alters individual key performance indicators, where decay occurs in relation to the reduction in competencies and capabilities of the people components*".

Member two's experience was supported by member three who responded similarly with one of panel member one's examples, stating "*staffs' lack of familiarization/awareness with procedural security during system checks leads to decay within the system. Such procedural decay results in technical decay; as it is not known if systems are truly working around its designed parameters*". The human aspect of security decay was considered by Underwood (1984, p. 250) who states "it is important that the security operation is subject to the same management-by-objectives as the other management functions in an organisation". In addition, all panel two participants reported real world examples of how they have experienced decay or degradation within PPS. For example, panel two member three, stated:

> "*I conducted a security audit of an old system; when I do an audit I look at management, physical and technological aspects. The system I was auditing had clearly suffered decay because no-body wrote down in the first place what the system was meant to achieve (no measures of performance). I found that a lack in education and awareness in how the system was meant to operate lead to decay*".

An example based support towards the phenomenon of security decay was also provided by member two. Member two stated "*decay is often why I as a consultant is called in, in the first place, to review security after an incident. In our experience we find that security decay occurs in non systems arranged approaches to security, where isolated security measures are failing*". Member two states "*during a security audit I found that whilst staff believed they were protected by a duress system, the system had been disconnected for two years*". Uniform with research panel one, a consensus was

achieved that decay embodies all aspects, constituents and elements within PPS. Research panel two reported that all aspects of PPS decay, where such decay occurs when performance falls below the system's preset parameters. In addition, panel two member two responded "*after a security event, often the security improvements become excessive"*. This view was supported by Underwood (1984, p. 249) who writes, "the immediate reaction is often to increase the security measures established, but in fact this is not usually necessary and all that may be required is the re-establishment of the intended level of protection".

9.3.2 Research sub-question two deductions

In response to sub-question two the evidence indicates that a consensus was reached within the study, where both research panels one and two supported the argument that security systems "do suffer from decay". The research sample's outcome is congruous with the pilot panel's finding. Accordant with the pilot panel's outcome, the evidence suggests that such decay relates to a failure to maintain security "systems" at their commissioned operating levels of effectiveness, diminishing their ability to deliver the required output goal (risk reduction).

9.4 Research sub-question three

Research question three directly related to the premises of Coole and Brooks (2009), and focused on the heterogeneous aspects of the Physical Protection "System" (PPS), in response to writings of Lovey and Manohar (2007, p. 99) and Styer (2000, p. 1). Lovey and Manohar (2007, p. 99) and Styer (2000, p. 1) stated that "all physical systems, if left to themselves, tend to maximise their entropy, true to the laws of thermodynamics". Accordant with the writings of Lovey and Manohar (2007, p. 99) and Styer (2000, p. 1) sub-question three asks "Do security experts support that security decay lies within the systems elements, constituents and their interrelationship"?

9.4.1 Research sub-question three Interpretation

The study asked panel members that in considering the argument that security controls decay, how did they think this occurs within a system approach to security? Too this question panel one member one stated:

> "*decay within a PPS occurs within its individual elements, and propagates through the system. Decay occurs at the base level over time. This decay at*

elemental level occurs through many causes, and the effect can result in major system breakdown".

Panel one member two responded similarly, stating "*decay occurs at the element level, the efficacy of the system decays as small changes occur, changes start small, however, spread when not detected and managed*", where according to member two, procedural decay starts initially, stating "*procedural decay occurs when staff no longer maintains their initial personnel based key performance indicators, where this initial decay propagates throughout the remainder of the system*". Panel one's viewpoints are compatible with Section 4.4 (Tables 4.1 and 4.2) which indicate how changes in a Physical Protection System's (PPS) microstates have a direct effect on its macro-state output measure.

Panel one's thoughts relating to security decay from a systems approach were also reported by research panel two. For example, panel two member three, stated "*decay occurs in each, or all aspects of the triangle* (Figure 8.1), *where based on what a system is, and how the system operates, decay occurs in-line with what underpins them*". During Delphi method round two all research panel two participants responded that they support research panel one's articulation of how decay occurs within a systems approach to security.

A consensus was reached within research panel two congruous with research panel one that within a systems approach to security, decay starts in one aspect of the system; however, this can be manifest simultaneously across several constituents. Then based on the systems interrelationships, decay propagates throughout the remainder of the system. Such propagation ultimately affects the system's response element and its deterrence aspects as well. For example, panel two member one stated "*something serious would have a knock-on effect*", where member two states, "*small changes can lead to large security implications, much like a chain. A chain is only as good as its weakest link or point. When the weakest point breaks, the result can be large*". Both research panel's views relating to security decay from a systems approach conform with the early works of Isacc Newton who stated "the extension, hardness, impenetrability, mobility and inertia of every object, depends on, the extension, hardness, impenetrability, mobility and inertia of its component parts (The Open University, 1976, p. 68).

Within the context of PPS, Newton's views are supported in the writings of Garcia (2006, p. 29) who states "system effectiveness can become degraded through the reduction in effectiveness of individual components". As Koniceck and Little (1997, p. 184) state "when a single part of a security system fails, such failure can cause degradation within the total system". Uniform with this view, panel one member three stated "*the selection of components is made based from their individual key performance indicators, such as probability of detection, nuisance alarm rate etc, then we combine them together into a designed "whole*" .

A consensus was reached within the research panel one that decay occurs within a PPS, within individual constituents and its effects propagate through the system from this point. For example, panel one member one stated:

> "*a system is a combination of elemental inputs, the system is very much dependant on the correct operation of the effectiveness of each of these elements in performing their function and supporting functions of other elements*".

The panel's responses are uniform to the literature stemming from Bertalanffy (1950; 1968) and Konicek & Little, 1997; Mosely and Coleman, 2000; Garcia 2006; Broder, 2006; Waldman, 2007). Furthermore, in providing his examples of decay manifestation within a PPS, panel one member one stated:

> "*each of the above may have only minor degradation, or degradation that is not significant in its own sphere, the accumulated impact however, presented significant risk. In this instance it was clear that the input changes or performance degradation with each element had the potential to result in large change or performance degradation without evaluation in consideration of the total PPS*".

Such a consensus was also reached by research panel two. For example, panel two member three stated, "e*ach system is a system of systems. Each system has to be integrated into other systems, where each must play its part, underpinned by mission critical infrastructure*". Research panel two supported the views of research panel one, who reported that the systems approach to security embodies the Physical Protection System (PPS) broken down, into its component parts, which relies on the other components within the system, where if one component within the system is broken or

removed, this changes the whole system. Once again, this view is uniform to Koniceck and Little's (1997, p. 184) who stated "when a single part of a security system fails, such failure can cause degradation within the total system".

The combined panels thoughts, feelings and experiences towards security decay are accordant with Section 4.3.2 (Chapter 4) which discusses the effects of entropic decay on PPS. Section 4.3.2 purports the original decay within a PPS expands to the boundaries of that specific subsystem component, resulting in a failure within this specific part of the system. Based on the system interrelationships between the Defence in Depth elements, results in the system becoming disordered, ultimately causing this point disturbance propagating through the remainder of the defence in depth system. In considering this aspect of security decay, all panel members supported the application of the "Butterfly" metaphor to PPS, which has been used to articulate such interrelated aspects of specific systems. For example, according to panel one member two, *"system training has a macro-level output through the system. However, over time the training levels set at the system's commissioning are allowed to decline, then the level of staff competency declines, affecting the remainder of the system"*. This view was also reported by panel one member one, and panel two member three.

9.4.2 Research sub-question three deductions

Based on the available literature, it is argued that the evidence indicates both research panels support the argument that security decay lies within the systems elements, constituents and their interrelationships. That is, based on panel member's responses, all panel members' support that decay occurs at the constituent level, manifests, then expands to incorporate and affect specific sub-system key performance indicators. Then expands to the specific Defence in Depth element for which it is located. Such decay then propagates throughout the remainder of the Defence in Depth system from that point, ultimately affecting the systems macro-state key performance indicator (Pi) based on the systems interrelations, consistent with the writings of Bertalanffy (1950; 1968).

9.5 Research question Interpretation

Results of the study indicates that both research panels, and the pilot panel's views relating to the implementation of effective security controls are congruous with the measures discussed in the study's security benchmark (Chapters 2, 3 and 4). Accordant with the underpinning principles of General Systems Theory (GST) all study panels

understand the systems purpose, its functions and its architecture, and comprehend the various interrelations, organisation and orderly aspects which achieve the systems output goal. Furthermore, all panels support and understand how, based on the systems interrelating aspects, small changes in one area of a system are associated with changes throughout the remainder of the system, and how these changes directly affect the various sub-systems and "whole" systems macro-state (key performance indicators).

In addition, a consensus was reached across the study's participant sample with the pilot panel, and research panels one and two supporting the study's security decay benchmark premise (Chapter 4) that physical security systems (Physical Protection Systems) "do suffer from decay". The panels supported that such decay relates to a failure to maintain security "systems" at their commissioned operating levels of effectiveness" and to deliver their required output goal (risk reduction).

Furthermore, all panels supported the argument that security decay lies within the systems elements, constituents and their interrelationships. That is, based on participants responses, all panel members support that decay occurs at the constituent level, manifests, then expands to incorporate and affect specific sub-system key performance indicators, then expands to the specific Defence in Depth element for which it is located, propagating throughout the remainder of the Defence in Depth system from that point. Such decay propagation ultimately affects the systems macro-state key performance indicator (Pi) based on the systems interrelations, true to the writings of Bertalanffy (1950; 1968).

In responding to the study's research question it is argued that the available evidence from the study indicates that the participant sample (N=9) collectively supported the view that security decay can be represented as "the gradual degradation of the microscopic quantities (constituents), and, or, the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system".

9.6 Security decay preliminary item bank

Consistent with the writings of Loewanthal (2001, p. 3) (Section) Table 9.1 presents the security expert's pool of variables and factors (item bank) associated with the concept of security decay. This item bank is underpinned by the expert panel's thoughts,

feelings and experience with degradation within Physical Protections Systems (PPS). Table 9.1 highlights participant's real world experiences and explanations relating to security decay.

Table 9.1 Security decay preliminary item bank

PPS Components	Decay Categories		
	Condition	Phenomenon	Consequence
Technical	Poor detection system maintenance	Triggers increased nuisance alarm rates	Staff ignore alarm, or, do not assess alarm causes properly reducing probability of accurate assessment KPI.
	Incorrect technical maintenance	Causes high nuisance alarm rates.	Staff become complacent, resulting in accurate assessment as a KPI diminishes.
	Degradation of lighting system	Light lamp failure affects the performance of CCTV systems.	Diminished ability to assess (discriminate) alarm sources.
People	Lack of professional management of the security function, as a system.	System decays across all aspects of the management triangle, technological, physical and procedural.	Eventually a security related event will occur due to a diminished risk reduction program.
	Poor, or lack of system testing, or, breaches of system testing procedures.	Accurate state of system efficacy not established.	Potential sub-system vulnerability manifestation.
	Poor formal training for new staff, where training occurs through handed down processes.	Incorrect procedures or bad habits passed on to new staff.	Cultural decay established within the human aspect of the system.
	Lack of qualified staff continuation training.	Decay in response requirements for non-routine events.	Decay in efficiency and efficacy of staff responses.
	People changing the built environment to suit personal requirements.	Changes various system inputs, discordant with their design specifications.	Can trigger small changes in various sub-system KPI's which are not understood until a security event.
	Fluctuations in staff competencies	Alters specific sub-system KPI's for where competency reduction is	Staff may not react in an efficient and effective manner, based

		related to.	on system design requirements.
	Poor physical attribute (lighting and air conditioning) within CCR.	Provide inappropriate output conditions.	Poor staff concentration and focus, degrading operator effectiveness within CCR.
	Standard operating procedures being modified without reference to holistic system requirements (to address minor elemental issues).	Degrades the performance of the operating system as a "whole".	System may not perform accordant with design specifications.
	Poor communication structures between Central Control Room (CCR) staff and security management and operational staff.	Degradation in efficacy across "whole" system.	System may not perform efficiently against defined threat, accordant with designed specifications.
Physical	Lack of maintenance of PPS environments (weeds and feral growth).	Triggers increased nuisance alarm rates	Staff ignore alarm, or, do not assess alarm causes properly reducing probability of accurate assessment KPI.
	Deterioration of delay physical elements.	Barrier effectiveness based on commissioning measures degrades against defined threat.	This changes the delay time along an adversary's path, altering the system's commissioning Pi.
	Physical components designed without considering physical environment impact.	Leads to premature physical decay.	Physical components may not perform as designed when put under defined threat stress.

(Adjusted from Gillham, 2000, p. 68).

9.7 Conclusion

This chapter presented phase four of the study, the deductive analysis of security expert's thoughts, feelings and experience with decaying security systems drawing on the outcomes of phase one, the conceptual review of literature as security (Chapters 2, 3 and 4) system decay benchmarks. Phases two (Pilot study) and three (Research panels one and two) provided the interview data for this deductive analysis. The study's research question was responded to by drawing on the deductive analysis of the three

research sub-questions. Research sub-question one asked: Do security experts support the systems approach to implementing effective security controls? Section 9.2 presented evidence that security experts do support the systems approach to implementing effective security controls. Research sub-question two asks: Do security experts support the argument that security systems can and do suffer from decay. Section 9.3 presented evidence that security experts do support the argument that security systems can and do suffer from decay. Research sub-question three asks: Do security experts support that security decay lies within the systems elements, constituents and their interrelationship? Section 9.4 presented evidence that security experts do support that security decay lies within the systems elements, constituents and their interrelationship.

Based on the sum of security experts responses to the research sub-questions, it is argued that it can be interpreted that the study participants do support that security decay can be represented by "the gradual degradation of the microscopic quantities (constituents), and, or, the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system". These results will be taken forward to Chapter 10 where the study's conclusions can be drawn, providing study findings, limitations and recommendations.

CHAPTER 10

CONCLUSIONS, LIMITATIONS AND RECOMMENDATIONS

10.0 Introduction

This chapter presents the study's conclusion, methodological limitations and recommendations. Section 10.1 provides a summary of the study's research enquiry and presents how the research data generated from this enquiry relates to previous works focusing on security decay theory. Section 10.2 provides a management philosophy and methodology (Figure 10.1) towards maintaining Physical Protection Systems (PPS) at their commissioned levels of effectiveness. In addition, this section presents a summary of how security decay directly relates to the degradation within a security "system" based on its designed purpose in relation to its defined threat (Figure 10.2). Furthermore, Section 10.2 presents the study's formal research findings. Limitations of the study are presented and discussed (Section 10.3), and recommendations for future investigations are made (Section 10. 4). Section 10.5 summarises this research enquiry providing the study's conclusion.

10.1 Summary of the study

As previously stated, to date there is a dearth of dedicated published literature underpinned by academic research pertaining to security decay. In considering such an academic void Koffka (1963, p. 4) explains that in contemporary times, knowledge is regarded as an aim in its own right, stating "find facts, and again find facts; when you are sure of your facts, try and build theories...But your facts are more important". The current knowledge and theory relating to security decay stems from the previous works of Underwood's (1984) writings in his book "The Security of Buildings", or McClure's (1997) thesis "Security Decay: The erosion of effective security", which is a dedicated published research works towards discussing the phenomenon of security decay. McClure (1997, p. 71) stated "s*ecurity decay theory is a long way from extending beyond being an abstract model*", where security decay theory is primarily concerned with the influence apathy has on security and how management react to risk materialization when decay is evident. However, McClure (1997, p. 71) recommended the pursuit of a more functional model of security decay.

In pursuing McClure's (1997, p. 71) recommendation, Hamlyn (1969, p. 16) states "explanations in science are and can be divided into two kinds, those which make reference to laws, and those which make reference to theories". In considering Hamlyn's (1969, p. 16) views, this study approached the investigation into security decay by drawing on both theory and laws. That is, the theory of Defence in Depth which achieves a functional security system, and General Systems Theory (GST) which provides a scientific frame for considering systems of all types, regardless of their purpose and components. In combining these theories, this research then drew on the laws of thermodynamics (Entropy law) to explain the natural decay occurring in systems of all types, regardless of make-up. This approach was considered necessary given the variety of different sciences which make a Physical Protection System (PPS) possible, where the one science which binds all various sciences to achieve the systems output goal is systems science (Bertalanffy, 1950; 1968).

In investigating the concept of security decay from a systems approach, contrary to McClure's (1997) works, this study argues apathy is not the salient factor driving decay. The study indicated that for Physical Protection Systems (PPS) apathy can actually be a product state, manifested in the poor management of PPS. For example, panel one member three, stated "*all technology decays, as technology decays it constantly false alarms, then staff ignore them, where ultimately they lose confidence in the system and their work decays*". Such a view was also reported by Howlet (1995, p. 222) who stated:

> "*from the time of taking a system into use it will start to deteriorate. No system, however well designed, can be completely reliable without proper maintenance. If left without attention it will become unserviceable...A poorly maintained security system will have many unexplained alarms, leading to the guard force losing confidence in the system and eventually ignoring a true alarm as just another false alarm. However, the operator may not be aware of it, but the system will not perform as intended*" (Howlet, 1995, p. 220).

Howlet's (1995, p. 220) viewpoint was supported through consensus across this study. The study identified that decaying work practices, manifested in technology decay (high nuisance alarm rates), can lead to a state of apathy. Such an account indicates that apathy can be a product state of decay, manifested in a specific constituent within the system, propagating to directly affect the human aspects rather than the salient driving

factor. Consistent with this view, panel two member three stated, "*a lack of professional management underpinned by poor knowledge and awareness of how the system was designed to work (manage the risks) leads to decay*". According to member three, "if you manage the triangle (Figure 10.1), you manage decay". A common theme emerged across the study from both the textual literature (Chapters 2, 3 and 4) and the panel interview data (Chapters: 6, 7 and 8), that as a result of the heterogeneous nature of a PPS, decay in one specific area (point disturbance) due to the interrelationships, propagates throughout the remainder of the PPS, ultimately changing the performance (Macro-state) of the system as a "whole".

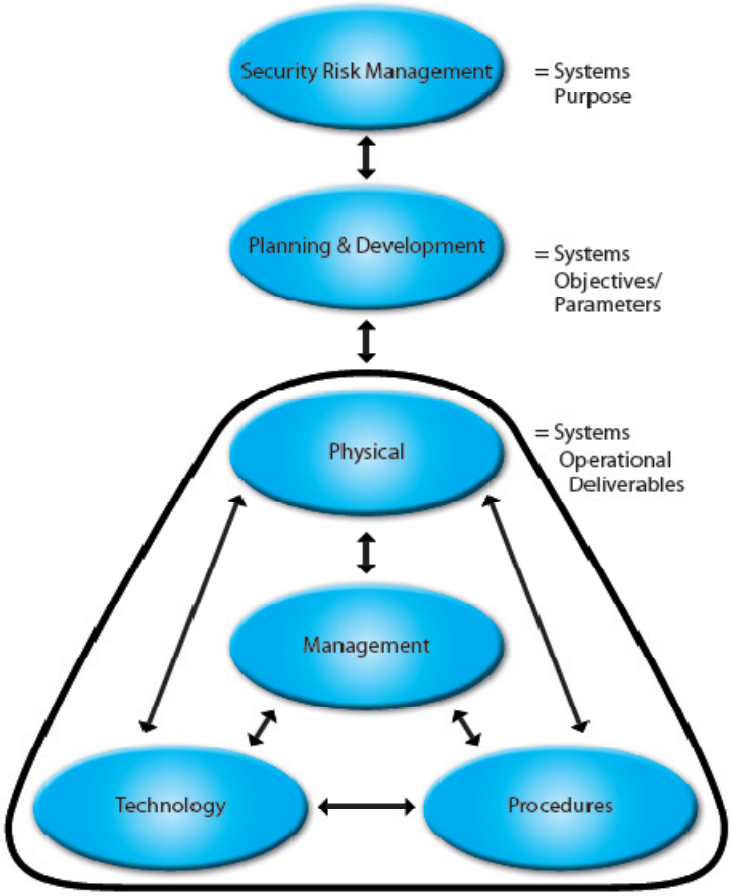


Figure 10.1 Security system management diagram.

Based on the available literature, the study proposes that for PPS to maintain their commissioned measures they must be managed as a "system", in-line with its original, or reviewed, design parameters, or as stated by Underwood (1984, p. 250) "managed by objectives". For example, Figure 10.1 graphically indicates a pyramid analogy of how the system starts with a top down approach, where based on a defined threat (systems purpose) the systems objectives and parameters are established, where accordant to Figure 8.1 (Campbell Triangle) the operational deliverables are implemented and

managed to ensure the system maintains its commissioned measures of performance or key performance indicators over time. However, if the system is allowed to decay, the effects of this decay propagate back up the pyramid, in a bottom up approach. Such propagation diminishes the risk reduction efforts increasing organisational risk exposure (see Equation 28). That is, it is argued security decay transcends all levels of systems management.

In addition, the study asserts that security decay is about the degradation within a security "system" based on its designed purpose in relation to its defined threat. For example, Howlet (1995, pp. 219-220) stated "without proper maintenance the system will not work", where the operator may not be aware of it, but the system will not perform as intended. This view was articulated by panel one member one who stated "*decay may not be a major failure of this system, but more incremental decrease in performance that occurs over time*". Based on the evidence, the study recognises that whilst a system may have a measure of decay, it is most probably still at a level where it would be effective against lower level, or lesser threats. As panel two, member three stated "*security role is to manage the threats that pose a risk to either: institutional, commercial and industrial organisation to mitigate the risks*".

It is argued decay in just one of the Defence in Depth elements may for some adversaries provide the necessary vulnerability, facilitating their opportunity to execute an attack and breach the layers of security. This opportunity is based on the defined threat's capabilities in relation to the other Defence in Depth elements within the system. The findings from this study suggest that a system may still be effective against a large percentage of a population, but not its defined threat, where the system is vulnerable to attack only by these higher level threat agents for which it was intended to defeat (Figure 10.2). This view was explained by Garcia (2001, p. 245) who argued that the adversary factor is strongly interrelated with the effectiveness measure of PPS, where the designer must understand the facilities operations and threat.

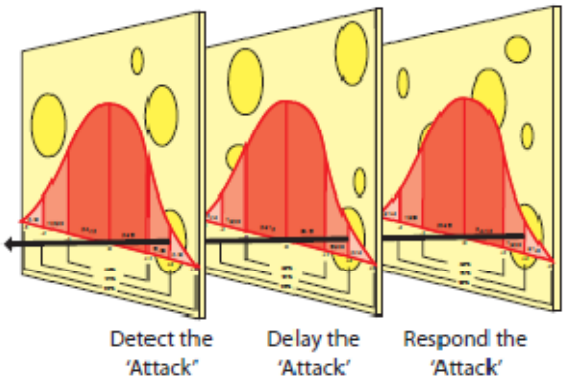


Figure 10.2 The effects of decay based on a normal distribution of attack capabilities.

For example, Figure 10.2 presents the argument that a system's defined threat is based on the combined capabilities of a threat agent/group across all Defence in Depth elements (see Section 3.4.1). It is therefore suggested that such capabilities would be held by a very small percentage of people within the general population. However, for a small targeted percentage of the population the system's vulnerability increases as the holes get bigger in the appropriate elements. Therefore the opportunity for success for this population sample increases. This aspect of system degradation is shown in Figure 4.2 (Section 4.5), where based on the principle equifinality (see Figure 2.5) in open systems the steady state reached is independent of initial conditions and determined by the systems parameters. Consistent with the principle of equifinality the system, based on alterations to these parameters, alters its original steady state, arriving at a new, lesser steady state condition. However, this new condition presents the intuitive perception it is still functioning at its commissioning state (see Section 4.5, Figure 4.2).

10.2 Research findings

McClure (1997, p. 1) wrote, "There is a complex interrelationship between technology, people and management processes within a security function". Consistent with McClure's (1997) viewpoint, the available literature indicates that within a systems approach to security, it is the interrelations which tie the system together towards achieving an output goal, rather than a collection of side-by-side or juxtafication of controls. Coole and Brooks (2009, p. 22) highlighted such a complex relationship within a PPS. They argued that an orderly relationship exists where the space and time distribution of the Defence in Depth elements creates a comprehensive state of order in relation to a Physical Protection System's (PPS) macro level of effectiveness. Consistent with this view the study presented the argument that as a result of managers

not understanding how the physical, technological and procedural aspects combine through management principles and processes within preset parameters to achieve and maintain the systems output goal, they decay. The available literature indicates that in order to maintain PPS at their commissioned levels of effectiveness during their life cycle, they need to be managed in accordance with their commissioned designed specifications. It is argued that the most appropriate means to manage decay within PPS is through the use of a performance indicator frame work, which enables full management of the heterogeneous nature as a "system".

Combining the summative aspect of a Defence in Depth system with the textual benchmark and the interview data, the evidence indicates that the study supported the proposition that security decay can be represented as: The gradual degradation of the microscopic quantities (constituents), or the gradual degradation in the relationship between the microscopic and macroscopic quantities within a security system. It is argued that such a definition provides rigor and genuine conceptual substance that can be integrated into Physical Protection Systems performance measures and appeal to both security academics and practitioners alike. Furthermore, the acceptance of entropic decay theory means that the laws, theories and principles of systems theory associated with maintaining PPS at their commissioned levels of effectiveness can be applied to the security function management processes. In addition, such an approach may also be applied to personnel and information frameworks to cover the entire security management system (see Figure 2.1).

The study defined the effects natural entropy has on a PPS, where such degradation reduces a PPS's effectiveness; however given the ubiquitous usage of entropy, limited understanding and definitional ambiguity, the study argues that consistent with Underwood's (1984) and McClure's (1997) writings, the term *security decay* become adopted to represent the effects and measure of degradation within PPS. Nevertheless, in considering such an outcome, the study argues that in contrast to Underwood's (1984) writings and the findings of McClure (1997) *security decay theory* is primarily concerned with managing the natural entropic processes/pressures occurring against commissioned levels of effectiveness across all elements within PPS. In some cases these processes are allowed to manifest due to a lack of professional management of the security function as a "system".

10.3 Study limitations

This section highlights the methodological limitations within the study. These limitations include a lack of published security benchmarking within the security domain. In addition, this section explains the limitations within the study due the small sample size. Furthermore, the study highlighted a potential cultural aspect to security decay; however, due to limitations in time this aspect was not pursued. Finally, the study's conceptual review of literature considered security decay to be an aspect predominately considered during the monitor and review stage of the risk management cycle, after the system was commissioned. However, the research indicated that decay should be considered well before this stage, at the design stage of a security project.

10.3.1 Benchmarking

Due to a lack in formal Physical Protection Systems (PPS) benchmarking, this research conceptually reviewed the literature (Chapters 2, 3 and 4). Whilst the principles of this benchmark had been peer reviewed prior to this study through the works of Coole and Brooks (2009), the conceptual review as a benchmark had not been double blind peer reviewed. This restricted peer review provides limitations within this study's deductive analysis.

10.3.2 Research Sample

The research panel participants formed a purposive sample (N=9), providing a relatively small research sample. In addition, whilst panel members were selected based on their meeting certain criterion, this sample was chosen based on geographical location and willingness to participate. Some security experts declined to participate, limiting the security domain specializations represented within this study. In addition, another limitation within the sample is the multidimensional nature and many practicing domains of security.

10.3.3 Cultural theory

Research panel two, member one, explained that security decay is like risk, you can accept some decay, mitigate some decay and avoid some decay. Consistent with this approach, according to member three panel two, he has come across some security functions in South East Asia which are so professionally managed that there is absolutely no decay That is, there is no procedural decay and the physical and technological parameters are managed in accordance with the systems designed specifications. This suggests, like risk, security decay has a degree of cultural aspect,

which could be organisational or geographical. This aspect of decay theory was not investigated during this study.

10.3.4 Security decay and risk management

Section 3.6 presents Figure 3.3 the security risk management cycle. At the start of the study, decay was considered to be an aspect which was predominately considered during the monitor and review stage of the risk management cycle, after the system was commissioned. However, the research indicated that decay should be considered well before this stage, at the design stage of a security project. Such an approach considers decay as a risk and treated as such. The aim would be to design and commission a system where decay has been considered and where possible, the system designed to minimize or mitigate decay before the system is commissioned. The study's conceptual review of literature benchmark did not consider this aspect of decay. Therefore this aspect of decay theory was not explored in depth.

10.4 Recommendations

In combining the findings from the study in conjunction with the conceptual review of literature as a benchmark (Chapters 2, 3 and 4), a number of recommendations have been made. These recommendations aim to further develop the knowledge and understanding of entropic security decay so that McClure's (1997, p. 71) recommendation, of pursuing security decay theory beyond an abstract model can be achieved.

10.4.1 Recommendation one: further research into Physical Protection Systems complex interrelations

The study's findings support McClure's (1997) view that there exists a complex interrelationship between technology, people and management processes within a security function. It is recommended that academia pursue further research into this complex interrelationship. The benefits would be the establishment of suitable security benchmarks facilitating more robust security research in the future.

10.4.2 Recommendation two: development of operational performance measures

It is recommended that academia pursue the development of performance measures or key performance indicators at the operational level, which would combine to achieve the tactical level measures presented in the EASI model. These measures would

facilitate the ongoing performance management of the operational deliverables that combine to achieve the tactical measures across the system. Such a management framework would assist security management develop further as a professional management domain.

10.4.3 Recommendation three: the teaching of systems theory for security

It is recommended that academia consider how security studies and security management is taught. This study indicates that a true systems based approach to achieving effective security is required. Therefore, security needs to be managed as a system to ensure that the natural entropic processes/pressures occurring against Physical Protection Systems are avoided or countered through management principles and processes. A significant amount of time is spent within management theory discussing open systems theory. As such, it is recommended that in teaching the management of the security function, that the academic focus towards systems science be adopted into security studies syllabus.

10.4.4 Recommendation four: security decay at the design stage

The research sample, as a consensus, considered that security decay needs to be considered at the design stage of a security project. The security body of literature has focused significantly into designing the environment to reduce crime, referred to as Crime Prevention through Environmental Design (CPTED). This study recommends applying such a philosophy to research how PPS can be designed to reduce/minimize decay over the systems life cycle.

10.4.5 Recommendation five: security decay and cultural theory

It is recommended that cultural theory be employed to investigate the cultural aspects leading to the manifestation of decay, or its avoidance within security systems management.

10.4.6 Recommendation six: the adoption of security decay into the body of knowledge

It is also recommended that the characteristics of security decay i.e. Table 6.1 (Section 6.6) and Table 9.1 (Section 9.6) be further defined, and that security decay theory become adopted into the security domain's body of knowledge. The adoption of security decay theory would enable security managers to draw on this body of knowledge when developing business cases for the ongoing maintenance and review of their respective organisational security functions.

10.4.8 Recommendation seven: the pursuit of a systems approach.

This research indicates that a true systems approach to implementing effective security controls is required to achieve a state of effective security. However, much of the security literature dissects security reviews and security auditing into discrete domain specific categories, including Crime Prevention through Environmental Design (CPTED) reviews, physical security audits, security lighting audits, etc. This study suggests that in order to maintain PPS at their commissioned levels of effectiveness during their life cycle, they need to be managed in accordance with their commissioned designed specifications as a "system". Therefore consistent with recommendation two, it is proposed that security auditing tools and methodologies be developed to audit the security function as a "system" rather than seeing security control components standing in a side-by-side relationship or Silo thinking. This focus was emphasised by Bertalanffy (1968, p. 18) who considered the systems approach to be one of organisation where phenomena are not observable by respective parts in isolation.

It is argued that a systems focus would highlight the quantitative aspect of security which leads to two different security states. These two states include security by denial and security by apprehension. For a denial state the system is commissioned to deny a defined threat access to a protected asset, where through the employment of mathematics the sensitivity settings within a PPS can be adjusted to ensure such an objective is achieved. In contrast, security by apprehension is a state where the system is commissioned to increase the level of difficulty associated with achieving a successful attack. However, the cost benefit analysis does not justify the level of Defence in Depth to resist high level attacks, where the system hinders the attack and facilitates the collection of evidence towards apprehending the offender/s at a later time. Such separation of two different security objectives provides a means of qualitatively articulating the effects of decay on a commissioned PPS, where the system can move from a denial state to one of apprehension.

10.5 Conclusion

This chapter presented the study's research conclusion (Section 10. 1) summarising the available literature relating to the concept of security decay towards presenting this study's research finding (Section 10.2). The study investigated the concept of security decay from a systems approach to implementing effective security controls. This investigation was framed within an open systems approach, drawing on the

underpinnings of General Systems Theory (GST). GST facilitated the examination of how individual security components are tied together to achieve a predetermined output goal. It was argued that this predetermined output goal is the systems purpose, which is achieved through the implementation of various layers of controls. These layers include the use of technological, physical and procedural aspects combined in an orderly relationship, which are interrelated and commissioned as a "whole" against a desired benchmark. This benchmark is designed to counter the threats that pose a risk to various organisations towards achieving the amount of desired risk reduction.

To account for the concept of decay within an open systems frame the study drew on the concept of entropy. Entropy as a concept is derived from a metric, defined as a measure of disorder in a system and a process characterised with: decay, running down, and becoming disordered. For a system it is argued that as its entropy level increases its output or working capabilities decrease. As such, entropy provided the scientific frame for considering security decay within a Physical Protection System (PPS). The study argued that if PPS are left to themselves, that is, not provided with the appropriate feedback open systems require too circumvent the effects of the second law (entropy law) of thermodynamics, they become closed. Closed systems eventually reach a state where they are no longer capable of delivering the required risk control they were commissioned to achieve.

The study recognised and highlighted the complexity of entropic decay theory and the professional management required to ensure that Physical Protection Systems (PPS) maintain their commissioned levels of performance over the course of their life cycle. This complexity is based on the vast number of domain specializations which draw on a variety of science disciplines to achieve the PPS's output goal. The evidence indicates that security decay can be seen as either technological, physical, or procedural in its manifestation. Based on what a system is, such decay can under certain conditions propagate to affect other sub-systems within the system and ultimately the system's macro-state output. The findings of the study suggest that for systems to maintain their commissioned levels of effectiveness over their life cycle they must be professionally managed. It is argued that such professional management requires a specific focus, where the technological aspects of the system are managed in accordance with their designed parameters. In addition, the physical aspects of the PPS needs to managed in accordance with their structural underpinnings, and the human functions and procedural

aspects must be managed by those principles and processes underpinning management theory.

The evidence indicates that these three aspects are the structural categories towards countering entropic decay within PPS. Consistent with this view it is argued that the systems objectives must be clearly defined and underpinned by key performance indicators which directly contribute to the systems output goal. This study purports that such a management philosophy will facilitate an efficacy based approach to the professional management of PPS. That is, facilitating the professional management by objectives.

The study also highlighted the problems associated security's lack in consensus definition. In addition, the dearth of knowledge and lack of dedicated published literature underpinned by academic research pertaining to security decay. In-light of this knowledge gap, this chapter presented a number of study limitations (Section 10.3), highlighting the complexity in conducting robust academic research within the security domain. Furthermore, this chapter presented a number of recommendations (Section 10.4) to both expand the knowledge relating to security decay and expand the robustness of security research for future knowledge categorisation development.

REFERENCE LIST

Abell, P. (1991). *Rational choice theory*: *Schools of thought in sociology*. London: Edward Elgar Publishing.

Adams, D. G., Snell, M. K., Green, M. W., & Pritchard, D. A. (2005). Between detection and neutralization. *Security Technology, 2005, Proceedings, IEEE, annual, 2005 International Carnahan Conference*: IEEE.

Adkins, C. J. (1975). *Equilibrium thermodynamics.* (3rd ed.). London: McGraw-Hill.

Akers, R. L. (1999). *Criminological theories*: *Introduction and Evaluation.* (2nd ed.). United States of America: Roxbury Publishing.

Albrecht, K. (2010). Organisational and intelligence & knowledge management: Thinking outside the silos. *Executive White Paper*. Retrieved May 2010, from http://.KarlAlbrecht.com

Ansell, J., & Wharton, F. (1992). Risk. *Analysis assessment and management*. New York: Chichester Wiley.

Armstrong, D. & Peile, C. (2005). Perimeter intruder detection systems performance standard. Security Technology, 2005, *Proceedings, IEEE, annual, 2005, International Carnahan Conference*: IEEE.

ASCD (2010). *The Normal Distribution*. Retrieved September 2010 from http://www.ascd.org/publications/books/101010/chapters/Applying-the-Research-on-Instruction@-An-Idea-Whose-Time-Has-Come.aspx

Aslaksen, E. W. (2004). System thermodynamics: a model illustrating complexity emerging from simplicity. *Systems Engineering*, 7 (3), 271-284.

Ball, J. (2007). Practical Experiments and simulations for nuclear safeguards education. *A thesis presented to the Faculty of the Graduate School at the University of Missouri-Columbia.* Retrieved, March 2010 from http://edt.missouri.edu/Winter2007/Thesis/BallJ-050307-T6657/

Barton, J. & Haslet, T. (2007). Analysis, Synthesis, Systems Thinking and Scientific Method: Rediscovering the importance of open systems. *Systems Research and Behavioural Science,* 24, 143-155.

Barton, J. & Selsky, J. W. (1998). *An Open-Systems Perspective on Urban Ports: An exploratory comparative analysis.* Monash University Faculty of Business & Economics. Working paper series 78/98.

Bashir, M., Afzal, M., T., Azeem, M. (2008). Reliability and validity of qualitative and operational research paradigm. *Pakistan Journal of Statistics and Operation Research*, 4 (1), 35-45.

Bedard, J. & Chi, M., T.H. (1992). Expertise. *Current Directions in Psychological Science,* 1, 135.

Bertalanffy, L., V. (1950). An outline of General Systems Theory. *The British Society for the Philosophy of Science,* 1 (2), 134-165.

Bertalanffy, L., V. (1950a). The Theory of Open Systems in Physics and Biology. *Science, New Series,* 111, (2872), 23-29.

Bertalanffy, L., V. (1968b). *General systems theory*: foundations, development, application. New York: George Braziller, Inc.

Best, J., W. (1989). *Research in Education.* (6th ed.). New Jersey: Prentice Hall.

Bittel, L., R. (1978). *Encyclopaedia of professional management: an authoritative guide to the profitable practice of management.* New York. McGraw-Hill.

Bitzer, E. G., & Hoffman, A. (N.D.). *Psychology in the study of physical security*. Retrieved February 2010 from http://jps.anl.gov/vol.2/4-Psychology_and_Security.pdf

Borgsdorf, D., & Pliszka, D. (1999). Management your risk or risk your management. *Public Management*, *81*(11), 6-10.

Borodzicz, E., & Gibson, S. D. (2006). Corporate security education: towards meeting the challenge. *Security Journal,* 19, 180-195.

Bussing, A., & Herbig, B. (2003). Tacit knowledge and experience in working. *Psychology Science,* 45, 142.

Broder, J. F. (2006). *Risk analysis and the security survey.* (3rd ed.). Oxford: Butterworth-Heinemann.

Brooks, D. J. (2007). *Defining security through the presentation of security knowledge categories*. Perth, Western Australia. Edith Cowan University, International centre for Security and Risk Sciences.

Brooks, D. J. (2008). The development and presentation of psychometric concept maps within the knolwedge domain of security risk management. Thesis Doctor of Philosophy, Curtin University of Technology, Perth, Western Australia.

Brooks, D. J. (2009). *Key concepts in security risk management.* Saabrucken. VDM Verlag.

Bohm, D., & Peat, D. (2000). *Science, order, and creativity* (2nd ed.). New York: Routledge.

Burns_Howell, T., Corider, P., & Erikson, T. (2003). *Security Risk Assessment and Control*. Leicestser: Perpetuity Press.

Byeon, J. H. (1999). Non-equilibrium thermodynamics approach to the change in political systems. *Systems Research and Behavioural Science*. 16, 283-291.

Byeon, J. H. (2005). A systems approach to entropy change in political systems. *Systems Research and Behavioural Science. 22, 223-231.*

Callister, W. D. (1997). *Materials science and engineering: An introduction.* (4th ed.). New York: John Wiley & Sons.

Carmichael, S. E., & Piquero, A. R. (2006). Deterrence and arrest ratios. *International Journal of Offender Therapy and Comparative Criminology*, 50, 71-87.

Charmaz, K. (2006). *Constructing grounded theory*: *A practical guide through qualitative analysis*. London: SAGE Publications.

Checkland, P. (1981). Systems thinking, systems practice. Salisbury: John Wiley & Sons.

Churchman, C., W. (1968). *The systems approach*. New York: Dell Publishing Co., Inc.

Cioffi-Revilla, C. (1999). Origins and age of deterrence: Comparative research on old world and new world systems. *Cross-Cultural Research*, 33, 239-264.

Clarke, R. V., & Cornish, D. B. (1987). Understanding crime displacement: An application of rational choice theory. *Criminology*, *50*(4), 933-947.

Cohen, L. & Felson, M. (1979). Social change and crime rate trends: a Routine Activity Approach. *American Sociological Review*, 144: 588-608.

Cohen, L., Manion, L., & Morrison, K. (2005). *Research methods in education.* (5th ed.). London: Routledge Falmer.

Collins Australian Pocket Dictionary of English Language (1994). Victoria: Harper Collins Publishers.

Coole, M., & Brooks, D. (2009). The theory of entropic security decay. *Proceedings from the Second Australian Security and Intelligence conference*. Perth, Western

Australia. Retrieved June 2010 from http://igneous.scis.ecu.edu.au/proceedings/2009/secintel/ASICProceedings.pdf

Cornford, I., & Athanasou, J. (1995). Developing expertise through training. *Industrial Commercial Training,* 27 (2), 10-19.

Corning, P., A. (1995). Synergy and self-organization in the evolution of complex systems. *Systems Research*. 12, (2), 89-121.

Coulter, D. T. (2008). *Defence in Depth*. Retrieved April 2009 from http://leetroxell.com/phrobus/DEFENSEINDEPTH.pdf

Craighead, G. (2003). *High-Rise Security and fire life safety* (2nd Ed.). Woburn, MA: Butterworth-Heinemann.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice,* 39 (3), 124-30.

Cumming, N. (1992). *Security*: *a guide to security system design and equipment selection and installation* (2nd ed.). Boston: Butterworth-Heinemann.

Dalkey, N. & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science,* 9 (3), 458.

Delbecq, A. L., van de Ven, A. H., & Gustafson, D. H. (1975). *Group techniques for program planning*: *a guide to nominal group and Delphi processes*. Glenview: Scott Foreman and Company.

Davies, D., & Dodd, J. (2002). Qualitative research and the question of rigour. *Qualitative Health Research*. Vol 12 (2). Pg 279-289.

Denbigh, K. G. (2009). *Note on entropy, disorder and disorganization*. Retrieved April 2009 from http://www.endeav.org/evolut/text/denbig1/denbig1e.htm

Dillon, J. A. (1983). Foundations of general systems theory. California: Intersystem's Publications.

Effective Management (N.D.). Delphi study. Victoria.: Department of sustainability and Environment. Retrieved February 2010 from http://www.dse.vic.gov.au/DSE/wcmn203.nsf/LinkView/D7B9E063A2B4FFAFCA25707E00248822EBB2EB2F9035229BCA257091000BF7A6

Eggers, R. M., & Jones, C. M. (1998). Practical considerations for conducting Delphi studies: the oracle enters a new age. *Educational Research,* 21 (3), 53.

Erricsson, K. A., Charness, N., Feltovich, P. J., & Hoffman, R. R. (2006). *The Cambridge handbook of expertise and expert performance.* New York: Cambridge University Press.

Felder, G. (2001). *Things fall apart: An introduction to entropy*. Retrieved April 2009 from http://www4.ncsu.edu/unity/lockers/users/f/felder/public/kenny/papers/entropy.html

Fennelly, I. J. (1997). *Effective physical security* (2nd ed.). Boston: Elsevier Butterworth-Heinemann.

Fink, D. G, & Beaty, W. (1978). Standard handbook for electrical engineers (11th ed.). New York: McGraw-Hill Book Company.

Fisher, R. J., & Green, G. (2004). *Introduction to Security* (7th ed.). Boston: Butterworth- Heinemann.

Forshaw, M. (2004). *Your undergraduate psychology project*: *A BPS Guide*. United Kingdom: Blackwell.

Francis, S. (1992). A gallery of security. *Security Management*, *36*(9), 126-131.

Garcia, M. L. (2001). *The design and evaluation of physical protection systems*. Boston: Butterworth-Heinemann.

Garcia, M. L. (2006). *Vulnerability assessment of physical protection systems*. Boston: Butterworth-Heinemann.

Gillham, B. (2000). *Developing a questionnaire*. London: Continuum.

Golfashani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report,* 8 (4), 597-607.

Hamlyn, D. W. (1969). *The psychology of perception: A philosophical examination of Gestalt Theory and derivative theories of perception*. New York: Routledge & Kegan Paul Ltd.

Hatfield, A. J., & Hipel, K. W. (2002). Risk and systems theory. *Risk Analysis*, *22*(6), 1043-1057.

Herman, M. (1999). *Entropy based warfare: Modelling the revolution in military affairs.* Retrieved April 2009 from http://209.85.173.132/search?q=cache:7Rigu4CTvaAJ:www.au.af.mil/au/awc/a

wcgate/jfq/1620.pdf+herman+entropy+based+warfare&cd=1&hl=en&ct=clnk&gl=au

Hilborn, R. C. (2003). Sea gulls, butterflies, and grasshoppers: A brief history of the butterfly effect in nonlinear dynamics. *American Journal of Physics,* 72 (4), 425-427.

Honkasalo, A. (1998). Entropy, energy and steady-state economy. *Sustainable Development.* 6, 130-142.

Howell, D., C. (2008). *Fundamental Statistics for the Behavioural Sciences* (6th ed.). California: Thompson Higher Education.

Howlet, J., F. (1995). Maintenance: The pacifier's influence. *Security technology, Proceedings IEEE annual 1997 International Carnahan Conference*. IEEE.

Jang, S. S., Kwak, S., Yoo, h., Kim, J., & Ki Yoon, W. (2008). Development of a vulnerability assessment code for a physical protection system: Systematic analysis of physical protection effectiveness (SAPE) *Nuclear Engineering and Technology*. 41 (5), 747-752.

Keren, M. (1979). Ideological implications of the use of open systems theory in political science. *Behavioural science,* 24, 311-324.

King, S. (2008). Computer weekly. Retrieved April 2009 from http://www.computerweekly.com/blogs/stuart_king/2008/09/security-entropy.html

Kline, P. (2000). *Handbook of psychological testing* (2nd ed.). London: Routeledge.

Koffka, K. (1963). *Principles of Gestalt psychology*. New York: Harcourt, Brace & World, Inc.

Kohler, W. (1975). *Gestalt psychology: An introduction to new concepts in modern psychology*. New York: LiverRight Publishing.

Konicek, J., & Little, K. (1997). *Security, ID systems and locks: The book on electronic access control*. New York: Butterworth-Heinemann.

Landsberg, P. T. (1956). Foundations of thermodynamics. *Reviews of modern physics*, 28 (4), 363-392.

Liamputtong, P. & Ezzy, D. (2006). *Qualitative research methods* (2nd ed.). Hong Kong: Oxford University Press.

Lin, N. (1976). *Foundations of social research*. New York: McGraw-Hill.

Loewenthal, K. (2001). *An introduction to psychological tests and scales* (2nd ed.). Psychology Press.

Lorenz, E, N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences,* 20, 130-141.

Lorenz, E, N. (1969). The predictability of a flow which possesses many scales of motion. *Tellus,* 20, 289-307.

Lovey, I., & Nadkarni, M., S. (2007). *How healthy is your organisation*. Westport, Connecticut: Praeger Publishing.

Manunta, G. (1999). What is security? *Security Journal*.12, 57-66.

Manunta, G. (2007). The management of security: How robust is the justification process? *Security Journal*. *20*, 41-43.

Martin, D., W. (2000). *Doing psychology experiments* (5th ed.). California: Wadsworth.

Maslow, A., H. (1970). *Motivation and personality* (2nd ed.). New York: Harper & Row.

Maxwell, J. A. (1992). Understanding and validity in qualitative research. *Harvard Educational Review*, 62 (3), 279-300.

McClure, S. A. (1997). *Security decay: The erosion of effective security*. Thesis (BSc (Hons), Edith Cowan University, Perth, Western Australian.

McCrie, R., D. (2004). The history of expertise in security management practice and litigation. *Security Journal*. Vol 17 (3), 11-19.

Meara, A. (2005). Facilitating change in open systems. *Gestalt Journal of Australia and New Zealand*. Vol 2 (1), 7-30.

United States Army (1993). Military Handbook Design Guidelines For physical Security of Facilities: MIL-HDBK, 1013/1. Retrieved January 2010 from http://www.wbdg.org/ccb/NAVFAC/DMMHNAV/1013_1a.pdf

Midgley, G. (2003). *Systems thinking: general systems theory, cybernetics and complexity.* London: SAGE Publications.

Morales-Matamoros, O., Tejeida-Padilla, R., & Badillo-Pina, I (2010). Fractal Behaviour of Complex Systems. *Systems Research and Behavioural Science,* 27, 71-86.

Moseley, K., Coleman, A., & Sinclair, W. G. (2000). *Barriers.* United Kingdom: Police Scientific Development Branch, Home Office.

Motz, L., & Weaver, J. H. (1989). *The story of physics*. New York: Plenum Press.

O'Block, R. L., Donnermeyer, J. F., & Doeren, S. E. (1991). *Security and crime prevention* (2nd ed.). Boston: Butterworth-Heinemann.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management,* 42, 15-29.

Olzac, T. (2006). Just enough security. *Security*, 43, (9), 114.

Oster, G. F. & Desoer, C. A. (1971). Tellegen's theorem and thermodynamic inequalities. *Theoretical Biology,* 32, 219-241.

Patton, M., Q. (2002). *Qualitative research and evaluation methods* (3rd ed.). California: Sage Publications.

Phinney, C., & Smith, C. (2009). Security education in Singapore: A study of knowledge structures in electronic security technology. *Security Journal,* 1-16.

Peirce, J. C. (2000). The paradox of physicians and administrators in health care organizations. *Health Care Management Review,* 25 (1), 7-28.

Pidwirny, M. (2006). "*Equilibrium Concepts and Feedbacks*". *Fundamentals of Physical Geography,* (2nd ed.). Retrieved February 2010, from http://www.physicalgeography.net/fundamentals/4f.html

Pitzer, K., S. (1995). *Thermodynamics*. New York: McGraw-Hill.

Post, R. S., Kingsbury, A. A., & Schachtsick, D. A. (1991). *Security administration: An introduction to the protective services* (4th ed.). Boston: Butterworth-Heinemann.

Price, H. (2003). The thermodynamic arrow: puzzles and pseudo-puzzles. *World Scientific*, 1-16.

Prigogine (1987). Exploring complexity. *European Journal of Operational Research,* 30, 97-103.

Pyett, P. M. (2003). Validation of qualitative research in the "real world". *Qualitative Health Research*, 13 (8), 1170-1179.

Rifkin, J., & Howard, T. (1982). *Entropy*: *a new world view*. New York: The Viking Press.

Ritchey, T. (1991). *On scientific Method- based on a study by Bernard Riemann*. Retrieved Jan 2010 from www.swemorph.com

Robinson, R. R. (1999). *Issues in security management: thinking critically about security.* Boston: Butterworth-Heinemann.

Roos, I. (1997). *The Debt of Systems Theory to Thermodynamics*. Working paper series 34/97. Monash University, Melbourne, Australia.

Ribbens, W. B., & Cole, D. E. (1989). *Automotive electronics Delphi. Office of the Study of Automotive Transportation*. The University of Michigan. Retrieved February 2010 from http://deepblue.lib.umich.edu/handle/2027.42/835

Rundblad, G. (2006). Recruiting a representative sample. Retrieved May 2010 from www.appliedlinguistics.org.uk

Runyon, R. P., Coleman, K. A., & Pittenger, D., J. (2000). *Fundamentals of behavioural statistics* (9th ed.). Boston: McGraw Hill.

Scaefer, K. E., Hensel, H., & Brady, R. (1977). *A new image of man in medicine: Toward a man-cantered medical science*. Vol 1. New York: Futura Publishing.

Schmidt, R., C. (1997). Managing Delphi surveys using nonparametric statistical techniques. *Decision Sciences,* 28 (3), 763.

Searle, A. (1999). *Introducing research and data in psychology*: *A guide to methods analysis*. London: Routledge.

Selksy, J. W., & Barton, J. (2000). Sources and Legacies of Emery's Open Systems Theory: An introduction to the special issue. *Systemic Practice and Action Research,* 13 (5), 615-622.

Sheard, S. A., Mostashari, A. (2008). Principles of complex systems for systems engineering. *Systems Engineering*. 12 (4), 295-311.

Silverman, D. (2001). *Interpreting qualitative data*: methods for analysing talk, text and interaction. London: Sage Publications.

Silverman, D. (2002). *Doing qualitative research: A practical handbook*. London: Sage Publications.

Silverman, D. (2002a). *Interpreting qualitative data: methods for analysing talk, text and interaction* (2nd ed.). London: Sage publications.

Singh, A. M. (2005). Private security and crime control. *Theoretical Criminology*, *9*, 153-174.

Skyttner, L. (1996). *General systems theory; an introduction*. London: Macmillan Press LTD.

Smallman, C. (2004). A grounded theory of hazard priorities in British organisations. *Risk decision and Policy*, *9*, 55-74.

Smith, C. L. (2003). *Understanding concepts in the defence in depth strategy*, School of Engineering and Mathematics. Edith Cowan University. Australia.

Smith, S. (1992). Global dumbing: the politics of entropy. *Progressive Review*. Retrieved April 2009 from http://prorev.com/dumbing.htm

Somerson, I., S. (2009). *The art and science of risk security risk assessment.* ASIS International. United States of America.

Spencer, D. D. (1998). Vulnerabilty assessment: correctional facilities are only secure as their weakest point. *Corrections Today,* 60 (4), 88.

Sproull, N., L. (1995). *Handbook of research methods: A guide for practitioners and students in the social sciences* (2nd ed.). Metuchen: The Scarecrow press, Inc.

Stake, R. E. (2010). *Qualitative research: studying how things work*. New York: Guildford Press.

Standards Australia. (2004). *AS/NZS4360:2004 Risk management.* Sydney: Standards Australia International Ltd.

Standards Australia. (2006). *Security risk management.* Sydney: Standards Australia International Ltd.

Strauss, A., & Corbin, J. (1990). *Basics of qualitative research: Grounded theory procedures and techniques.* London: Sage Publications.

Styer, D. F. (2000). Insight into entropy. *American Journal of Physics*, *68*(12), 1090-1096.

Tarr, C., J. (1994). Cost effective perimeter security. *Security Technology, 1994, Proceedings, IEEE, annual, 1994 International Carnahan Conference*: IEEE.

Tassios, D. (1999). Management of Resources for Sustainable Development: Entropy "shows" the way. *Proceedings of the sixth International conference on Environmental Science and Technology*. Greece: Pythagorion, Samos,

The New Oxford School Dictionary (1991). Victoria: Harper Collins Publishers.

Tejeida-Padilla, R., Badillo-Pina, I., & Morales-Matamoros, O. (2010). A Systems Science Approach to Enterprise Resources Planning Systems. *Systems Research and Behavioural Science,* 28, 87-95.

Tester, J. W. & Modell, M. (1996). *Thermodynamics and its applications* (3rd ed.). New Jersey: Prentice Hall.

The Open University (1976). *Towards a mechanistic philosophy*. Worchester:

Open University Press.

Thompson, T. (2002). *Definitions of entropy*. Retrieved April 2009 from http://www.tim-thompson.com/entropy1.html

Trusted Information Sharing Network for Critical infrastructure Protection, (2008). *Defence in depth*. Retrieved April 2009 from http://www.dbcde.gov.au/__data/assets/pdf_file/0006/88359/Defence-in-Depth-CIO-15_Oct-2008.pdf

Underwood, G. (1984). *The security of buildings*. London: Butterworths.

Vannini, A. (2005). Entropy and Syntropy: from mechanical to life science. *NeuroQuantology* (2), 88-110.

Voorthuijsen, G., Van Hoof, H., Klima, M., Roubik, K., Bernas, M., & Pata, P. (2005). CCTV effectiveness study. *Security Technology, 2005, Proceedings, IEEE annual 2005 International Carnahan Conference*: IEEE.

Waldman, J. D. (2007). Thinking systems need systems thinking. *Systems Research and Behavioural Science,* 24, 271-284.

Walker, P. (1988). *Electronic security systems*: *better ways to crime prevention* (2nd ed.). London: Butterworths.

Walliman, N. (2004). *Your Research Project* (2nd ed.). London: Sage publications.

Walliman, N. (2005). *Your undergraduate dissertation: The essential guide for success*. London: SAGE Publications.

Warren, K., Franklin, C., & Streeter, C. L. (1998). New directions in systems theory: Chaos and complexity. *Social Work,* 43 (4), 357.

Weiten, W. (2002). *Psychology: themes and variations* (5th ed.). California: Wadsworth, Thompson Learning.

Winoto, P. (2003). Controlling malevolent behaviour in open multi-agent systems by means of deterrence theory. *Proceedings of the IEEE/WIC international Conference on intelligent agent technology* (IAT'03).

APPENDIX A

SEMI-STRUCTURED INTERVIEW RESEARCH QUESTIONNAIRE LETTER

The Theory of Entropic Security Decay

Thank you for considering participating in our research study pertaining to the concept of security decay. This research project is being undertaken as part of the requirements of a Master of Science degree at Edith Cowan University. Your insights will be extremely helpful in evaluating the existence of this phenomenon within the security domain.

Aim: To develop the concept, define the term and establish a framework for measuring entropic decay within a security system.

Benefits: This research will develop an understanding of how the characteristics that may make an organisation prone to entropic decay can be identified, and measured. Once these characteristics are understood, this will enable the use of small funding to stimulate and maintain the effectiveness of various security risk mitigation strategies. This information can assist managers when conducting formal risk assessments to ensure their risk reduction strategies take into account the decaying aspect of implemented security controls.

The theory of entropic security decay

The theory of defence in depth aims to link layered security elements into a system incorporating; people, technology, barriers and procedures to ensure a holistic and functional security system. This system aims to deliver effective risk based decisions, enhanced operational effectiveness, and reductions in overall risks and costs for a facility. However, it has been argued that security controls degrade over time reducing the effectiveness level of risk treatment. This argument was first considered by Underwood (1984) who referred to this as decaying security, stating "***Security decay***" is the most serious threat to a security system, and that such decay must be "expected", "avoided", and "countered".

The theory of entropic decay considers that security controls are implemented within a systems approach towards reducing security related risks, and that in line with the premises of systems theory the elements of defence in depth (detect, delay and response) must be employed and successfully achieved within their sequential order and that over time all systems are prone to entropic decay, including security systems.

This study requires your assistance to explore the application of security controls within a systems frame. Specifically, we seek your experience with the argument that in line with the principles of systems theory, all systems includes security systems degrade over time, leading to decay, and that this decay does/is manifested within the system.

Results from this study will be integrated into the conceptual literature review framing the theory of entropic security decay for interpretation and analysis towards drawing conclusions relating to the research questions. In addition, each participant within the study will receive a critique of the findings as they occur. This will provide you with the most up-to-date discourse relating to the concept of security decay.

Guidelines: This research enquiry is employing a Delphic poll methodology. The purpose of a Delphic Poll is to gather a consensus of expert opinions relating to a specific topic under investigation using several rounds of interviews or questionnaires to facilitate the identification, evaluation, and clarification of research problems and establish positions towards identifying solutions, by drawing on the current knowledge of participating experts. You have been nominated by your peers as a security expert.
This Delphic study will be undertaken utilizing Interviews as they are a systematic means of discussing with people an area under investigation towards collecting data and constructing knowledge in research. The use of interviews in research considers that knowledge is something generated between people, often through conversation. Interviews enable research participants in a study to discuss their interpretations of the world in which they live, and to express how they regard issues under investigation from their personal experience. As sch the core aspect of your role within this study will consist of providing experience-based knowledge when answering interview questions.

Risks and Discomforts
There are no foreseeable risks or discomforts associated with your participation in this study. However, you will be required to participate in two rounds of interviews, with an information feedback process between these rounds.

Confidentiality
Information obtained from this study which could identify you will be kept private to the extent allowed by law. However, information which may identify you will be shared with research supervisory staff from Edith Cowan University where necessary.

Results
The results of this study will be published as a thesis and made available through various library catalogues. In addition, it is anticipated that the results of this study will be reported in conference proceedings and relevant journal publications. The reporting of results will not include any information that may identify individual participants. This study incorporates a Delphic Poll, as such results will be disseminated to participants during the course of the research phases, and final results will be reported to all participants once conclusions have been drawn at the completion of the research phase.

Refusal or withdrawal without penalty
Your taking part in this study is your choice. There is no penalty if you decide not to be in the study. In addition, you are free to withdraw from this research study at any time. In addition, you may be removed from this study without your consent if Edith Cowan University chooses to end the study.
If you have any questions, concerns, or complaints about this research or a research-related enquiry, please contact this research's supervisor Dr Dave Brooks;
d.brooks@ecu.edu.au or telephone: 08 63045788, or
Student Researcher; Michael Coole: 0415874595 or email, mcoole@our.ecu.edu.au

INFORMED CONSENT

Thank you for choosing to participate in this research study. Your signature below indicates that you agree to participate in this study. If you agree to participate in this study you will receive a copy of this signed document.

I_____ agree to participate in this research study (the theory of entropic security decay). I have had the aims of the study explained to me, its research methodology and my commitment requirements. In-line with the requirements of informed consent, I provide my informed consent.

Signature_____ Date____/____/____.

This document was Witnessed by Michael Coole_____Date___/___/____.

APPENDIX B

PILOT STUDY SEMI-STRUCTURED INTERVIEW QUESTIONNAIRE

Category	Questions	Responses Date: ___/___/___ Panel No._____ Round No._____
Systems approach to security. **Prompts and Probes**: **a)** Would you elaborate on that? **b)** How did that come about? **c)** That's helpful I'd appreciate it if you could give more detail. **d)** Some say,..do you agree? **e)** What you're saying now is very important, and I want to make sure that I get it down exactly the way you mean it, please explain some more.	**a)** Can you please tell me from your experience what the role of security is within an organisations • Do you see it as a risk reduction role? **b)** Can you tell me how you apply the body of knowledge including theories and principles of security, specifically DiD • Do you support a systems approach? Can you please explain to me your understanding of a system • Do you consider the relationships between the micro state and the macro state? • What do you think this involves? **c)** According to the principles of systems theory small changes within a specific part can lead to a large change at the output of the systems • Do you agree with this premise? **d)** Systems theory is concerned with those key performance indicators that are directly related to the whole systems key performance indicator. • Within your understanding of a systems approach, can you tell me what you believe the key performance indicators are within a PPS • Based on your experience, do you believe the key performance indicators of the systems are related to the systems effectiveness?	

Security Decay This study is specifically focused towards establishing an understanding of the concept of security decay. **Prompts and Probes**: **a)** Would you elaborate on that? **b)** How did that come about? **c)** That's helpful I'd appreciate it if you could give more detail. **d)** Some say,..do you agree? **e)** What you're saying now is very important, and I want to make sure that I get it down exactly the way you mean it, please explain some more.	**a)** Based on your experience do you believe that security systems decay; **b)** What is your understanding of security decay; **c)** Can you tell me about a time when you experienced security controls degrading; **d)** In considering the argument that security controls decay, how do you think this occurs within a systems approach to security; **e)** The theory of entropic security decay argues that the concept of decay within a PPS occurs within the individual constituents, within the PPS, and its effects propagate through the system from this point. Based on your experience, do you support this premise; **a)** Systems theory, and specifically an effect referred to as the butterfly effect suggests small input changes within a system can result in large changes at the macro output. Do you feel this applies to a PPS; Can you give me an example where you have come across this; **b)** Based on your experience, what do you consider the effects of decay are; **c)** Once decay has set in, do you think its effects, both at the point of manifestation, and throughout the remainder of the system are reversible; **d)** Do you think decay can be avoided; **f)** Do you believe the concept of decay has a place in the risk management formula?	

Biographical data	
Participant No. Panel No.	
What is your current security employment context and role?	
Can you please tell me what type of security advice you supply in this role?	
How long have you been in this role?	
Can you please tell me what formal qualifications you hold for this role?	

APPENDIX C

FINAL SEMI-STRUCTURED INTERVIEW QUESTIONNAIRE

Category	Questions	Responses Date: ___/___/___ Panel No._____ Round No._____
Systems approach to security. **Prompts and Probes**: **f)** Would you elaborate on that? **g)** How did that come about? **h)** That's helpful I'd appreciate it if you could give more detail. **i)** Some say, do you agree? **j)** What you're saying now is very important, and I want to make sure that I get it down exactly the way you mean it, please explain some more.	**1)** Can you please tell me from your experience what the role of security is within an organisation? **2)** Do you see it as a risk reduction role? **3)** Can you tell me how you apply the body of knowledge including security methodologies and concepts? Do you use DID? (If not stated). **4)** Can you please explain to me your understanding of a system? Do you consider the relationships between the components and the goal of the system? **5)** Do you support a systems approach towards security? Yes/No. **6)** What do you think the systems approach towards security involves? According to the principles of systems theory small changes within a specific component can lead to a large change at the output of the systems **7)** Do you agree with this premise? Yes/No Can you explain why? Systems theory is concerned with those key performance indicators that are directly related to the whole systems key performance indicator. **8)**Within your understanding of a systems approach, can you tell me what you believe the key performance indicators are within a PPS **9)** Based on your experience, do you believe the key performance indicators of the systems are related to the systems effectiveness? Can you explain how?	
Security Decay This study is specifically focused towards establishing an understanding of the concept of security decay.	**10)** Based on your experience do you believe that security systems decay; **11**) What is your understanding of security decay; **12)** Can you tell me about a time when you experienced security controls degrading, what occurred?	

Prompts and Probes: **f)** Would you elaborate on that? **g)** How did that come about? **h)** That's helpful I'd appreciate it if you could give more detail. **i)** Some say, do you agree? **j)** What you're saying now is very important, and I want to make sure that I get it down exactly the way you mean it, please explain some more.	**13)** In considering the argument that security controls decay, how do you think this occurs within a systems approach to security; The concept of security decay argues that decay within a PPS occurs within the individual constituents, within the PPS, and its effects propagate through the system from this point. **14)** Based on your experience, do you support this premise Yes/No, why, why not? Systems theory, and specifically an effect referred to as the butterfly effect suggests small input changes within a system can result in large changes at its macro output. **15)** Do you feel this applies to a PPS? Yes/No. Can you give me an example where you have come across this? **16)** Based on your experience, what do you consider the effects of decay are? **17)** Once decay has set in, do you think its effects, both at the point of manifestation and throughout the remainder of the system are reversible? Yes/No. How do you think so? Or, why don't you think so? **18)** Do you think decay can be avoided? Yes/No. How do you think the effects of decay within a security system can be avoided? Or, why don't you think the effects of decay within a security system can be avoided? **19)** Do you believe the concept of decay has a place in the risk management process? Yes/No. If so, where in the process? If not, why not? **20)** Based on your experience, is there any facet of security decay which you can add to the research enquiry? This may include factors associated with either the cause of decay or impacts from it.	

APPENDIX D
RESEARCH PANEL ONE: PHASE THREE EXPERT INTERVIEW AND FEEDBACK TRANSCRIPT

The following transcript was taken from panel one member two's feedback (Round two participant interview) transcript from questions 1-10 to demonstrate a typical interview .

Interview transcript

Question 1: Can you please tell me from your experience what the role of security is within an organisation?

You answered: Security's role is the protection of assets, including: physical information and personnel in order for the organization to function to achieve its business objectives. Security should be integrated with the organization to assist it in achieving its objectives.

Participant 1; Re: Security depends on context and relates primarily to the safety of people, not Occupational Safety and Health, but the safety of people from human adversaries. It also encompasses asset protection, secure containment and incident management.

Participant 3; Re: For me, in principle, the role is around maintaining custody and containment of all prisoners within the justice system. This is achieved through the provision of physical, procedural, dynamic security measures in a balanced and holistic approach.

Feedback: Both yourself and panel member number one (1) stated that security's role is the protection of assets. However, panel member number three (3) stated that security's role encompasses and is achieved through the provision of physical, procedural, dynamic (intelligence) measures in a balanced and holistic approach.

Qu: Do you agree with panel member number three's (3) statement?

Res: These are functions towards achieving the objective, that is, this is how a state of security is achieved.

Furthermore, the pilot study panel concluded that security at the tactical level of management relates to the holistic implementation of procedural, physical and electronic measures which aims to protect an organisation's assets which includes people, information and physical property through their ability to deter, detect, delay and respond against organisation specific threats.

Qu: Do you agree with the pilot panel's conclusions?

Res: Yes.

Question 2: Do you see security roles as a reduction role?

You answered: Yes, because its role is to mitigate known or perceived threats to an organization.

Participant 1; Re: Yes, everything is risk based. Without knowledge of risk there is no baseline.

Participant 3; Re: Most definitely, it is about reducing risk all the time, not just within the justice system, but across the wider community.

Feedback: All panel members responded yes to this question, that security is a risk reduction role. As such, it is interpreted that a consensus exists amongst the panel members that security is a risk reduction role.

Qu: Do you support this interpretation?

Res: Yes I do.

In addition, the pilot panel reported that security is a risk reduction role at the strategic level of management.

Qu: Do you agree with the pilot panel?

Res: Yes, of course.

Furthermore, the pilot panel as a consensus agreed that security also has a deterrent role within an organisation towards preventing security related incidents.

Qu: Do you support the pilot panel's views in relation to this aspect of security's role within an organisation?

Res: Yes, it is one of its functions.

Question 3: Can you tell me how you apply the body of knowledge including security methodologies and concepts. Do you use defence in depth?

You answered: I combine all aspects of defence in depth, Crime Prevention Through Environmental Design (CPTED) and risk management to achieve security objectives. These are, and need to be interrelated. To achieve defence in depth, in-line with a security context requires all aspects of security. For example, security intelligence (SYNT) aligns with risk management to ascertain how defence in depth will be achieved. For example, CPTED detection or a technology based detection component. This takes into account zoning at a facility, where different levels of risk reduction are required within each zone (Hierarchical system) of defence in depth, where defence in depth achieves a level of access control.

Participant 1; Re: It depends on the security context. Defence in depth is an absolute underpinned by security risk management. That is, you need to understand the client's needs and their risks. It needs to be very functional.

Participant 3; Re: I definitely adopt the principles of defence in depth, also crime prevention through environmental control (CPTED) within physical security. I utilize CCTV as alarm verification/discrimination. For me It incorporates a balanced approach of physical, procedural, dynamic (Intelligence) and risk management.

Feedback: For this question, all panel members responded that they employ defence in depth interrelated with risk management to establish a level of security based on risk. As such, it is interpreted that al panel members agree that the consistent body of knowledge employed to security an organisation's assets is defence in depth and risk management.

Qu: Do you agree with this interpretation?

Res: Yes.

In addition, panel member number two (2) stated that he employs a hierarchical system of defence in depth, where defence in depth achieves a level of access control, within zones to achieve a desired level of risk reduction.

Qu; Do you support panel member number two's (2) approach?

Res: Yes.

In addition, panel member number one (1) stated that when employing the security body of knowledge it needs to be very functional. That is, applied from a functional approach.

Qu: Do you agree with panel member number one's (1) views relating to the employment of security's body of knowledge?

Res: Yes.

Question 4: Can you please explain your understanding of a system? Do you consider the relationship between the components and the goal of the system?

You answered: For a system, you tie in a group of elements and constituents which maintain a role towards an overall outcome. All aspects are interrelated, it depends on how they are interrelated, and yes I certainly consider the interrelationships.

Participant 1; Re: The systems approach is a holistic approach, "seen as a whole". It requires structure with good interactions between components (highly interrelated) interface between components. "It's a top down process". A systems approach considers strong interrelationships between interrelationships at the design stage with operator interface. That is, the components must help achieve the objective of the system.

Participant 3; Re: For me systems are the components and linking's between them, the physical components and procedures are linked to achieve a goal, which for me the goal is to reduce risk.

Feedback: For this question both yourself and panel member number one (1) focused on linking in individual components and their various interrelationships to achieve an overall goal or objective. Specifically, panel member number one (1) stated that a system a system is a top down process which requires structure incorporating components with good interactions between them, and all being highly interrelated to achieve the objectives of the system. However, the system should be seen as a "whole".

Qu: Do you agree with panel member number one's (1) views?

Res: Yes.

Furthermore, panel member number three (3) stated the systems approach links in the physical components and human procedures to achieve the systems goal, which in the security context is the reduction of risk.

Qu: Do you agree with panel member number three's (3) views?

Res: I do in a security context, but a systems goal may not be to reduce risk. As such, I think this is an oversimplification.

In addition, the pilot panel reported through consensus that the systems approach to security relates to how risks can be reduced through a holistic approach, interrelating the separate components which combine together to achieve an overall goal.

Qu: Do you support the pilot panel's consensus?

Res: Yes.

Question 5: Do you support a systems approach towards security?
You answered: Yes for sure.

Participant 1; Re: Yes, as long as the systems are properly designed tools for the management of security risks (systems are sets of tools).

Participant 3; Re: Yes, definitely.

Feedback: For this question all panel members responded yes, that they support a systems approach towards security. It is therefore interpreted that a consensus was reached with this question. Such a consensus was also reached by the pilot panel.

Qu: Do you agree with this interpretation?

Res: Yes.

Question 6: Too the question**:** What do you think the systems approach towards security involves?

You answered: The same as it does with any organization. The Physical Protection System (PPS) broken down into its component parts relies on the other components within the system. If one component within the system is broken, or removed, this

changes the whole system. For example, defence in depth relies on all its elements to be interrelated and at their measure of effectiveness.

Participant 1; Re: The systems approach to security is a holistic approach that recognizes the main contributions to the security solution. Be it, management processes, procedures, technology, people and physical security, the built environment and planning. It is how each of these elements are implemented, recognizing the importance of each other and how the interactions compliment and influence each other. Each element is configured or implemented to support each other to form a holistic security system approach, and recognizes the Swiss Cheese choice approach.

Participant 3; Re: The systems approach means to have sound security practices in place before an event occurs. This applies the dynamic approach (Intelligence) to security. The systems approach adopts the principles of security, and has them in place before an event, to reduce the risks associated with a security context. The systems approach starts before a security project commences. The majority of risks should be mitigated before, at the planning stage.

Feedback: To this question panel member number one (1) focused on the idea that the systems approach is a holistic approach that recognises the main contributions to the security solution, be they management processes, procedures, technology, physical barriers, built environment and people, and how each of these components are implemented to compliment and support each other.

Panel member number one specifically draws on the Swiss cheese analogy presented in Standards Australia (HB 167: 2006, p. 59), where many security controls will exist in a "layered" or defence in depth structure, where under normal circumstances the holes in each layer are covered up by subsequent layers of controls.

Qu: Do you agree with panel member number one's (1) views?

Res: Yes.

In addition, panel member number three (3) stated that he views the systems approach as being sound security practices in place before an event occurs, that is, adopting the principles of security to reduce risks associated with a security context at the start of a security project.

Qu: Do you agree with panel member number three's (3) views?

Res: I don't agree as I don't think he really has answered the question. Looking at it from management theory, the systems approach is about putting in place a combination of strategies to achieve a set goal. That is, systems theory should be applied to the security function.

Furthermore, the pilot panel reported through consensus that the systems approach to security relates to how risks can be reduced through a holistic approach, interrelating the separate components which combine together to achieve an overall goal.

Qu: Do you agree with the pilot panel's consensus relating to the systems approach?

Res: Yes, this makes what panel member number three (3) seem clearer.

Question 7: According to the principles of systems theory, small changes within a specific component can lead to a large change at the output of the systems. Do you agree with this premise, can you explain why?

You answered: Yes, it comes down to a cause and effect. By one small element changing, results in a larger-more-macro change. This stimulates a chain reaction through the system.

Participant 1; Re: I agree with this comment.

Due to the reliance on each element, the systems based approach must regularly be reviewed or weaknesses are created. These small changes can have a domino effect on each of the other elements that combines to the systems based structure. The changes may be small, but if not considered in a holistic manner or without a clear understanding of why an element was implemented or structured in the first place you can change the basic premise of why and how it supported other elements within the system. Using the Swiss cheese analysis you can actually move the "hole" so that it now aligns with another hole. Do this with several or many small changes and you can create a weakness that is substantial, yet difficult to recognize or identify.

A clear understanding of the system is needed. This understanding needs to be underpinned by security risk management, integrated through security management plans, assessed and reviewed regularly with understanding of the holistic approach. For example, time changes in procedures, staff, complacency and a lack of training or understanding of initial concepts are enemies of the systems based approach.

Participant 3; Re: Yes I do. For me, one of the reasons our system breaks down is that we are unable to intervene, based on the intelligence due to pressures (political) on the system. Small systems changes can have a significant impact at a much higher level and can change the strategic direction of an agency.

Feedback: Too this question both panel members' number one and three agreed. In addition, panel member number one's (1) views were in-line with your own, and states "due to the reliance on each element small changes in a system can have a domino

effect on each of the other element that combines to the systems based structure". The changes may be small, but if not considered within a holistic manner or without clear understanding of why an element was implemented or structured in the first place, you can change the basic premise of why and how it supported other elements within the system.

Panel member number one (1) draws on the Swiss cheese analogy from Standard Australia (HB 167: 2006, p. 59) where under normal conditions the holes in each security layer are covered up by subsequent layers of controls. However, small changes in the system results in the holes aligning with another hole, where if you do this with several or small changes you can create a weakness that is substantial, yet difficult to recognise or identify.

Qu: Do you agree with panel member number one's (1) views?

Res: Yes, each hole gets bigger as decay sets in, eventually aligning the holes.

In addition, panel member number three (3) stated that he agrees as small system changes can have a significant impact at a much higher level, and can change the strategic direction of an agency.

Qu: Do you agree with panel member number three's (3) views in relation to this specific principle of systems theory?

Res: I am not sure.

Question 8: Within your understanding of a system, can you tell me what you believe the key performance indicators are within a PPS?

You answered: The key performance indicators give you a measure, where you set goals in an organization to ensure you are achieving what the system is designed for, it is a monitoring process. As such, the elements of the PPS become the key performance indicators. They start off with a probability of detection, then a probability of transmitting an alarm actuation, followed by a measure of accurate assessment of the alarm cause, then a probability of communicating that alarm source to the appropriate response component of the system. Then, the delay time and response time based on their mean average become the following system measures.

Participant 1; Re: Key performance indicators are those items that you can use to monitor the effectiveness of the ongoing performance of each element of a system. If key performance indicators are not being met this could strongly suggest that a specific element is not delivering the full capacity or the outcomes for which it was specifically designed.

If an element is not delivering required performance full capacity or outcomes it may therefore not be supporting other elements within the total system in the manner for which it was intended to, designed and implemented.

These shortfalls in elemental performance is very likely to have an impact on the whole of the systems performance and therefore if "whole of system KPI's" are correctly identified, structured and monitored these will be directly influenced by elemental KPI's.

The KPi's include:

Management/Procedures

Log in out systems each shift, recorded training frequency, recorded proficiency assessment, recorded regular performance diagnosis. Annual-Bi-annual audits of staff training levels, of Standard Operating Procedures (SOP's), of response procedures. In addition, minutes of team meetings, minutes of management meetings and activities altered from annual, bi-annual audits.

Planning/Built environment

Frequency of physical inspections, frequency of maintenance (gardening type), frequency of maintenance (structure type), annual, bi-annual audit, action on annual, bi-annual audit. Inspection of Central Control Room (CCR) and physical environment. Inspection of perimeter zones (erosion, debris, materials) and actions, results of inspections.

Technology

System false alarm rates, nuisance alarm rates, maintenance records, service breakdown records, system down time records, repair period records, record of maintainer training records, records of maintainers agent accreditation, records of maintainer's site induction training, records of length of time to rectify "sign off" fault, independent audit of routine maintenance, records of daily tests and results, regular audit of compo entry integration testing.

Participant 3; Re: From a prisons perspective, the key performance indicators relate to the core elements of defence in depth, they start at deterrence where reducing opportunity provides a level of deterrence, then a capability of detection, within a context, the verification (assessment) of an alarm event, the delay aspects, where all of this is measured against the response capability. In addition, aside from key elements other key performance indicators include: fit for purpose (environment) reliability, robustness, and technical support. These aspects relate to probability of detection, nuisance alarm and false alarm rates.

Feedback: Too this question, panel member number three (3) followed a similar view to yours, proving what is considered tactical level key performance indicators within the system, as the systems key performance indicators.

Qu: Do you agree with this view relating towards the level of key performance indicators?

This view was also supported by the pilot panel study. However, panel member number one (1) provided a much more detailed account of the system key performance indicators, some of which were also reported by panel member number three (3). It is considered therefore that the key performance indicators reported by panel member number one (1) are operational level key performance indicators.

Qu: Do you support this interpretation?

Res: Yes, I mean ultimately it is a broad question. As such, a hierarchical level of key performance indicators needs to be articulated. The system needs to be designed and key performance indicators established through a top down approach, however, audited utilizing a Bottom up approach where the operational key performance indicators directly relate to the tactical key performance indicators which ultimately relate to the systems strategic objective.

Question 9: Based on your experience, do you believe the key performance indicators of the systems are related to the systems effectiveness? Can you explain how?

You answered: Yes. This is your means to ensure the elements are achieving your design goals. To ensure you can measure for any problems at its earliest opportunity. Key performance indicator reduction at the micro-level reduces key performance indicators at the macro level. The overall key performance indicator provides a strategic level of monitoring effectiveness.

Participant 1; Re: Yes, KPi's are and should be related to system effectiveness. If you refer back to my answer to question 7, I believe that KPi's are a measure of whether an element and therefore a system is delivering the outcomes and functionality for which it was designed. This directly determines or impacts on the elements effectiveness as a single element performing its required function and effectiveness is supporting other elements in its functions within the total system. Again, the Swiss cheese effect. If one or more elements of a system are not performing in the manner intended, they do not support system security and would therefore directly impact on KPI's.

Participant 3; Re: I do believe the systems performance indicators are related to the systems overall key performance indicators. We look at the selection of components from their individual key performance indicators, such as probability of detection,

nuisance alarm rate, false alarm rate etc, then combine them together into a designed whole.

Feedback: Too this question all panel members reported that they do believe the key performance indicators of the system are related to the systems effectiveness, based on the argument that key performance indicator reduction at the micro-level reduces key performance indicators at the macro level, where according to panel member number one, if one or more elements of a system are not performing in the manner intended, they do not support system security and would therefore directly impact on it.

Such a consensus was also reported by the pilot study.

Qu: Do you support that a consensus to this question exists?

Res: Yes.

Question 10: Based on your experience, do you believe that security systems decay?
You answered: Yes they do decay.
Participant 1; Re: Yes I do believe that security systems can and do experience decay.
Participant 3; Re: Oh yes.
Feedback: Too this question all panel members reported yes. Therefore it is interpreted that a consensus exists amongst the panel that security systems do suffer from decay.

In addition, a consensus was also reported by the pilot study congruent with this panel's consensus.

Qu: Do you support such an interpretation?

Res: Yes I do.

APPENDIX E
RESEARCH PANEL TWO: PHASE THREE EXPERT INTERVIEW AND FEEDBACK TRANSCRIPT

The following transcript was taken from panel two, member three's feedback (Round two participant interview) transcript from question 10 -20 to demonstrate a typical interview.

Interview transcript

Question 10: Too the question: Based on your experience, do you believe that security systems decay?

You answered: I believe security systems categorically decay. There is however, not a reason in the world why you can't keep the system working properly; however, to achieve this, over time maintenance costs will increase.

Participant 1; Re: Yes they do if they are not maintained.

Participant 2; Re: Yes of course.

Feedback: Too this question, all panel members responded yes, providing a consensus amongst the panel supporting the argument security systems decay. Furthermore, a consensus supporting the argument that security systems decay was also achieved by research panel one and the pilot panel. As such, it is interpreted that a consensus achieved across the research panel that security systems decay.

Qu: Do you support this interpretation?]

ANSW: Yes.

Question 11: Too the question: What is your understanding of security decay?

You answered: People install systems that do not understand what underpins them. We do design in parameters to facilitate for decay. For example, Figure 3 Shows how decay is considered in engineering aspects.

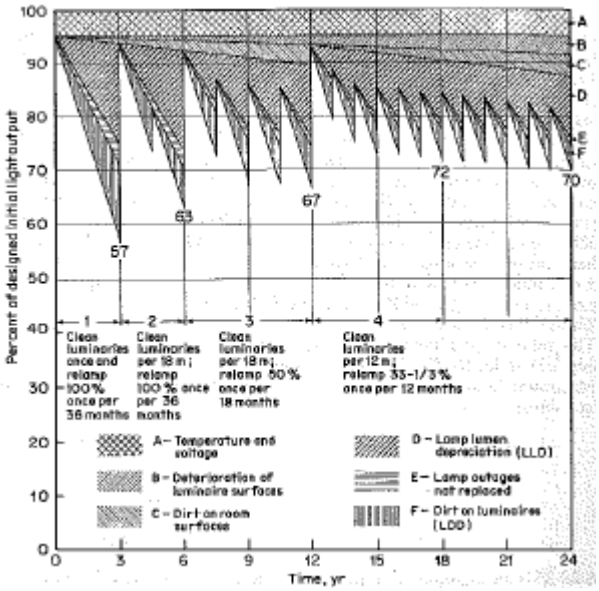


Figure 3: panel member three's lighting degradation diagram

However, the lack of knowledge and management of these parameters leads to security decay.

That is, a number of factors lead to decay:

- Lack of professional management is a significant factor,
- Lack of continuity in educating management on how the system works,
- Lack of formal training, where training is handed down rather than through formal processes,
- Physical aspects decay through lack of maintenance,
- Technology does get old and decays.

This once again refers back to the Campbell triangle (Figure 7.1), where decay occurs in all three aspects: management, technology and physical engineering.

There is however, no reason in the world why you can't keep the system working properly. That is, if you manage the engineering aspects of decay, there is no reason that you shouldn't be able to avoid decay.

Participant 1; Re: The degradation of security systems, processes and hardware (security) arrangements, and personnel procedures.

Participant 2; Re: The decline in the efficacy (effectiveness), and efficiency of the security function, and correlating increase in risk. Also the inappropriate response to security events which causes a new or updated security function which has no impact in altering or managing the risk, decay leads to adhoc security.

Feedback: To this question, panel member two (2) responded that security decay relates to the decline in the efficacy (effectiveness) of the security solution, and its correlating increase in risk. Panel member one (1) responded that degradation of the security systems, processes and hardware arrangement and personnel procedures is what he consider to be security decay. In considering these views, panel member one (1),

research panel one (1) stated, “Security system decay is the degradation in the performance of an element of the security solution. Both as a single element performing a specific function, and its role in supporting other elements in their function within the total system. This may not be a major failure of the system, but mere incremental decrease in performance that occurs over time. This decay may however occur incrementally and continue over an extended period to the point it has a significant impact on performance and effectiveness. Furthermore, this may be compounded further where this decay occurs over many or all of the elements within a system.

Qu: Do you agree with this view relating to security decay?

ANSW: Yes.

In considering panel member one’s (research panel one) views, you stated that systems are designed with parameters to facilitate for decay. Figure ? shows an engineering aspect of such inbuilt tolerance. That is, decay occurs when performance falls below these engineered parameters. However, a lack of knowledge and poor management of these parameters leads to security decay

QU: Do support this representation of your views?

ANSW: Yes that’s right. Build in the quality that will maintain the system over time.

Question 12: Too the question: Can you tell me about a time when you experienced security controls degrading, what occurred?

You answered: I cannot name specific areas or organisations. An audit (security audit) I did was on an old system. However, I had the privilege of speaking directly to the people who set it. When I do an audit I look at:

- Management
- Physical
- Technical.

The system I was auditing had clearly suffered decay because no-body wrote down in the first place what the system was meant to achieve (no measures of performance). I found that a lack of education and awareness in how the system is meant to operate. To overcome such systemic decay, the systems purpose and aspects needs to be written down, as a document. What occurs is that changes based on wants are implemented; however these changes are made to satisfy people, not to maintain the security plan. The system needs a defined security plan otherwise changes occur which lead to decay.

Participant 1; Re: Yes in people’s apathy, for us, day one we give them an induction awareness lecture, then they walk out and forget it immediately. Then security processes

decay over time when nothing happens. For example, people do not report security incidents, even though they have been told and trained to report them. This failure breaks down the knowledge of what is going on in the field.

Participant 2; Re: Often why I as a consultant is called in, in the first place is to review security after an incident. In our experience we find that security decay occurs in non systems arranged approaches to security, where isolated security measures are failing. For example, I conducted a cash handling audit for local government. During the audit I found that whilst staff believed they were protected by a duress alarm system, the system had been disconnected for two years. In addition, the built environment maintenance had decreased due to leasing issues. However, the operational environment had changed, where cash movements had increased dramatically. I was called in as a robbery in the area occurred, where in response to that robbery the security improvements were excessive after the fact.

Feedback: To this question all panel members provided practical examples, highlighting they have experienced security decay. In-line with this panels self report of experiencing security decay, both the pilot panel and research panel one also provided practical examples of where they have experienced security decay. For example, research panel one provided the following examples:

Participant 1; Re: There are many practical examples of where elemental and or, systems decay/degrading. Examples include:

1. Lack of maintenance in the perimeter zones (weeds and other feral growth) causing an increase in nuisance alarm rates, causing lack of confidence and increasing operator's complacency, Lack in electronic system maintenance, having the same cause and effect as above.
2. Poor or total lack of daily testing procedures being implemented, resulting in a failure to identify systems not working. Training occurring for new staff by handed down experience rather than from training processes, meaning incorrect procedures or bad habits being passed down.
3. A lack of ongoing training to reinforce correct processes and procedures, having the same cause and effect as above.
4. Changes to the perimeter built environment or changes to adjacent areas without considering the perimeter detection and surveillance systems.
5. Changes to the Central Control Room (CCR) physical environment without consideration of operational efficiency or operational performance.

6. Changes to electronic systems, set up in CCR, i.e. CCTV/SMS etc to suit personal preference without reference to initial design considerations and integrated response requirements.
7. Physical deterioration of physical elements, which are not maintained, reducing the effectiveness of the element as a barrier, or in whatever function it performs. There are many others

Participant 2; I have noticed that as staff competencies fluctuate, this fluctuation alters individual key performance indicators where decay occurs in relation to the reduction in competencies and capabilities of the people components. That is, most agencies work at the lowest common denominator where system key performance indicators are based on the lowest standard, this includes training, of competency to achieve that aspect of the system. System key performance indicators increase with competency increase, and of course decrease as those competencies decrease.

Participant 3; Re: Yes, a situation involving staff's lack of familiarization/awareness with procedural security, during perimeter alarm checks. A system we put in introduced a microphonic alarm in a cowling, where the decay relates to improper testing around its designed requirement. Often staff do not test systems properly, in-line with their procedures resulting in technical decay as we do not know if the system is working based on its design configuration. Also camera alarm presets, staff when testing perimeter systems do not test all aspects such as alarm preset positions and field of view objectives for cameras.

Also, environmental impact on physical structure, for example, on a high security fence the plinth was not designed to move water, therefore water sat at the base of the fence, and due to the high salt content in that area physical decay of the barrier occurred. Such physical decay needs to be considered at the design stage of a security project.

As such, it is interpreted that security decay as a phenomenon has been directly experienced by all research sample members.

Qu: Do you support this interpretation.

ANSW: Yes.

Question 13: Too the question: In considering the argument that security controls decay, how do you think this occurs within a systems approach towards security?

You answered: Once again the Campbell triangle (Figure ?), decay occurs in each, or all aspects of the triangle, then based on what a system is, and how the system operates, decay occurs in-line with what underpins the system.

Participant 1; Re: Based on what we have talked about, normally a benign security environment leads to a reduction in the security program, that is small changes. These changes eventually leave the system vulnerable so when something does happen everybody's guard is down.

Participant 2; Re: A breakdown in monitoring and reviewing, as well as accountability, against external pressures, finance, people over time. Systems require efficiencies, but security events can lead to spending cuts within the system which can lead to a large change within the system.

Feedback: To this question, you responded, once again the Campbell triangle (Figure ?), decay occurs in each, or all aspects of the triangle, then based on what a system is, and how the system operates, decay occurs in-line with what underpins the system. In-line with your views, panel member one (1) research panel one (1) stated, "I believe that security decay within a PPS occurs within its individual elements, them propagates through the system. Decay occurs at the base elemental level over time". In-line with this approach, panel member three (3), research panel one (1) stated, "Any aspect of decay affects the rest of the system". For example, multiple false alarms can propagate through the rest of the system, when complacency sets in, alarm inputs are not discriminated or reported, ultimately affecting the response aspect of the system.

Qu: Do you support this approach to how security decay occurs within a systems approach?

ANSW: Yes, it can be an outcome.

Furthermore, panel member three (3), research panel one (1), and the pilot panel reported that security decay can affect the systems deterrence aspect as well.

Qu: Do agree with this view?

ANSW: Yes it can, that's a fact.

Question 14: Too the question: The concept of security decay argues that decay within a PPS occurs within individual constituents, within the PPS, and its effects propagate through the system from this point. Based on your experience, do you support this premise and why/why not?

You answered: Yes, decay can occur in all three elements based again on the Campbell triangle.

Participant 1; Re: Yes. Something serious would have a knock on effect elsewhere.

Participant 2; Re: Yes. Small changes can lead to large security implications, much like a chain. A chain is only as good as its weakest link or point. When that weakest point breaks the result can be larger.

Feedback: To this question, all panel members responded yes, based on and in-line with their earlier responses. In considering the panel's consensus responses to this question, research panel one supported through consensus the summary that a system is a combination of various inputs, where each of these inputs has a function in performing a specific function and supporting functions of others (interrelationships) therefore small changes across many/all elements can have a major impact on the system at the macro level.

Qu: Do you agree with this summary and support that a consensus exists within the research sample that, based on the above reasoning, decay within a PPS occurs within individual constituents, within the PPS, and its effects propagate through the system from this point.

ANSW: Yes.

Question 15: Too the question: Systems theory and specifically an effect referred to as the butterfly effect suggests small input changes within a system can result in large changes at its macro output. Do you feel this applies to a PPS? Can you give me an example where you have come across this?

You answered: Yes. However, every time you do a security system, there are 2 x mission critical analysis.

1. Establishes the context required, analyses the system for single point failure. This analysis considers built in redundancy to stop single point failure.
2. Apply the tools, to look for the single point factor, which leads to the butterfly effect, to overcome it. That is, compatibility of design, where the key is inbuilt redundancy. Once again, Figure ? Shows how inbuilt redundancy works, decay occurs when the effectiveness falls below this inbuilt redundancy.

If these aspects of system design do not occur, yes you will have the Butterfly effect.

Participant 1; Re: Yes it does. For us, during drug and alchohol testing for mine sites. If the system is not in place, or effective, this deficiency can lead to a security or safety related incident.

Participant 2; Re: Yes, as discussed above, one small change leads to larger chain reactions.

Feedback: Too this question, all panel members responded yes. However, panel member three (3) highlights the point that inbuilt redundancy to stop single point failure is/should be built in, where decay occurs when the effectiveness falls below this inbuilt redundancy, and states "if these aspects (Figure) of system design do not occur, or are not maintained, yes you will have the "Butterfly" effect. In considering panel member three's (3) views, panel member two (2), research panel one (1) provides the following supporting statement: Yes I agree with this metaphor being applied to PPS. The example I can give relates to procedural decay. I have observed that for systems an initial level of training is introduced, at a specific level. This training has a macro-level output throughout the system. Over time, when this level of training is declined, that level of competency is declined, affecting the remainder of the security system.

As such, it is interpreted that, certain conditions considered in-line with panel member three (3), research panel two (2), that a consensus exists across the research sample that the "Butterfly" metaphor does apply to a PPS.

Qu: Do you support this interpretation?

ANSW: Yes.

Question 16: Too the question: Based on your experience what do you consider the effects of decay are?

You answered: The effects are that if the system decays, it is directly proportional to the loss of risk management.

Participant 1; Re: A more apathetic work force, degradation may affect assets, personnel and the service delivery of your product.

Participant 2; Re: Invariably it will lead to a security related incident, a degree of loss, then in response excessive spending, and potentially re-justification of the system itself.

Feedback: To this question, a common theme is that security risks increase as a direct result of decay within a security system. Research panel one (1) supported through consensus that decay occurs at the component/constituent level, then degrades key performance indicators, reducing sub-system key performance indicators. Such decay ultimately affects the risk reduction aspects of the system, bearing a strategic impact on the organisation.

Qu: Do you support such a view towards the effects of security decay?

ANSW: Yes.

Question 17: Too the question: Once decay has set in, do you think its effects, both at the point of manifestation and throughout the remainder of the system are reversible. How do you think so, or why don' you think so?

You answered: Yes, absolutely. Because as soon as decay has been recognised (independent audit is usually required), through professional management of the problem the decay can be overcome.

Participant 1; Re: Yes, but it does come down to leadership and management support and of course the necessary resources. You need the will to turn decay around.

Participant 2; Re: Yes they are reversible. Whether that happens comes down to management structure, through maintenance review, awareness recognition, and preventative maintenance.

Feedback: To this question, all panel members responded yes, providing a consensus within the panel that decay, both at its point of manifestation and throughout the remainder of the system are reversible. Such a consensus was also achieved by the pilot panel. However, research panel one (1) argued that it depends on what the decay is related to. Research panel one (1) agreed that procedural decay could be reversed and prevented through management, that is, ongoing monitoring and reviewing of the people component of the system. However, physical and technical decay can only be controlled/delayed through processes. Research panel one (1) agreed that all physical and technology components have a life cycle, where eventually they will decay beyond a repairable state. However, with proper maintenance, decay can be slowed and managed.

Qu: Do you agree with these additional aspects relating to security decay from a systems perspective?

ANSW: All points are right to a point. From an engineer's perspective, technology has a finite life 8-10 years, however this is usually pushed to 12, it does vary from system to system. There is no reason why the system cannot be kept at the original detection capabilities, however these costs associated with this will rise each year. If you budget for about 10% of the systems costs a year it would balance out across the systems life cycle. With proper maintenance there is no reason why the system cannot maintain its design specification capabilities over its life cycle.

My philosophy is that decay is a quantifiable factor, decay must be managed so it does not fall below the inbuilt redundancy level.

Furthermore, panel member two (2), research panel one (1) stated, "decay can only be countered if it is understood".

Qu: Do you agree with this panel member's view?

ANSW: Yes, once again you need to professionally manage the system in-line with the triangle, to do this you must understand how it works, if you don't understand how it works how do you manage decay?

Question 18: Too the question: Do you think decay can be avoided. How do you think the effects of decay within a security system can be avoided, or why don't you think the effects of decay within a security system can be avoided.

You answered: Absolutely, and unequivocally. It can be done (avoided) through professional management which looks after the technology, physical aspects and operational aspects. If you manage the triangle you manage the system, avoid decay, that is, avoid the movement below the level of inbuilt redundancy.

Participant 1; Re: Yes, possibly. It comes down to management's will and capacity. Decay is a political concern rather than a technical aspect.

Participant 2; Re: Yes it can be avoided, through the proper management, the monitoring and review of the systems key performance indicators, as the key performance indicators tell you what is going on and wrong. In addition, through a system driven by clear policy.

Feedback: To this question, all panel members responded that decay can be avoided, where panel member three (3) stated through professional management, focusing on technology, physical and operational (procedural) aspects. According to panel member three (3), if you manage the triangle, you manage the system, and avoid decay, that is, you avoid the movement below the level of inbuilt redundancy. In-line with panel member three's (3) views, panel member two (2) states, "proper management, monitoring and reviewing the systems key performance indicators enables decay to be avoided, the key performance indicators tell you what is going on and wrong.

However, research panel one (1) argued that procedural decay can be avoided, however, technical and physical decay can only be managed, and its effects delayed through proper monitored maintenance.

QU: Do you agree with this additional information?

ANSW: Not true, as stated, both physical and technical aspects of the system can be maintained at their commissioned level over time, that is over the cycle of the system. It can be maintained to ensure over the systems life cycle that it performs at the designed capabilities, for example the designed detection capabilities "Commissioned level performance" .

As such, at this point, it is interpreted that a consensus exists within the panel that decay can be avoided through professional management, which focuses on the aspects of panel

member three's (3) triangle, where by focusing on the systems performance measures (KPI's) enables the professional management of the triangle, towards avoiding decay.

Qu: Do you support this summary and interpretation that a consensus in relation to these aspects of security decay.

ANSW: Yes, but I still don't like the key performance indicator terminology as you could end up with a tick in the box approach, the system requires professional knowledge to manage the system to avoid decay. What worries me is the idea that we can develop a tick box solution where it is considered that the sheets provide the expertise not the people, especially since over time the impression will be anybody can manage the system using the tick box approach, and this just isn't true.

Question 19: Too the question: Do you believe the concept of decay has a place in the risk management process. If so where in the process, if not why not?

You answered: Yes it does have a valid place, you would have to assess for decay. You need to able to take the security objective measures to management, to show them how we don't have enough money to manage the system. The only place decay has, is that if you don't manage it properly.

Participant 1; Re: Yes, I think in the ISO 31000, the context section, decay is a risk.

Participant 2; Re: Yes, in establishing the context. Security decay is a context, recognising it as a risk. Also, in the evaluation process.

Feedback: To this question, all panel members responded yes. In addition, a theme developed where the majority of the research sample see that decay needs to be considered as a security risk. A consensus was reached by research panel one (1) that security decay should be considered as a "system", considered at the design stage, considered against its consequences, with a view to countering it where practicable as a risk treatment, towards designing out decay, then continually assessed for in the monitor and review stage.

Qu: Do you support this summary and finding?

ANSW: Yes.

Question 20: Too the question: Based on your experience, is there any facet of security decay which you can add to the research enquiry. This may include factors associated with either the cause of decay or impacts from it?

You answered: Decay is caused because of a lack of professional management, security management. That is:

- Lack of education
- Lack of system awareness

- Employing the wrong people to manage it, for example ex police or ex military people who don't understand the technical aspects of security, what they are actually managing. This goes back to the quantifiable performance measures of the system.

Participant 1; Re: Security decay as a concern will be constantly driven by organizational culture, then the resources prioritization, coupled with the threat landscape.

Participant 2; Re: Security decay is common in various forms.

Feedback: Too this question panel members from research panel one (1) provided the following responses:

Participant 3; Re: Security decay will always be managed against the level of recurrent funding available.

Feedback: Too this question, panel member number three stated that security decay will always be managed against the level of recurrent funding available.

Qu: Do you agree with this point?

ANSW: No necessarily, it comes down to professional management.

Res: When you put your capital submission forward you must, at a strategic level, indentify whether the system you are putting in is achievable, and you can maintain the system you are putting in. This recurrent funding submission is required at the design stage.

Qu: Do agree with panel member three's responses?

ANSW: Absolutely.