SAFETY CRITICAL MARITIME INFRASTRUCTURE SYSTEMS RESILIENCE: A CRITICAL REVIEW

(DOI No: 10.3940/rina.ijme.2016.a3.369)

A John, Petroleum Training Institute, Effurun, Nigeria, and **T C Nwaoha**, Federal University of Petroleum Resources, Effurun, Nigeria

SUMMARY

Safety Critical Maritime Infrastructure (SCMI) systems are vulnerable to diverse risks in their challenging field of operations due to their interactions and interdependence. In addition, the multiplicity of stakeholders in these systems and the complex operational scenarios are often associated with a high level of uncertainty because they usually operate in a dynamic environment in which the boundaries of safety are pushed, leading to the disruption of operations. Therefore, the safety of these systems is very important to ensuring resilience of their operations. This research is focus on the background analysis of SCMI systems. This includes operational processes of SCMI systems, security threats and estimates of economic damage to the system, resilience engineering literature relevant to maritime operations; regulatory overview including risk governance of the systems, lessons learnt from major accidents and a concluding remark is drawn.

1. INTRODUCTION

Safety Critical Maritime Infrastructure (SCMI) Systems which are defined as ports, waterways, vessels and their intermodal connections are faced with high operational uncertainties due to the dynamic interactions among their interrelated components. Analysing the systems in terms of their interdependences which include infrastructure systems' characteristics, operational relationships, environmental impacts, technical efficiency, failure types and states of operations provides insight into the complexity of the systems while enabling a collaborative modelling to take place (John et al. 2015 [15] and Mansouri et al. 2010 [19]).

When critical systems such as the SCMI systems do not have the robustness to recover in the face of disruption, they present themselves as attractive targets to terrorism related attacks. Given that approximately 90% of the world's trade is transported by sea (Riahi et al. 2012 [28]), the global economy is heavily dependent on the effective operation of these systems, resulting in a high level of systemic complexity; disruptions at any point within their operation could potentially result in catastrophic and long term consequences.

Building resilience in their operations requires creating capabilities and a sustained engagement from the stakeholders involved in maritime operations. In addition, academics and industrialists acknowledge that safety and security efforts that are aimed at reducing risks will always reach a point of diminishing returns. A more realistic way of optimising the system's defence capability is to incorporate resilience into its operations to adapt, cope and recover to a desired level of functionality. An emphasis on resilience provides a flexible and collaborative modelling of SCMI systems to address the diverse risks of disruption proactively, particularly as new hazards and threats are constantly evolving (John et al. 2014 [16]).

2. OPERATIONAL PROCESSES OF SCMI SYSTEMS

Modern seaports, which are integral component of SCMI systems, focus their operations on continuous handling of flows and efficient transport. A comprehensive analysis of the SCMI systems has revealed that they consist of ports, terminals, intermodal connects, navigable waterways and vessels as shown in Figure 1.

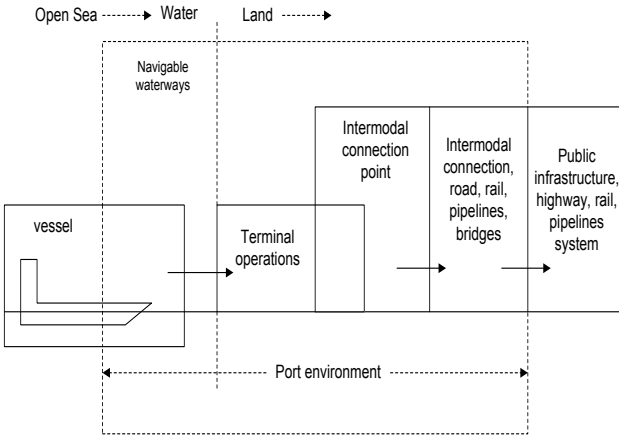

Figure 1: Sea-Land Interface of Maritime Transportation Systems [7] (Berle et al. 2011 [3])

Seaports are the business hub of terminals in the provision of critical infrastructure functions such as port roads and rails, and safety and security functions, which involve customs, investments, developments and marketing. Review of literature revealed that the critical way some elements of SCMI systems may fail when operating in an uncertain environment could be summed up as loss of capacity to supply, financial flows, transportations, communication, internal operations/capacity and human resources (Berle *et al*., 2011 [3]).

The analysis of disruption in complex sociotechnical systems' operations is essential to the investigation of resilience. Disruptions are situations or events of high uncertainty that obstruct or impede a system's normal operations by creating discontinuity, confusion, disorder or displacement of its functions in a dynamic environment (Madni, 2007 [18]). Experience has shown that these adverse situations can take a variety of forms such as operational contingencies, natural disasters, terrorism, political instability and financial meltdowns.

3. RESILIENCE ENGINEERING LITERATURES RELEVANT TO SCMI SYSTEMS

Over the last decade, safety analysts have acknowledged the limitations and weaknesses in the existing approaches to system safety and risk assessment processes. Resilience engineering (RE) was developed to provide insight into and improve the shortcomings of the existing approaches in the assessment of high reliability, complex and socio-technical systems such as the SCMI systems. Subsequently, significant effort has been made in trying to highlight the basic features of resilient systems and the development of robust, flexible and acceptable concepts, principles and methods that can serve as the basic building blocks and approaches to enriching the field of resilience and RE (Aven and Steen, 2010 [2]; Nameth *et al*., 2009 [20]; Hollnagel *et al*., 2008 [13; 12], 2006; and Woods, 2000 [35]).

Moreover, RE was suggested as a strategy to be used when systems are faced with complexity and uncertainty induced risks. It is seen as an alternative to the prescriptive (safety regime) risk management approaches which are based on calculating historical failure data probabilities of systems leading to disruptions (Renn, 2005 [27]).

Prescriptive safety regimes are considered inadequate due to the lack of structures and flexibilities to address the present day systems' risks. Hollnagel et al, (2006) [12] revealed that socio-technical systems have been developed rapidly over the last decades and the approaches to address their safety issues have not. This has revealed a clear need to develop advanced risk assessment approaches and safety management system, and RE has been proposed as a solution to address that need.

In practical applications of socio-technical systems operations such as SCMI system, adopting the resilience concept can help to improve awareness of dependencies and couplings in a realistic manner. Based on Johnsen and Veen, (2012) [17], the most important issues bordering on systems performance in modern organisations are complexity, uncertainty, pressure, continuity and cross-organisational factors.

Hollnagel et al, (2006) [12] defined resilience as the intrinsic ability of a system to adjust its functioning prior to or following changes and disturbances so that it can sustain operations even after a major mishap or in the face of continuous stress. Thus, the implication of this definition is that, for a system or an organisation to be resilient under uncertainty, it must have the following capabilities (Hollnagel, 2006 [13]):

- Anticipate risk events and opportunities.
- Respond to regular and irregular threats in a robust yet flexible manner.
- Monitoring capabilities.
- Learning from experience.

Since the processes for creating resilience in systems go beyond traditional risk assessment methods, it is important to note that a significant consideration in the design of resilient systems, either human-intensive or technological, is their capability to anticipate, respond, monitor and learn so as to be proactive. Based on the analysis of high reliability systems from Woods (2006b) [36] and Jackson (2010) [14], some key resilience attributes are identified and presented as follows:

- Redundancy.
- Capacity.
- Flexibility.
- Culture and risk.
- Inter-element collaboration.

Based on expert opinions, HAZard and OPerability studies (HAZOP) can be seen as a useful tool to explore resilience using key words of the resilient attributes during a workshop session to reveal uncertainties in complex system operations during group decision making for collaborative modelling and resilience improvement.

Since complex systems operations involve uncertainty, security incidents may be characterized by the exploitation of vulnerabilities in the system to achieve a certain degree of disruption. Resilience can be used as an innovative management strategy to achieve a high level of security in an uncertain and dynamic environment. Weick and Roberts (1993) [34] and Johnsen and Veen, (2012) [17] revealed that the benefits derived from strategic use and implementation of resilience in complex systems operations can be in the form of:

- Increased focus on proactivity, i.e. mindful of anticipating unexpected and uncertain events that may disrupt system processes in a systematic fashion.
- Ability of the system to adjust operation in the face of adverse operational scenarios in order to maintain its functionality.
- Ability to prepare for the unexpected in a pragmatic environment.

Mansouri et al. (2010) [19] revealed that integrating resilience into the design and operation of seaports can be potentially costly. However, investigations into their

operations have shown that losing the entire service delivery in the face of disruptions could lead to a long-term consequence. Omer et al. (2012) [21] proposes several schemes that help to improve resiliency by reducing the system's vulnerability and increasing its adaptive capacity. The paper further highlighted the need for implementing resiliency in systems so as to improve their ability to cope with disruptions hence minimising losses. Also, John et al. (2014) [16] proposed a collaborative modelling and strategic fuzzy decision support system for selecting appropriate resilience strategies for seaport operations. The decision support model allows for a collaborative modelling by multiple analysts in a group decision making process. To this end, decision makers are faced with a high degree of strategic decisions that involve uncertainty and major resource implications regarding investment in appropriate resilience strategies in order to bolster the performance effectiveness of their operations.

In light of the above, RE is about increasing the ability of organisations to make appropriate adjustments to the current system operations. These adjustments must be in such a way that organisations anticipate adverse events and act in a proactive manner. Acting in a proactive manner means that organisations should see safety and risk management as a critical capability for system resilience and recognise the combined contribution to it by the network of components and the multiplicity of stakeholders in the system (Dekker, 2005 [6]; Jackson, 2010 [14]).

4. SECURITY THREATS TO SCMI SYSTEMS' OPERATIONS

Maritime security threats encompass a wide range of attack scenarios due to the complex nature of their operations. Securing seaports against disruptions due to flaws within the system present an enormous task for security analysts. The threat of a cyber-attack is increasingly of growing relevance in maritime information, communication and control systems. Due to the criticality of complex processes being managed in maritime operations, a cyber-attack can compromise data confidentiality, integrity and availability. Based on the description of SCMI systems, there are three main potential system targets with cyber access. These are summarised as follows:

- Sea and land-based systems such as vessel tracking and information system (VTIS), automatic identification system (AIS) or long range identification and tracking system (LRIT).
- Container terminal operating systems (CTOS).
- Port electronic data interchange (EDI) system for domestic and international trade.

Attack scenarios to disrupt the smooth operation of SCMI systems can be identified during a HAZOP study session and presented as follows (Pate, *et al*., 2008 [25]; Parfomak and Frittelli, 2007 [26]; Greenberg, *et al*., 2006 [11]; Percival, 2005 [23]; Clarke, 2005 [5]; Rupert and Lauren, 2004 [29]; Garrick et al. 2004 [10]; Campbell and Gunaratna, 2003 [4]):

- Sink a large commercial cargo ship in a major shipping channel, thereby blocking traffic to and from the port.
- Seize control of a large commercial cargo ship and use it as a collision weapon for destroying a bridge or refinery located on the water front.
- Use land around the port's system to wreak havoc possibly on refineries located in industrial port areas and on other port facilities.
- Attack vessels or ports used to supply military operations overseas and interfere with those operations.
- An attack to disrupt the world oil trade and cause large scale environmental damage.
- An attack on or hijacking of a large ship containing volatile fuel (i.e. Liquefied Natural Gas (LNG) or Liquefied Petroleum Gas (LPG)) and detonation of it to cause in-port explosions.
- Use of commercial cargo containers to smuggle terrorists, nuclear, chemical or biological weapons, components thereof or other dangerous materials into the country.
- Directly target a cruise liner or passenger ferry to cause mass casualties by contaminating the ship's food supply, detonating an improvised explosive device (IED) or ramming the vessel with a fast-approach small attack craft.

4.1 ESTIMATES OF THE ECONOMIC DAMAGE TO SCMI SYSTEMS DUE TO SECURITY INCIDENTS

Over the last decade, the potential for a port closure due to severe disruptions of operations has been made clear several times by intelligence security experts as a result of the dynamic nature of operations taking place within a port's systems and its immediate environment. Research into the effects of port disruptions conducted by Talas and Menachof (2009) [30] and Greenberg *et al*. (2006) [11] has revealed that economic damage to ports can be both direct and indirect in nature. This may be in any form of:

- Damage to port infrastructure systems.
- Life and injury compensations.
- Repair and replacement of port infrastructure and other public property.
- Losses of cargo and destroyed private property.
- Increased insurance cost.
- Business disruptions through closure.
- Contamination of port infrastructure systems.
- Long term adjustment to transport systems.

- Lost revenue to the port's management and to the public purse.

Additionally, economic damage to ports can be a consequence of strike and industrial dispute between the workers and the ports management, as experienced in the West Coast port disruption (Yang *et al*., 2009 [37]).

4.2 AN OVERVIEW OF THE INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE (ISPS CODE)

The ISPS Code is a comprehensive and structured set of measures to enhance the security of port systems. It was developed in response to perceived threats to port facilities and ships by terrorism organisations in the wake of the 9/11 attacks. The Code establishes the maritime authority's ability to designate security levels and further develop guidelines and measures for protection against security threats. It is important to emphasize that the ISPS Code is implemented through Chapter XI-2's special measures of the International Convention for the Safety of Life at Sea (SOLAS) to enhance maritime security effectiveness.

The research conducted by Orbeck (2009) [22] and Bichou (2004) revealed that some of the requirements of the ISPS Code are compulsory (e.g. Part A, requiring adequate and sufficient operational, technical and physical measures in all relevant established port/terminal facilities), while the others are described more as recommendations (e.g. Part B, non-compulsory guidance undertaken to comply with the provisions of Chapter XI-2 and of Part A).

In an attempt to strengthen the ISPS Code within its territory, the European Union (EU) has developed a regulation to ensure strict compliance to Part B of the ISPS Code through EC 725/2004 (Anyanova, 2007 [1]; Dekker and Stevens, 2007 [7]). This has led to a significant improvement in the security system performance of EU port operations. Given the importance of the ISPS Code in strengthening maritime security, the objectives of the code can be summarised as follows (Orbeck, 2009 [22]):

- Prevention and detection of security flaws within an international framework.
- Enabling collection and exchange of security information.
- Providing a methodology for assessing security and ensuring that adequate measures are in place.
- Establishing roles and responsibilities of Port Facility Security Officers (PFSOs).

Additionally, the ISPS Code further requires PFSOs to control access to port facilities and monitor the activities of personnel and cargo within the port systems. A rational and in-depth analysis of the Code revealed the following approach (Orbeck, 2009 [22]):

- Formal procedures and description of processes for handling port equipment and facilities.
- Enabling specific competence and the use of common sense in identifying threats to operations.
- Use of qualitative and subjective risk assessment in the operational planning process of port/terminal systems to detect security loop holes.

In light of the above, it is worth mentioning that the ISPS Code has helped to strengthen the port security system through the designation of personnel on each ship, and in each port facility and shipping company for analysis and review of security levels to enhance the performance of port operations.

5. LESSONS FROM MAJOR ACCIDENTS IN THE MARITIME INDUSTRY

This section describes a selected set of accidents within the maritime industry where strength and weaknesses are expressed in terms of either the resilient attributes, system resilience and related concepts, or in terms of specific analytical processes that may have been neglected, such as design requirements, verification, reliability or interface management. Based on Jackson (2010) [14], modelling of past accident events and scenarios have the following advantages:

- Provides insights into how a disruption can be survived even if it is not avoidable.
- Provides an avenue for system definition.
- Provides the basis for risk analysis of the system in order to reveal its vulnerabilities.

In line with the modelling approach presented in Jackson (2010) [14], the following accidents are analysed and presented.

5.1 THE LOSS OF THE FLARE VESSEL

On the 16th January 1998, the Cyprus registered 29,222dwt bulk carrier *Flare* owned by ABTA shipping was on a scheduled route from Rotterdam, Netherlands, to Montreal, Quebec, when she split into two during rough weather conditions approximately 45 miles southwest of the French island of St. Pierre and Miquelon resulting in the loss of 21 crew members. The contributory factors that led to the loss of many lives are summarized as follows (Wang and Trbojevic, 2007 [32]):

- The sinking was due to inadequate ballast distribution of the vessel which made it vulnerable to pounding and slamming in the seaway (the Flare was without cargo when she sank).

- The owners failed to carry out structural repairs to the vessel: the owners could have completed critical repairs in Rotterdam before the *Flare's* fatal voyage, but instead attempted to carry them out at sea using riding crew with welding equipment.
- The vessel's emergency radio beacon and other distress equipment failed to activate, which caused the rescue operations to take several hours to locate the vessel, resulting in the loss of many seafarers in the freezing sea.
- The master and the majority of the crew were new to the vessel, having joined in Rotterdam. No proper training or life-boat drills took place and the crew were not familiar with abandon ship procedures. This resulted in the crew being unable to release the life-boats after the vessel broke into two.
- Lack of attention to safety: investigations into the accident highlight the owners' failure to maintain and operate a safe ship, which served to increase the death toll.
- Though multinational crewing of vessels is a long-established practice in maritime operations, the problem of a language barrier, which resulted in uncertainty, misunderstanding and lack of control, was evident in the *Flare* accident.

Based on the review of the investigation conducted by the Transport Safety Board (TSB) Canada, some resilience aspects of the *Flare* vessel's accident are presented in Table 1.

Table 1: Some Resilience Aspects of the Flare Vessel's Accident

Risk Management	Deficient
Decision making	Deficient
Cultural Factors	Deficient
Verification and Inspection	Deficient
Safety	Deficient
Regulatory Oversight	Deficient

5.2 HERALD OF FREE ENTERPRISE DISASTER, 1987

The Herald of Free Enterprise was operated by Townsend Car Ferries Ltd, a subsidiary of P&O Steam Navigation Company and her normal routes were Dover-Calais and Dover-Zeebrugge. As presented in Wang and Trbojevic (2007) [32], on the 6th March 1987, four minutes after leaving Zeebrugge harbour she capsized. As a result at least 150 passengers and 38 crew members lost their lives. The contributory factors that led to the accident are as follows:

- The location of the ship's centre of gravity, which was critical to the stability of the vessel, was faulty.
- Failure of management on board: there was lack of attention to safety as the bow door was left open and the speed of the vessel just before she capsized was very high.
- The basic ro-ro ferry design was questioned, in particular the single compartment standard for G-deck.
- There were no watertight bulkheads at all on this deck to prevent shipped water from spreading along the full length of the vessel.

Based on the analysis of the investigation of report by the UK Department of Transport (UKDT), some resilience aspects of the Herald of Free Enterprise (HFE) accident are presented in Table 2.

Table 2: Some Resilience Aspects of the Herald of Free Enterprise Accident

Risk Management	Deficient
Decision making	Deficient
Cultural Factors	Deficient
Safety	Deficient
Regulatory Oversight	Deficient

5.3 LOSS OF DERBYSHIRE, 1980

As presented in Wang and Trbojevic (2007) [32], during a typhoon in the Pacific on the 9th September 1980, the Derbyshire cargo ship of 169,044 dwt and length of 294 m, disappeared in mysterious circumstances when she was en route for Kawasaki, Japan. The tragedy cost 44 lives. The Derbyshire was not well prepared to take the rigours of the typhoon seas. It can be explained that the cargo holds (1, 2 and perhaps 3) in the bow flooded after the covers were washed away.

Based on the analysis of the investigation report by the UK Department of Transport (UKDT), some resilience aspects of the Derbyshire accident are presented in Table 3.

Table 3: Some Resilience Aspects of the Derbyshire Accident

Risk Management	Deficient
Design Tolerance	Deficient
Regulatory Oversight	Deficient
Safety	Deficient
Verification	Deficient

5.4 LOSS OF ESTONIA, 1994

The Estonia was carrying 989 people and the Bow visor locks broke and the visor fell off pulling open the inner bow ramp. Water flooded the main ro-ro deck and the vessel lost stability and sank in the northern Baltic Sea early hours of the 28th September, 1994. Only 137 passengers survived the accident. The principal ingredient that contributed to the accident are the inappropriate design and manufacture of the bow visor locks, the vessel not being seaworthy in terms of SOLAS requirement and crew making mistakes during the accident (Wang and Trbojevic, 2007 [32]).

Based on the analysis of the investigation report by the UK Department of Transport (UKDT), some resilience aspects of the Estonia accident are presented in Table 4.

Table 4: Some Resilience Aspects of the Estonia Accident

Risk Management	Deficient
Design Tolerance	Deficient
Defect detection and correction	Deficient
Decision Making	Deficient
Regulatory Oversight	Deficient

5.5 THE SEA EMPRESS ACCIDENT, 1996

On 15 February 1996, the tanker Sea Empress grounded off the middle Channel Rocks in the approaches to Milford Haven, eventually resulting in 2,500 tonne of crude oil escaping and a further 69,000 tonne lost during the salvage operation. The major contributing factor was the inability of the pilot to take appropriate and effective action to keep the vessel in the deepest part of the channel (Wang and Trbojevic, 2007 [32]).

Based on the analysis of the investigation report by the UK Department of Transport (UKDT), some resilience aspects of the Sea Empress accident are presented in Table 5.

Table 5: Some Resilience Aspects of the Sea Empress Accident

Management Oversight	Deficient
Expertise	Deficient
Risk Management	Deficient
Decision Making	Deficient
Regulatory Oversight	Deficient

5.6 LOSS OF PRESTIGE, 2002

The Prestige carrying 77,000 tonne of heavy oil broke into two and sank about 133 nautical miles off the coast of Spain on the 19th November 2002, seriously polluting the Spanish coast.

The ship lost its propulsion in the heavy seas near Spain. Crews were evacuated, salvos towed ship out to sea. The major contributing factor to the accident was the ageing of the ship with single bottom hull (Wang and Trbojevic, 2007 [32]). Based on the analysis of the investigation report by the UK Department of Transport (UKDT), some resilience aspects of the Derbyshire accident are presented in Table 6.

Table 6: Some Resilience Aspects of the Prestige Accident

Design	Deficient
Regulatory Oversight	Deficient
Risk Management	Deficient
Management Oversight	Deficient

There are slight changes in the order of factors in the left hand column of Tables 1-6. It is important to note that no priority is attached to these changes. The change is the result of different accidents scenarios analysed and the prevailing factors surrounding their occurrence.

6. RISK GOVERNANCE OF SCMI SYSTEMS

Governance refers to the review and oversight of all activities in any phase of a system's life cycle, which may be in the form of peer reviews, design reviews and independent reviews, especially during the development phase of a technological system (Jackson, 2010 [14]). Most safety researchers and analysts agree that risk governance in critical infrastructure systems is a key aspect of systems resilience.

Risk governance in a broad context, as defined by International Risk Governance Council (IRGC) (2005), is the identification, assessment, management and communication of risks. In a similar manner, the International Maritime Organization (IMO) has adopted the definition of the Formal Safety Assessment (FSA) as a process of identifying hazards, evaluating risks, developing risk control measures, cost-benefit assessment, and making decisions and taking actions to manage these risks (Wang and Trbojevic, 2007 [32]). Based on the IMO's definition, the basic elements of FSA can be presented in Figure 2.

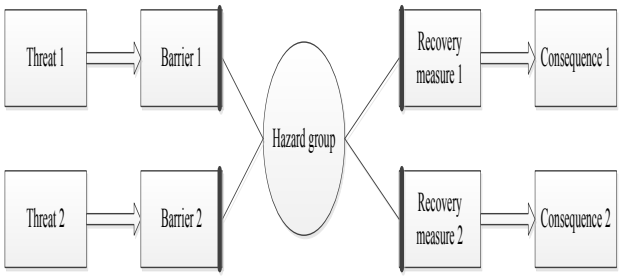

Figure 2: Risk Assessment Bow-tie (Source: Wang and Trbojevic (2007) [32])

Figure 2 shows the bow-tie diagram. The starting point on the left hand side is a hazard which is defined as a situation or condition with the potential to cause harm. The centre part (hazard group) is the top event, which is the release of the hazard. Based on Wang and Trbojevic (2007) [32], these conditions or situations can be technical, organisational or human factor related and can be in any of the following:

- Hazardous elements such as hydrocarbon under pressure, explosives etc.
- Initiating event causing the top event to occur.
- Threat and target, personnel or a system that is vulnerable to an attack.

A hazard can be triggered by one or several threats (e.g. mal-function, excess pressure, corrosion, design fault, etc.) which if not checked would lead to an initiating event or loss of control situation (as shown by a circle perimeter in Figure 2). To prevent this, resiliency measures or barriers are put in place. The left hand side of the bow-tie is also called the causation part and requires causation analysis in the FSA or risk governance process (hazard analysis, failure mode and effect analysis, fault tree analysis etc.).

A barrier system based on Figure 2 is to reduce the probability of release of hazards with the aim of buffering the system from major external and internal disruptions, thereby absorbing shocks and reducing system uncertainty. These barriers may include monitoring systems enabled with sensors, connections, feedback loops, action capabilities, etc. The same is true about the recovery measures or resiliency measures at the right hand side, which can include actions in the form of procedures' inspections, and drills that can be standardized as various policies based on the evaluation of the system using event tree analysis, consequence analysis and so on (Mansouri *et al*., 2010 [19]; Wang and Trbojevic, 2007 [32]).

The right hand side of the bow-tie depicts the escalation or outcome analysis which could take place if all barriers are breached and the hazard is released. This event could then escalate to different outcomes, each of which would have specific consequences such as loss of life, fire/explosion, etc. In light of the above, a risk management system can be envisaged as a critical and key aspect for improving resilience in complex systems operations by maintaining barriers and recovery measures.

6.1 APPROACHES TO MEASURING RESILIENCE

Measuring resilience of SCMI systems is a very challenging task. Evidence from their operations reveals that the only way to measure and analyse their resilience is to measure the potential for attaining or achieving resilience in systems (Woods, 2006a [36]). Based on Wang and Trbojevic (2007) [32], human-related factors are responsible for about 80% of maritime accidents. This assertion was also corroborated by Flin (2007) [8], who revealed that technical related factors are responsible for 20-30%. It was further revealed that, even among the human factors, about 80% can be attributed to organisational and cultural factors and about 20% are operator factors.

Jackson (2010) [14] revealed that most failures occurred as a result of human intervention or negligence at various stages in the life cycle of the system's operation, which includes production, development, maintenance and operation. However, in all cases, humans were rarely observed to be the root causes but rather were mere factors in larger systemic causes of disruptions. Experience has shown that in order to be resilient, a system needs to be reliable in its operation.

6.2 RISK ASSESSMENT OF SCMI SYSTEMS

Hazard identification is the first process of a risk assessment methodology. It has been part of decision making in analysing and characterising the extent of the potential threat and the risk associated with an infrastructure system. Garrick *et al*. (2004) [10] suggest that formal application of risk assessment to critical infrastructure began in the late 1900s and many risk analysis methods have been developed and put into practice to support decision making processes. The research revealed that these methods have had a major impact on policy making in areas such as environmental regulations, public health, safety regulations, and the performance of technological systems, especially those involving hazardous materials. However, the breakthrough in probabilistic risk assessment (PRA) of technological systems came in 1975 with the publication of the reactor safety study by the US Atomic Energy Commission (USAEC).

The most widely used causal modelling techniques in risk analysis are fault tree analysis (FTA) and event tree analysis (ETA). A number of direct causes of disruption (e.g. loss of containment (LOC)) of a system can be analysed and modelled as a joint event consisting of an initiating event and failure of one or more safety functions. Experience has shown that detailed models for these types of direct causes can be built using FTA and ETA, which provide system insights resulting in computation of uncertainty/probability indices (Papazoglou *et al*., 2003 [24]).

Normally, the computation of these indices can be based on generic data or more specific data for the relevant system being studied in a systematic manner. Wang (1997) [31] revealed that risk analysis can be divided into two broad categories of quantitative and qualitative nature depending on data availability. However, in situations of unavailability or lack of data, expert opinions are required to implement such risk analysis (Wang *et al*., 1995 [33]).

As discussed earlier and in all types of systems, there are different tools for identifying hazard. These hazards and their effect need to be evaluated prior to systems construction and operations. This makes hazard evaluation phase a key step in risk assessment for resilience improvement of a system. Based on the type of application, there are several hazard identification techniques; these include (Jones and Israni, 2012 [9]):

- What if /Checklist Analysis
- Hazard and Operability Studies (HAZOP)

- Failure Mode Effect and Criticality Analysis (FMECA)
- Fault Tree Analysis (FTA)
- Event Tree Analysis (ETA)
- Cause-Consequence Analysis and Bow-tie Analysis

Each of these methods provides insight on the hazard associated with a particular system. The hazard evaluation provides a sense of direction toward the risk assessment process. Based on the risk assessment outcome, decisions may be undertaken on the viability of a project design, with respect to the harm on human life.

7. CONCLUSION

This paper has presented a general overview of SCMI systems operations, some aspects of system resilience and lessons learnt from major accidents in maritime industry to serve as the basic building block for the development of frameworks and methodology to be used in enhancing safety, security and resilience of SCMIS. It has also been established from research and analysis of literature that systems resilience is dependent on factors encompassing technical, operational, security, organisational and external issues. Thus, this necessitates the development of a generic model that can be used to model disruption scenarios in a straightforward manner to enhance the resilience of maritime systems.

The study has highlighted factors such as poor communication, design and decision making and how they have contributed to accidents within the maritime industry. The literature review has further revealed that researchers and industrialists alike agree in all respects that the catastrophic accidents that have occurred were preceded by deficiencies and near misses that should have been used as warning signs to develop capability for resilience, but were neglected. The root cause of most accidents or disruptions was the lack of resilience. Hence, building resilience into these systems is a key to assuring safety, security and efficiency of operations.

8. ACKNOWLEDGEMENTS

This research was partially supported by Liverpool Logistics Offshore Marine Research Institute (LOOM) and Petroleum Technology Development Technology (PTDF) Abuja-Nigeria.

9. REFERENCES

1. ANYANOVA, E. 2007, "The European Commission on Enhancing Ship and Port Facility Security', *International Journal of Commercial Law and Technology*, Vol. 2, Issue 1, pp. 1-7.
2. AVEN, T. and STEEN, R. 2010, "A Risk Perspective Suitable for Resilience Engineering" *Journal of Safety Science,* Vol. 49, pp. 292-297.
3. BERLE, O. and RICE, J.B. 2011, "Formal Vulnerability Assessment of a Maritime Transportation Systems", *Reliability Engineering and System Safety*, Vol. 96, pp. 696-705.
4. CAMPBELL, T. and GUNARATNA R. 2003, "Maritime Terrorism, Piracy and Crime", in Rohan Gunaratna, ed., *Terrorism in the Asia-Pacific: Threat and Response*. Singapore: Eastern Universities Press, pp. 70-88.
5. CLARKE, R.A. 2005, "Liquefied Natural Gas Facilities in Urban Areas", A Security Risk Management Analysis for Attorney General. Patrick Lynch, Rhode Island.
6. DEKKER, S. 2005, "Ten Questions about Human Error: A new View of Human Factors and System Safety". Mahwah, NJ: Lawrence Erlbaum Associates.
7. DEKKER, S. and STEVENS, H. 2007, "Maritime Security in the European Union, Empirical Findings and Financial Implications for Port Facilities", *Maritime Policy and Management*, Vol. 34, No. 5, pp. 485-499.
8. FLIN, R. 2007, "Managerial Decision Making: Counterbalancing Risks between Production and Safety", A Presentation at the Industrial Psychology Research Centre, University of Aberdeen, Scotland.
9. JONES, F.V. and ISRANI, K. 2012, "Environmental Risk Assessment Utilising Bow-Tie Methodology" Society for Petroleum Engineers SPE/APPEA/International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production, Perth, Australia, September 11-13, 2012.
10. GARRICK, B.J., HALL, J.E., KILGER, M., MCDONALD, J.C., O'TOOLE, T., PROBST, P.S., PARKER, E.R., ROSENTHAL, R., TRIVELPIECE, A. W., ARSDALE, L.A.V. and ZEBROSKI, E.L. 2004, "Confronting the Risks of Terrorism: Making the Right Decisions", *Reliability Engineering and System Safety*, Vol. 86, pp. 129-176.
11. GREENBERG, M., CHALK, P., WILLIS, H., KHILKO, I. and ORTIZ, D. 2006, "Maritime Terrorism: Risk and Liability", RAND Corporation Centre for Terrorism and Risk Management Policy, Pittsburgh, USA.
12. HOLLNAGEL, E., WOODS, D.D. and LEVESON, N. 2006, "Resilience Engineering Concepts and Precepts", *Ashgate Publication*, ISBN: 978-0-7546-4641-9.
13. HOLLNAGEL, E., NEMETH, P.C. and DEKKER, S. 2008, "Remaining Sensitive to the Possibility of Failure in Resilience Engineering Perspectives", Vol. 1. Ashgate *Publication*,

Resilience Engineering 2006, ISBN: 978-0-7546-4641-9.

14. JACKSON, S. 2010, "Architecting Resilient Systems, Accident Avoidance and Survival and Recovery from Disruptions", Wiley Series in Systems Engineering and Management, ISBN: 978-0-470-40503-1.
15. JOHN A, RIAHI R, PARASKEVADAKIS D, BURY A, YANG Z, and WANG J. 2015, "A New Approach for Evaluating the Disruption Risk of a Seaport System", Safety and Reliability: Methodology and Application-*Nowakowski et al. (eds),* Tailor and Francis Group, London, ISBN 978-1-138-02681-0.
16. JOHN A, PARASKEVADAKIS D, BURY A, YANG Z, RIAHI R and WANG J. 2014, "An integrated fuzzy risk assessment for seaport operation", *Safety Science*, Vol. 68, pp. 180-194.
17. JOHNSEN, S.O. and VEEN, M. 2012, "Risk Assessment and Improvement of Resilience of Critical Communication Infrastructure" Advances in Safety, Reliability and Risk Management. Taylor & and Frances Group, London, ISBN 978-0-415-68379-1.
18. MADNI, A. M., 2007, "Designing for Resilience", *ISTI Lecture Notes on Advanced Topics in Systems Engineering*.
19. MANSOURI, M., NILCHIANI, R. and MOSTASHARI, A. 2010, "A Policy Making Framework for Resilient Port Infrastructure Systems", *Marine Policy*, Vol. 34, pp. 1125-1134.
20. NEMETH, P.C., HOLLNAGEL, E. and DEKKER, S. 2009, "Preparation and Restoration of Resilience Engineering Perspectives", *Ashgate Publication, Vol. 2, 2009*. ISBN: 978-0-7546-7520-4.
21. OMER, M., MOSTASHARI, A., NILCHIANI, R. and MANSOURI, M. 2012, "A Framework for Assessing Resiliency of Maritime Transportation System", *Journal of Maritime Policy and Management*, Vol. 1, pp. 1–19.
22. ORBECK, E. 2009, "Implementation of the ISPS Code in Norwegian Ports and Harbour Protection through Data Fusion Technologies", Springer Science + Business Media B.V.
23. PERCIVAL, B. 2005, "Indonesia and the United States: Shared Interests in Maritime Security", Washington, DC: United States-Indonesia Society, June.
24. PAPAZOGLOU, I.A., BELLAMY, L.J., HALE, A.R., ANEZIRIS, O.N., POST, J.G. and OH, J.I.H. 2003, "IRisk: Development of an Integrated Technical and Management Risk Methodology for Chemical Installations", *Journal of Loss Prevention in the Process Industries*, Vol. 16, pp. 575 - 591.
25. PATE, A., TAYLOR, B. and KUBU, B. 2008, "Protecting America's Ports: Promising Practices", Vol. 221075, No. 2003-IJ-CX-1021. [Online] *www.ncjrs.gov/pdffiles1/nij/grants/221075.pdf* (Accessed: 16th April, 2014).
26. PARFORMAK, P.W. and FRITTELLI, J. 2007, "Maritime Security: Potential Terrorist Attacks and Protection Priorities", Congressional Report Service.
27. RENN, O. 2005, "Risk Governance - Towards an Integrative Approach" International Risk Governance Council, White Paper No.1.
28. RIAHI, R., BONSALL, S., JENKINSON, I and WANG, J. 2012, "A Seafarer's Reliability Assessment Incorporating Subjective Judgements", A Proceeding of the Institution of Mechanical Engineers, Part M: *Journal of Engineering for the Maritime Environment*.
29. RUPERT, H.B. and LAUREN, Z. 2004, "Drawing the Line between Piracy and Maritime Terrorism", *Jane's Intelligence Review*, September, pp. 3.
30. TALAS, R. and MENACHOF, D.A. 2009, "The Efficient Trade-Off between Security and Cost for Seaports: A Conceptual Model", *International Journal of Risk Assessment and Management*, Vol. 13, No. 1, pp. 46-59.
31. WANG, J. 1997a, "A Subjective Methodology for Safety Analysis of Safety Requirements Specifications", *IEEE Transactions on Fuzzy Systems*, Vol. 5, No. 3, pp. 418-430.
32. WANG, J. and TRBOJEVIC, V.M. 2007, "Design for Safety of Large Marine and Offshore Engineering Products", *Institute of Marine Engineering, Science and Technology* (IMarEST), London, UK, ISBN: 1-902536-58-4.
33. WANG, J. YANG, J.B. and SEN P. 1995, "Safety Analysis and Synthesis Using Fuzzy Set Modelling And Evidential Reasoning", *Reliability Engineering & System Safety*, Vol. 47, No. 3, pp. 103-118.
34. WEICK, K.E. and ROBERTS, K.H. 1993, "Collective Mind in Organizations: Heedful Interrelating on Flight Decks", *Administrative Science Quarterly*. Vol. 38, No. 3, pp. 357-38.
35. Woods, D.D. 2000, "Lessons From Beyond Human Error, Designing for Resilience in the Face of Change and Surprises", *Design for Safety Workshop*, NASA Ames Research Centre.
36. WOODS, D. 2006a, "Resilience Engineering Precepts, In Hollnagel, E., Woods, D. & Leveson, N. (Eds). Resilience Engineering: Concepts and Precepts. Aldershot, UK: Ashgate.
37. YANG, Z.L., WANG, J., BONSALL, S. and FANG Q.G. 2009, "Use of Fuzzy Evidential Reasoning in Maritime Security Assessment", *Risk Analysis*, Vol. 29, No. 1, pp. 95-120.

