American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

The Application of the Tripod Beta Approach in Assessing the Effectiveness of the Port Security Measures in Compliance to the International Ship and Port Facility Security Code

Ghim Teck Lee[a*], Muhammad Zaly Shah[b]

[a]*Malaysian Maritime Academy, Window Delivery 2051, Masjid Tanah Post Office, 78300 Masjid Tanah, Melaka, Tel:606-3882270, Fax: 063876700*

[b]*Transportation and Logistics Research Group, Faculty of Built Environment, Universiti Teknologi Malaysia*

[a]*Email: lee_ghimteck@alam.edu.my,* [b]*Email: b-zaly@utm.my*

Abstract

Presently the port facility measures their compliance ISPS Code requirement is via periodical internal and external audit where documentations sampling are cross reference to the measures and procedures stipulated in the Port Facility Security Plan (PFSP). Unlike the safety related processes where the availability of positive performance measurement system allows an organization to determine the effectiveness of the system implementation and identification of level of performance. The absent of such system in the security environment leave questions on the method of determination on it effectiveness level, and how the port facility would positively identified gap(s) in the implementation without having to expect for accidents or attacks on the facility to occur, to determine the level of effectiveness. This research studies the various quality and quantity assessment process for determining risk and accident investigation tools used by the industry. From the tools available, Tripod-Beta accident investigation approach is identified as the most appropriate approach to measures the effectiveness of security measures and procedures implemented by the port facility. From there the audit measurement methodology was developed and tested on port facilities that complied to the ISPS Code requirement.

Keywords: International Ship and Port Facility Security (ISPS) Code; Security Risk Assessment; Accident Investigation; security measures and procedures; Security Audit; Threats; Vulnerability and Consequences.

---

* Corresponding author.

1. Introduction

Follow up from the attacked on two targets in United States on 11 September 2001, the International Maritime Organization (IMO) proposed the implementation of a new security measure applicable to ship and port facility. This proposal is contained in the International Ship and Port Facility Security (ISPS) Code [9] and its came into force on 1 July 2004. In compliance of the ISPS Code, the ships are issued with International Ship Security Certificate (ISSC) and for the port facility, the Statement of Compliance for Port Facility (SoCPF). Both certificates have the validity of five years. For the purpose of ensuring continuous effectiveness of the ISSC and SoCPF, the administration set out the mandatory requirement of periodical external and internal audit.

1.2 Statement of the problem

In the implementation of the ISPS Code for port facility, IMO empowered the port facility to carryout self-assessment audit on its own facility in the form of self-assessment questionnaires made available in Maritime Safety Committee (MSC) Circular 1131 [14]. Detailed study of the questionnaire demonstrated that the focus fulfilling terms and conditions spelt out in the Code. Thus the MSC 1131 checklist is superficial as the PFSP must fully comply with the ISPS Code before they could be approved.

The analysis of the data collected and with reference to the literature review indicated that the present checklist MSC Circ.1131 does not completely cover the audit requirement where it lacked the following areas:

- It focuses heavily on the fulfilling the ISPS Code requirement, thus neglecting the actual implementation of security measures and procedures in the PFSP;
- The Circ.1131 checklist only cross checked with a single source only and that is with the PFSO but not with other sources of data or information;
- The Circ.1131 does not provide a structured audit management program which was needed in this type of environment as the objective of the checklist only on ISPS Code general compliance but not the PFSP requirement which is more specific or individual in nature;
- There is no continuity between prevention and response with consequences management, which mean that the before event initiatives is not coincide with the mitigation strategies in after math of any particular event.

For the above reason, the statement of problem for this research is “The absent of security performance measure system for ISPS Code resulted in difficulty in measuring and managing the effectiveness in the implementation of the security plan for port facility”.

1.3 Objectives of the research

With reference to the above statement, the objectives of the research is to provide a performance measurement tool to measure the effectiveness of the security implementation in the proactive manner.

1.4 Literature Review

In security, hazards occurred due to intentional activities with objectives of causing disruption, damages, injury and even to the extent of death and environmental catastrophes by the intent individual or organization. Reactive approach for performance measurement is not an acceptable norm for security environment as the extent of damage would probably be huge and it is coupled with the capability of the individual or organization as mentioned by author [15]. Thus a proactive approach would be seen as the only option of ensuring unforeseen event or threat does not occur.

MCS/Circ. stated that the effectiveness of the implementation of port facility security measures is a continuing responsibility. The weakness of the self-assessment audit as well as any other auditing processes, where its worked on the comparison of stated objectives against the actual implementation of the agreed processes, but not the effectiveness of the security initiatives, which is protecting the facility against any possible threats. SOLAS [12] is one of IMO's convention govern the safety of life at sea.

Author [16] defines risk as a measurement of a hazard's significance involving simultaneous examination of its consequences and probability of occurrence using a combination of practical experience and relevant information on the system and its operating environment, and another author [11] defines risk assessment is define as "The process which determines what can go wrong: the pro-active approach" and is intended to be a careful examination of what, in the nature of operations, could cause harm, so that decisions can be made as to whether enough precautions have been taken or whether more should be done to prevent harm. British Standard (BS 4778) defines risk management as the process whereby decisions are made to accept a known or assesses risk and /or the implementation of actions to reduce the consequences or probability of its occurrence. According to United State Coast Guard (USCG)'s Coast Guard Marine Safety and Environmental Protection Business Plan (2005), there are different types of risk are an important factors in many types of decisions and risk assessment can be range from very simple, personal judgements by individuals to very complex assessments by expert teams using a broad set of tools and information. The key to risk assessment is choosing the right approach to provide the needed information without overworking the problem.

Author [5] agreed that risk assessment is the proactive approach in identifying risks or hazards, and it will likely be experience in certain work processes. It is generally carried out before the commencement of any tasks and it is used as an approach of proactively developing or incorporating preventive measures to ensure the least possible disturbance toward achieving organizational objectives. In simple wording, it is a process that provides early warning of possible risk or threats. Risk assessment can be approach in a macro and micro way as the process can be varied depending on the nature of the objectives and resources involved in supporting the realization of the objectives. The author [17] explained that risk assessment has to be systematically done because failure to identify the correct hazards would result in the failure to apply correct preventive measures.

There are two forms of approaches used in carry out risk assessment and at time both approaches are combined to provide more effective evaluation of the specific area of work or concern as mentioned by the author [6]. The first approach is the quantitative approach which is used when there is sufficient data to work with in identifying

hazard and likelihood of threat, such data include previous accident/incident records, survey reports, research data and equipment manufacturer manual, which are provide factual data to allow for the quantifiable input to be placed in evaluating processes. The second approach is used in situation where the related work processes is still new and lack of factual data, the qualitative approach of risk assessment is used to facilitate risk identification and formulation of preventive measures including placement of necessary physical barriers. The existing of records of past event would able to provide quantitative assessment possible but in situation where the absent of such data in situation where it is a new facility and lack of enforcement agencies support, the qualitative assessment approach have to be in place and data collection is through second party resources through public domain. Ratings allocated for the likelihood of occurrences to allow easy measurement and determination in the focuses on the undesired event. It is necessary so that the organization could place priority of a particular event and at the same instances to allow allocation of resources and concentration during the risk assessment processes as there may be large numbers of possible occurrences that might be experience by the organization especially when handling high volatile cargo or consignment. As time would be limited, thus by assigning specific value rating, it allow the organization to paid extra attention on undesired event that having high value and allow the organization to return to tackle low value event. The availability of past record would further facility this stage of assessment.

At time, the assessor will require to provide measurable statement to each sub-heading to facilitate the level of consequences for measurement purposes. The level of consequences will be based on the weightage place on each consequences and its contribution to the functions of an organization and the rate of recovery in case where the actual event occurred. The ratings allocated generally depending on the risk assessment tools that are being applied at the time of the assessment. Some of these risk assessment tools are such as Fault Tree, Checklist, Brainstorming, HAZard Operability (HAZOP), What if, Structured What If, and Failure Mode Effect Analysis (FMEA).

Accident investigation is the reactive and systematic approach in determining what causes a particular accident or incident. Author [19] emphasis that the focus is from the identification of direct, indirect and root causes, a lesson can be learned so that future similar occurrences can be avoided all together. Accident is defines as “An unexpected, unplanned, unorganized, unpleasant, unfortunate “event” that happened and resulted in damage, injury etc”. Investigation is defined as “An effort to discover and examine all the information, facts about “something” example are near miss, incident and accident. Accident is always unplanned and generally does not necessary occurred in a particular instances or single cause, as it is always believed, there must be existence of error chain or error trail that leading to an unsafe event. The accident investigation purposes are to determine those causes and identified weaknesses in the existing barriers. Only from that approach is the investigator would be able to identify the root cause and recommend enhancement in the existing processes and/or procedures to prevent recurrences. Authors [19, 4] agreed that accident investigation is a process of determining the facts contributing to an accident and no intention of placing blame on any individual although presently that the common practice in the industry.

Author [19] mentioned that fact-finding or investigation begins during the collection of evidence. All sources of information (e.g., accident site walk-throughs, witness interviews, physical evidence, policy or procedure

documentation) contain facts that, when linked, create a chronological depiction of the events leading to an accident. Facts are not hypotheses, opinions, or analysis. Facts are deduced to determine the causal factor that contributed to the accident and he [19] defined Causal Factors as "the events and conditions that produced or contributed to the occurrence of the accident". Causal factors can be divided into three separate but inter-related types of causal factors and they are:

a) Director causes
b) Contributing causes or indirect causes
c) Root causes

The direct cause of an accident is the immediate events or conditions that caused the accident whereas contributing causes are "events or conditions that collectively with other causes increased the likelihood of an accident but that individually did not cause the accident", and root causes are the causal factors that, if corrected, would prevent recurrence of the same or similar accidents. Root causes may be derived from or encompass several contributing causes.

After any accident, the investigator commences evidence collection activities through various resources available at the time in various forms mainly human or testamentary evidence, physical evidence and documentary evidence. The evidences collected will be studied in three general approach, they are the deductive approach, the inductive approach and the morphological approach using various tools available today such as Fault Tree Analysis, FMEA, HAZOP, Tripod Beta and Event Tree Analysis. All these tools have a single objective that is to identify failed barrier and determine why these barrier failed.

The Nautical Institute defines safety management as a process which coordinates resources and activities to ensure that an acceptable level of safety is achieved for a situation or system as mentioned by author [17], and in Clause 8 Paragraph 8.1 and 8.3 of International Safety Management (ISM) Code made it mandatory for the shipping companies to document the actions required in situations that may be constitute as emergency situation and at the same time identified all possible hazard that the vessel/s would likely encountered or experienced. Similar requirement also stated in Section 9.4 and 16.3 Part A of the ISPS Code where the ship and port facility respectively in their security plan to document the possible hazards or risk that they might encountered and the response measures in cases of emergency. It has becomes a mandatory requirement in any company safety or security management system and manual to have risk management as well as mitigation strategies for emergency situations to be in place.

Authors [15, 17, 18, 19, 20] emphasis the need to include both element of risk management and emergency respond in the security and safety manual respectively as it provide a totality in the safety management of the company activities. Presently both activities of risk management and emergency respond are handled as separate initiatives and most of the occasion they are not interrelated. When the activities were developed on the piece meal basis, the effectiveness of the implementation may become a question as the barriers created will also be fragmented.

The earliest origins of bow-tie methodology are unknown but the earliest mention appears to be an adaptation from the ICI plc Hazan Course Notes 1979, presented by The Universitity of Queensland, Australia [7]. Authors [7,21] said that the ultimate aim of bow-tie to demonstrate control of hazards, it is therefore necessary to identify those hazards in the first place and follow up with the risk assessment and provide a framework to demonstrate effective control. Figure 1 illustrate typical structure of bow-tie diagram where the event is placed at the centre of the attention rather than at the end if compared with risk assessment and accident investigation methodologies where the event is located at either end and from there works forward or backward.

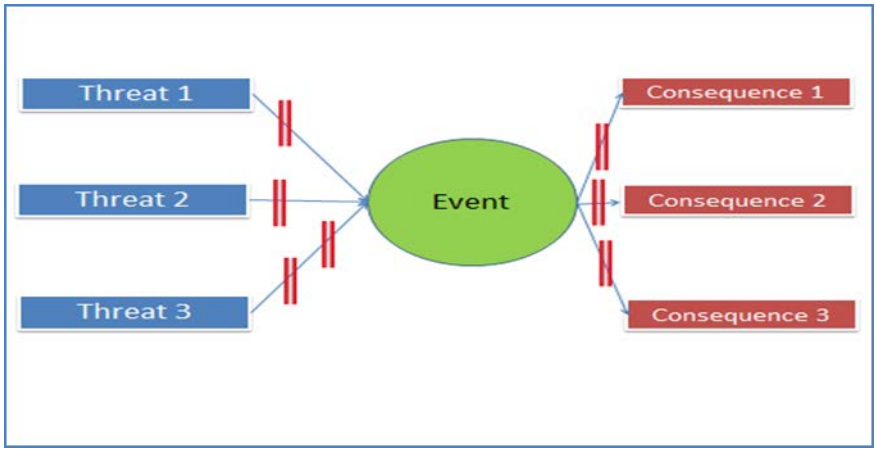

Figure 1: Illustrate a typical Bow-tie diagram in

Bow-tie models are tools for integrating broad cases of cause-consequence models. The familiar fault tree and event tree models are 'bow-tied' in this way and indeed attaching the fault tree's 'top event' with event tree's 'initiating event' originally suggested the bow-tie methodology. It is provide a 'bird's eye view for focusing on causal chains and projecting these onto the space of consequences. These consequences will be factored into decision problems for risk management. Bow-tie consequences side forms an interface with the decision models. Decision taken will reflect backward to causes. This structure not only has proven a worthwhile concept in accident prediction, it also has proven its worth in analyzing past accidents and suggesting improvements to prevent further re-occurrence which back up the original objective of accident investigation of "lesson learned". The selection of the centre of the bow-tie is crucial for the analysis. Author [1] mentioned that the causes and consequences of this event form the bow-tie and form a slice out of all the things that happen in this world. Any event can be considered a cause and any event can be considered a consequences.

According to the author [7], Bow-tie provides a robust, comprehensive yet simple means of "rolling out" the main points from a risk assessment exercise or HSE case. Authors [2] agreed that it is possible to use the bow-tie in conjunction with Tripod technique as well as Layer of Protection Analysis (LOPA) which provide for the qualitative and quantitative approach respectively in risk assessment.

After the causes and consequences are recognized, the barriers can be placed in between them which may be in the form of operation procedures and management system. The barriers as illustrated in Figure 1 comprises of various approaches and generally they comprises of passive barriers, active barriers and behavioural barriers.

Passive barriers are those barriers that perform their function without any intervention, whether they control expected flows of energy or protect against unexpected one. Active barriers do need some activation to become functional, which may be hardware or software driven. Very often a barrier involved hardware, software and behavioural elements because the full operation of a barrier to fulfil a safety function has to have 3 separate activities or phases. The 3 phases are detection, diagnosis and action.

Author [3] agreed that the setting of barriers at the fore part of the event alone would not be sufficient thus it is recommended barriers to be setup after the event has Figure 1 Bow-tie with barriers placed on either side of the event occurred with the purpose of ensuring further damage or lost of life would be minimized.

2. Methodology

In the effort to determine the most suitable methodology to be used for the purpose of this research for the development of Security Performance Measurement System (SPMS) with the purpose of providing the Port Facility Security Officer (PFSO) with structured security risk assessment methodology and a measurement tool to allow the PFSO to measure the effectiveness of the security implementation in the proactive manner. A total of 24 risk assessment and accident investigation methodologies were studied with the following criteria:

a) Value to the analysis – whether qualitative and/or quantitative;

b) The need of specialization and training in the use of each methodology;

c) Its application – whether applicable for risk assessment, accident investigation or both;

d) Its ability to determine the root cause/s;

e) Its process application – whether for existing work process, new work process or applicable to both new and existing processes.

The above five criteria were chosen for the following reasons:

1. In item (a) above, the qualitative or quantitative approaches would allowed the analysis outcome to be determined either on the quality or quantity of the assessment for the purpose of evaluating the relevancy of the data collected and at the same time allowing assessor to make decision based on specific facts or numerical measurement, or both;

2. With reference to (b), the knowledge and experience poses by the evaluator/assessor/investigator would able to add value to any analysis as they are able to appreciate the processes involved and the reason for specific actions taken in assessing specific situation or scenario and the knowledge and experience would allow the assessor to provide specific recommendation to further enhances the processes and suggest improvement steps to avoid future recurrences, the subject matter expert knowledge and experience would be more relevant in methodology where qualitative approach of assessment is in discussion;

3. With reference to (c), some methodology is design purely for specific activities and at time it has difficulties to provide complete picture or bird eye's view of the whole assessment processes. The criteria is chosen to determine the methodology that would able to cover the whole work activities and demonstrate that various steps are put in place to manage the risk as well as mitigate the consequences, which is at the after the event where the mitigation activities are demonstrated;

4. With reference to (d) above, root cause analysis is a critical step to determine what are the actual causes that contributing to the failed barriers and it also demonstrate the level of support up to the management level put into place to ensure it is implemented;

5. Reference to (e) above, any level of application reflects the effectiveness of the system to foresee potential risks and determine the action necessary to prevent unforeseen occurrences.

Analysis of the various methodologies observed that Event Tree Analysis (ETA) and Fault Tree Analysis (FTA) methodology are the two analysis tools that can be applied for the risk assessment and accident investigation and at the same time provide qualitative and quantitative analysis/measurement outcome. At the same time, FTA and ETA also suitable to be used for existing activities as well as new activities. For the context for this research, existing activities are referred to activities that has been carried out before or routine FTA and ETA processes also allow the assessors/investigators the determined the root causes or contributing factors leading to any failure in the process delivery so that remedial actions can be taken to prevent future recurrences. It is also observed that Tripod Beta methodology which traced its origin from Tripod methodology provide full view of the assessment flow including it capability by be used not only from the traditional accident investigation point of view but also risk assessment as agreed by both authors [18,21]. As Tripod Beta methodology main focus is to identify root causes to system/process failure, it is feasible tool to determine system effectiveness and with reference to the earlier security assessment principle that the vulnerability of a particular security measures and procedures would depend on the internal organization effective in ensuring effective implementation as the external factor such as threat is beyond organizational control. Thus Tripod Beta methodology would be an ideal tool for measuring effectiveness of the security implementation and at the same time identified root causes of implementation failure. Bow-Tie methodology is observed in comparison with other methodologies that provide combination of risk assessment and accident investigation in assessment of risk, is that it provides a total coverage in a simplified bird-eye view (single diagram). At the same time, Bow-Tie methodology allowed adaptation of other methodologies in risk assessment or accident investigation, and combination of both. This combination would be ideal in the security environment, the stress in not only in risk assessment but also consequences management for the purpose of preventing or minimizing further damage as mentioned by author [17]. The Tripod Risk Analysis approach is use as the tools to measure the effectiveness of the implemented security initiative as it provide an inclusive view of every aspect in term of mechanism of implementation as well as root causes of possible failure. The Tripod Beta approach is favour in this research as it is a tool that provides a complete view of possible direct failure as well as indirect contribution to implementation of specific approach in accident investigation as well as in risk assessment as described by both authors [3, 7], and supported by another author [21]. Tripod is the methodology which can be applied to identify possible failure in each security barrier and identify whether these possible failure in the security barriers were recognised by the

management of the facility and preventive actions were in-place to ensure sufficient supports were provided. For each security barriers in-placed as barrier to provide protection to the potential target, the possible immediate cause to the barrier failure is identified and this is known as active failure, Pre-condition is where the contributory factor/s that may cause the failure and the Latent failure is the root cause/s that contributed the this overall failure and in most cases that may be leading to the failure of management to provide effective support or better known as root cause. This approach is recommended based on account that the major elements that is within the control of the port facility against any possible threat is its vulnerability and the raise or down grade of the vulnerability lies sole with the port facility as the first line of defence whereas intervention by government security agencies generally will be based on intelligent information received at the time and after event response, which would be too late in term of avoiding damages or the event occurrences. In most instances, single security measure will be able to provide solid security barriers against any possible threats and at the same time, any security barriers would require organization commitments to materialize it. These commitments will be based on the nature of barriers put in place. For example, if security personnel are position at the guardhouse to monitor the movement of vehicle accessing the facility and at the same time to ensure no unauthorized person able to gained access into the facility. The port facility need to ensure that the security personnel are trained in identifying and recognising behaviour of suspicious person or vehicles, parking bays are allocated outside the guardhouse to allow sufficient time for security personnel to verify the driver identification and contact relevant person in the facility without obstructing the incoming vehicles, physical barrier such as vehicle posts are positioned at the gate to inform approach vehicle that they have to stop and obtain permission before access, clear signage before the entrance to let the vehicle know that they are approaching a restricted are.

Table 1: Example of Tripod Methodology Adaptation to Proactive Assessment

Security Measure	Active failure	Pre-Condition	Latent Failure
Procedures to prevent unauthorized person and vehicle accessing the port facility	• Training of security personnel • Vehicle waiting area • Guard post/barrier • Signage	• Training need analysis • Threat and risk identification	• Company security policy • Management support

In the Tripod approach, the Active Failure is referred to the direct causes of particular accident and generally it associated with unsafe act or unsafe condition whereas Pre-Condition is associated with Personal Factor or Job Factor, and Latent Failure is the root cause leading toward the development of unsafe act or unsafe condition. Table 1 is the example of Tripod Methodology Adaptation to Proactive Assessment. Table 2 is the measurement tool developed for the purpose of measuring the effectiveness of the implementation of the PFSP for port facility. The table is divided into 4 columns with the column on the left taken directly from the Appendix 5 of

MSC 1131 covering the 3 major parts of the PFSP and the remaining are subdivided into 3 columns coincide with the Tripod Risk Analysis model of "Active Failure", "Pre-Condition" and "Latent failure". The second column from the left of the table 2 are the indicators of the physical or documentary evidence that the port facility must have in place to ensure effectiveness of the specific initiative that required to be enforced to ensure the security integrity of the port facility. Failure to have it in place could lead to failure of effective implement of specific security measures and procedures in compliance to the requirement of the Code. Column 3 reflects the circumstances of failure to put the initiatives into place and column 4 is the probable root causes that resulted in the initiatives were left out and not being focuses on. This tool will allow the PFSO to determine the initiatives required to ensure effectiveness of specific measures and procedures by obtain the necessary support but and also allow the PFSO determine the further initiative need to support the implementation of an effective security measures. To facilitate ease of measurement of the security implementation, the rulers in Table 2 are converted into single A4 page, which is name as Failure Contributory Factor (FCF) Checklist. This checklist content comprises of the reference to ISPS Code Requirement based on MSC Circular 1131, the ISPS Code descriptor with reference section of the Code including the code requirement below it and this is reference to MSC Circular 1131, and finally the three column namely active failure, pre-condition and latent. A total of 43 areas of security initiatives will be failure observed during the field research.

3. Result and Discussion

Table 2: FCF Checklist (2004)

FCF Checklist **ISPS Code Requirement (MSC Cir 1131)**	**Failure Contributory Factors** **Active Failure** **Pre-Condition** **Latent Failure**	
Ensuring the performance of port facility security duties (ISPS Code sections A/14.2 land A/14.3)		
(a). Does the port facility's means of ensuring the performance of all security duties meet the requirements set out in the PFSP for security level 1 and 2? (ISPS Code section A/14.2.1)		
(b) **Active Failure**	**Pre-Condition**	**Latent Failure**
• Security threat and assessment • Acceptable risk score • Barriers in placed • Clear documentation • Drills/exercises • Security awareness training	• Hazard and threat identification • Budget constraint • Lack of knowledge • PFSO competence	• Management support • Company security policy
(c) Evidence: 1. TRAM assessment contain percentage of acceptable risk score to indicate the level where further mitigation procedures/strategies are not required; 2. Availability of physical barrier in placed such as fencing, perimeter lighting, patrol schedule including at level 1 and 2, its frequency of patrol; 3. Confidentiality of M/PFSP including its physical location, and control of access to the plan; 4. Frequency of security inspection and check including random sampling reflected in term of percentage of vehicles check as well as type of vehicles; 5. Security awareness training for all port personnel where evidence are available through training record, schedule and modules covered; 6. Competency assessment through participation in the drill, exercises and periodical evaluation to continuously evaluate performance of all staff designated with security duties; 7. M/PFSO and support staff training ,drill and exercises; 8. Security and emergency response flow chart detailing contact list, contact point and external security assistance availability and contact including flow chart display in the control room for easy reference. (d) Remarks: 0 | 1 | 2 | 3		

For the purpose of determination of the level of effectiveness, a percentage compliance measurement system is devised to facilitate the Port Facility Security Officer to determine the overall level of effectiveness on the security measures and procedures implemented.

In the Failure Contributory Factor Checklist, a total of 43 areas of security initiatives and these 43 areas are grouped into 3 separate groups in the Table 3 below.

Table 2: Security Initiatives Grouping

Sr. No	**Grouping**	**Number of Security Initiatives**
1	Ensuring the performance of port facility security duties.	18
2	Controlling access to the port facility	17
3	Monitoring of the port facility, including anchoring and berthing areas	8

A point system is allocated for each security initiatives as in Table 4.

Table 3: Points Allocation Criteria

Compliance Points	Criteria for the points
0	Initiatives recorded in the PFSP but no evidence of physical/documentary support visible. Management support is absent.
1	Less than 50% of the security activities in Active Failure column are present with specific areas of concern for further improvement. Evidence available in physical/documentary forms.
2	50% and more of the security activities in Active Failure column exist and without specific area/s of concern. Evidence available in physical/documentary forms.
3	100% of the security activities in Active Failure with further enhancement initiatives.

With reference to table 3 and 4 above, a percentage weightage is allocated for each security initiatives implemented and the weightage is divided according to grouping as well as overall.

The purpose of dividing the initiatives in grouping to allow for better focus during improvement processes. The overall weightage calculation determination is as per table 5 below.

Table 4: Weightage Calculation

Group	Number of Security Initiatives	Maximum Points	Weightage Calculation (%)
1	18	3	Σ(Points Earned)/ (18x3) x 100 = X
2	17	3	Σ(Points Earned)/ (17x3) x 100 = Y
3	8	3	Σ(Points Earned)/ (8x3) x 100 = Z
Overall			(X + Y + Z)/3 = Overall Performance in %

3.1 Data Collection and Analysis -- Outcome of Field Test on Port A

This port specialises on handling of container cargoes including hazardous cargoes in container. This port is in existence in Malaysia for over 15 years and is one of the container ports in Malaysia that has the highest throughout per annum.

The port complied with the requirement of ISPS Code since 1 July 2004 and has already undergoes 1st renewal verification by Malaysia Marine Department and next renewal verification will be in 2014. The port has dedicated security department headed by a senior manager.

The following observations were noted during the field test on the FCF Checklist applicability:

a. The lists of deliverables in the active failure, pre-condition and latent failure columns need further explanation to assist the PFSO in tracing the support documents as it do not reflect the actual operational documents practice by the port facility and the coding of the documents are based on port specific coding system;

b. The criteria for staff, visitor and ship crew are not applicable as the port facility practices issuance of pass based on duration of stay in the port facility;

c. The checklist able to link a particular element of security equipment failure to lack of management involvement to effort to ensure immediate rectification is made on this equipment due to various level of approval are needed from separate department due to company policy of restriction the responsible department to deal directly with the vendor based on level of urgency and its criticality;

d. The port security assessment adapted the methodology recommended by the International Labour Organization's Code of Practice on Security in Port (2003) and there is no actual percentage on acceptable risk score to reflect the criticality level of each entity to be protected;

Table 5: Level of Compliance Score for Port A

Group	Number of Security Initiatives	Maximum Points	Weightage Calculation
1	18	3	34/ (18x3) x 100 = 62.9%
2	17	3	32/ (17x3) x 100 = 62.7 %
3	8	3	14/ (8x3) x 100 = 58.3%
Overall			(62.9 + 62.7 + 58.3)/3 = 61.3% Performance in %

With reference to Table 6, overall compliance score for Port A is 61.3% where it is noted that the port fully complied with the MSC 1131 requirement for access control, restricted areas as well as the management of the security and at the same time leaving more room for improvement.

3.2 Outcome of Field Test on Port B

This is one of the oldest port in Malaysia and the port handle multiple type of cargoes ranging from break bulk cargo, containers to liquid cargoes in bulk and hazardous cargo. This port has the capacity to handle vessel on domestic voyage right up to vessel on unlimited voyage trade. The compliance to the requirement of the ISPS Code is under the purview of the Safety and Security Department under the stewardship of a Senior Manager. Full co-operation was extended by the Senior Manager for the conduct of the field studies as well as drive through visit to the entire perimeter of the port facility. The port complied with the Code requirement since 2004 and the compliance endorsement was issued by Malaysia Marine Department.

The following observations were noted during the field test on the FCF Checklist applicability:

a. The lists of deliverables in the active failure, pre-condition and latent failure columns need further explanation to assist the PFSO as the support documentations were not named as per checklist and at the same time PFSO has not access to certain support documents as it is residing at other department such as maintenance record of certain security equipment such as Close Circuit Television Camera (CCTV) as well as maintenance contract;

b. The criteria for staff, visitor and ship crew passes are issue in electronic format and coding of the passes can be accessible electronically;

c. The checklist able to link a particular element of security equipment failure to lack of management involvement to effort to ensure immediate rectification is made on this equipment due to various level of approval are needed from separate department due to company policy of restriction the responsible department to deal directly with the vendor based on level of urgency and its criticality. This observation is similar to the first port;

d. The port security assessment adapted the methodology recommended by the International Labour Organization's Code of Practice on Security in Port (2003) and there is no actual percentage on acceptable risk score to reflect the criticality level of each entity to be protected. This approach is very common to all ports in Malaysia as it is a recommended approach by Malaysia Marine Department;

e. The checklist able to detect several weaknesses in the implementation of the Code especially the training provided for security personnel is very much based on the schedule training programme set up by the port and not through the actual need of the port with reference to the Training Need Analysis.

Table 6: Level of Compliance Score for Port B

Group	Number of Security Initiatives	Maximum Points	Weightage Calculation (%)
1	18	3	30/ (18x3) x 100 = 55.6%
2	17	3	34/ (17x3) x 100 = 66.7%
3	8	3	17/ (8x3) x 100 = 70.8%
Overall			(55.6 + 66.7 + 70.8)/3 = 64.4% Performance in %

With reference to Table 7, overall compliance score for Port B is 64.4% where it is noted that the port fully complied with the MSC 1131 requirement for access control, restricted areas as well as the management of the security and at the same time leaving more room for improvement.

3.3 Failure Contributory Factor Checklist Review

The field test carryout on the use of FCF Checklist noted that the checklist failed to facilitate the PFSO to carryout self-assessment of the effectiveness of the implementation of the security measures and procedures required under the Code even-though the checklist able to detect weaknesses in the implementation. The ability to detect these weaknesses lies most of the time on the knowledge acquired by the researcher based on his working experience in the field which is not the objective of this research.

The FCF Checklist must be able to facilitate the PFSO in carryout the self-assessment without the aids of external party and it should be able to provide relationship or link to the requirement under the Code. For the purpose the FCF Checklist was further enhanced by incorporating additional guidance note at the beginning of the checklist and the Criteria for FCF was included as an accompany document which will allow the PFSO to use as reference to the compliance to the Code.

For the FCF Checklist, it is further divided to 4 sections named as (a), (b), (c) and (d). These sub-divisions is to allow the PFSO to cross reference between the guideline and individual table. The sub-section (a) is remained the same which is the measurement criteria set out in MSC Circular 1131. The sub-section (b) comprises the 3 column which contain the bullet points checklist on the support documents, measures, processes and procedures

in Active Failure column follow by the Pre-Condition column which contained the bullet points checklist on the contributory factor the lead to the Active Failure and finally the Latent Failure column which reflect possible root cause to the failure to effectively implement the measures and procedures as stipulated in the Code. The sub-section (c) is a new sub-section incorporate into the checklist, this sub-section provide further elaboration on the nature of the support documentations needed during the self-assessment process by the PFSO. This additional sub-section was incorporated to remove the difference in the coding or naming of the support documents which may varies with difference port facility. It is self-explanatory and do not need further guidance to the PFSO. The sub-section (d) is blank so as to provide space for the PFSO to insert remarks of any observations or additional action required as after audit follow-up action/s.

4. Conclusion

The conclusion is that the initial FCF Checklist is able to detect weaknesses in the effective implementation of the security measures and procedures covering for access control and restricted areas. Due to varying practices in these ports under the study, the checklist points caused some level of mis-interpretation by the PFSOs. Modifications are made to further facilitate the effectiveness of the checklist so as to allow the PFSOs to carry out the assessment unaided.

In conclusion, the SPMS system can be used to measure the completeness of the security threats for a port facility and its success depend mainly in the Port Facility Security Officer and his/her assessment team to take into consideration the totality of the port facility operation and not solely focuses on nature of threat alone but the associate entities that critical to the port operation. The FCF Checklist able to support the PFSO in carryout his/her security measures and procedures depend mainly on his/her ability to proactively determine it weaknesses as well as opportunities for improvement.

5. Recommendations

A structure security risk assessment is critical in the security associated environment as the external threat recognition through intelligent sources is practical not available to the PFSO in his/her daily challenges of determining possible threat that may be experienced by the port facility thus he/she can only look from internal perspective to determine the types of security which are effective for the entities it is protecting. Thus he/she need a very structure approaches and base mostly on the limited internal record that they possessed to determine the right proactive deterrence measures and procedures.

The PFSO is recommended to use the FCF Checklist format and replace the descriptors with the actual initiatives in the respective port facility security plan and carry out the self-assessment. This would be able to make easier as the PFSO understand better their security measures and procedures better.

References

[1] Bellamy L. J. et al. Storybuilder – A Tool for the Analysis of Accident Report. Reliability Engineering and System Safety. 92 (2007). Elsevier pp735-744. 2006..

[2] Bridges W & Clark T.. Key Issues with Implementing LOPA (Layer of Protection Analysis) – Perspective from One of the Originators of LOPA. 5th Global Congress on Process Safety, American Institute of Chemical Engineerings, . New York 6-7 June 2009. pp 5.

[3] Cambon J., Guarinori F. & Groenweg J. Towards A New Tool for Measuring Safety Management Systems Performance. Netherland: Centre for Safety Research, University of Leidan. 2008. pp 2-4

[4] Clifton A.. Accident Investigation Using EEFTA. Proceedings of the 18th International System Safety Conference 2000 Washington. 23 February 2000. pp 1-9.

[5] Eliana F. Risk Assessment and Risk Management under the Cartagena Protocol on Biosafety. ASPAC J.Mol.Bio.Biotechno. Vol. 17 (3). 2008. pp 97-98.

[6] FATF Secretariat**.** Money Laundering & Terrorist Financing Risk Assessment Strategies. Paris: FATF Secretariat, OECD. 2008, pp 5-6.

[7] Hurst S. & Lewis S.. Lessons Learned from Real World Application of Bow-Tie Method. United Kingdom: Risktec Solutions Limited. 2005, pp 1.

[8] International Labour Organization. Code of Practice on Security in Ports. IMO-ILO Tripartite Meeting of Experts on Security, Safety and Health in Ports. Geneva. 2003. pp 28 to 36.

[9] International Maritime Organization. International Ship & Port Facility Security Code and SOLAS Amendments 2002. London: IMO. 2002, pp 6-29.

[10] International Maritime Organization. Appendix 2, Interim Guidance on Voluntary Self- Assessment by SOLAS Contracting Governments and By Port Facilities. Maritime Safety Committee's Circular 1131. 14 December. London. 2004. pp 5 to 14.

[11] International Maritime Organization. Maritime Safety Committee Circular 1131. London: IMO Publication. 2004. pp 5-14.

[12] International Maritime Organization., SOLAS (Consolidated Edition 2004). London: The Bath Press. 2004.

[13] International Labour Organization. Code of Practice on Security in Ports. IMO-ILO Tripartite Meeting of Experts on Security, Safety and Health in Ports. 8 – 17 December. Geneva. 2003, pp28 to 36.

[14] International Maritime Organization.. Interim Guidance on Voluntary Self-Assessment by SOLAS Contracting Governments and by Port Facility – MSC/Circ. 1131. London: IMO Publication. 2004, pp 2.

[15] Jones S. Maritime Security: A Practical Guide. London: The Nautical Institute, 2006, pp 15.

[16] Kuo, C.. Managing Ship Safety. London: LLP Ltd. 1998, pp 6-12.

[17] Kuo C. Safety management and its Application. London: The Nautical Institute. 2007, pp 7.

[18] Reason J. et al.. TRIPOD, A principled basis for accident prevention. Manchester: University of Manchester. 1988, pp 23.

[19] Sklet S.. Methods for accident investigation. Norway: Norwegian University of Technology Publication. 2002, pp 72.

[20] Stranks J. A Manager's guide to Health & Safety at Work. London: Kogen Page Limited. 2001, pp 11.

[21] Turksema R. & Postma K. Tripod Beta and Performance Audit. , International Seminar on Performance Auditing. 23 - 25 May. Oslo. 2007, pp 1 – 12.