The Next Step: A Fully Integrated Global Multi-Modal Security and Safety Management System

R. W. Fletcher, P. Eng., M. Sc., PMP, PCIP

Keywords: system, security, safety, management, global, risk, hazard, threat, integrated

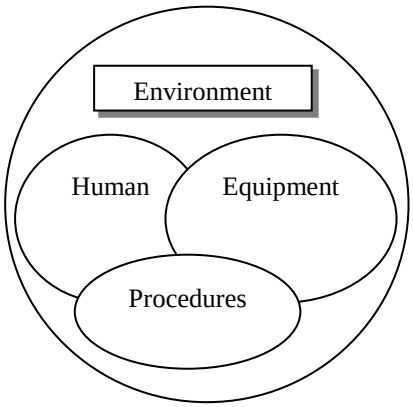
Abstract

System safety professionals must consider all aspects of a nation's and the world's critical resources and seek to protect against harm or loss. Critical Infrastructure Protection (CIP) involves both security and safety aspects of systems. Critical infrastructure has been defined as infrastructure so vital that its incapacity or destruction would have a debilitating effect on national security, the economy, public health and safety. Critical Infrastructure consists of the physical and information technology facilities, networks, services and assets essential to the health, safety, security and economic well-being of a population and the effective functioning of government. The private sector owns over 80 per cent of the critical infrastructure; however, the government primarily takes the lead to inform industry of the threats and hazards that it faces. The CIP Risk Management model seeks to establish measures and controls to safeguard assets. It assesses the phase before and after a catastrophe in terms of management action and reaction. The assets include personnel, material, facilities, information and activities essential to the critical infrastructure of a nation. This paper will show how this model will become the next step in creating a fully integrated global multi-modal security and safety Management System.

Introduction

This paper seeks to build on the concept of a system and to show how analysis techniques have moved from the simple which was adequate for small systems (e.g. a basic assembly line for manufacturing clothing), to very complex systems with many interfaces and interactions and with equipment controlled from great distances moving at high speed (e.g. military drones, or spacecraft landing on Mars). A system is a set of interacting or interdependent components forming an integrated whole. A simple diagram of a system is shown in Figure 1 below.

Figure 1: System with its Basic Elements



Dr. Ian Sommerville states; "A system is a collection of interrelated components that work together to achieve some objective. [1]

The complex relationships between components in a system mean that the system is more than simply the sum of the parts. It has properties that are properties of the whole. They cannot be attributed to any specific part. These are called emergent properties. … ". Based on this simple mental model, more complex mental models can be developed showing how systems' thinking has expanded to enable hazard and threat analyses of increasingly more complex systems. Hazard analysis has introduced new and more complex

techniques as technology has become more complex. Since the industrial revolution, the pace of work and the complexity of tasks has become more intense. Systems have now reached the level where they are so complex that they are no longer intellectually manageable. More complex mental models are required to describe how systems thinking needs to be done to help think about the system more appropriately to conduct Threat and Hazard Identification and Risk Assessment (THIRA).

Safety in the workplace received its initial impetus from the number of workers that died in various duties and from large accidents from fire and similar disasters. In 1911 a fire in a clothing factory in New York resulted in the formation of the American Society of Safety Engineers (ASSE). Laws were passed to make the employer more responsible and accountable for safety in the workplace. Prior to 1911, the law did not protect the worker. It was understood that if a worker willingly accepted a job that was inherently hazardous then the employer shared no responsibility for death or injury on the job.

In 1931 Heinrich created a pyramid that showed the ratio for every one death to the number of injuries and near misses. Recently evidence has shown that this ratio is not effective in that disasters occur without any relationship to the number of deaths or injuries. The reason for this is that the ratio is based on simply counting the deaths and injuries as an outcome without consideration of what is happening in the organization from a total systems point of view. Technology has continued to advance driven primarily by World War II. In the 1950's, aviation, nuclear power plants, oil and gas, and other complex safety critical industries introduced new analysis techniques to cope with complexity. Potential losses could no longer be identified and mitigated based on reacting to failures. Many of the losses were due to unreliable equipment. The 1950s and 1960s saw a dramatic improvement in the quality and reliability of equipment or the *Technical Factors*. As complexity in operations continued to grow, it became evident that the "fly-fix-fly" approach was not sufficient. In the 1970s and 1980s, emphasis was placed on *Human Factors*. For twenty years great effort was concentrated on how the human could be most effectively and safely integrated into the operation of the equipment. Ergonomics, fatigue, psychological factors and other aspects were the focus of system development. Overlapping this era and on into the 1990s, the focus was placed on *Organizational Factors*. It became clear when designing new systems that the equipment, the human and the complete organizational decision making needed to be considered in the context of ensuring safety of operations.

Since the 1990s and into the 2000s, it became evident that the old ways of performing hazard analysis based on cause and effect chains could not capture the complexity of the complete system. Even though in-depth hazard analysis was used in designing and operating complex systems, accidents still continued to happen. The shuttle disasters Challenger and Columbia, the nuclear disasters Chernobyl, Three Mile Island and Fukushima, continued aircraft accidents, many preventable deaths in hospitals, high speed train crashes in China, continued automobile accidents, multiple mining accidents, and other types of accidents have led engineers to suggest that a new way of analyzing systems is required. Instead of decomposing a system into the multiple cause and effect chains related to a threat or hazard, it is more effective to consider the system as a whole and see safety as an emergent property that must be maintained. A simple analogy is the way a thermometer is set to maintain a set temperature. It should be possible to consider a system from a control theory perspective and maintain safety as a property of the system during its operation.

In the same way as safety is an emergent property of complex systems, security is also an emergent property. This became undeniably clear on 11 September 2001 when terrorists attacked the World Trade Center in New York City. It is interesting to note that safety and security are included together in the Wikipedia article regarding the new One World Trade Center. [2] "… s*afety features were included in the building's design, in order to better prepare it for a major accident or terrorist attack. ... In addition to optimum safety design, new security measures will also be implemented."* Since the 9/11 event, safety and security have merged in terms of their association in the design and operation of complex systems.

The ICAO Safety Management System model which uses the traditional "cause and effect chain of events" thinking throughout the whole organization is not sufficient to capture all threats and hazards in a complex system design and its operations. It is not possible given the system complexity and circumstances that could initiate an accident for sufficient hazards and threats to be identified and mitigated. The ICAO SMS mental model is based on the Domino and Swiss Cheese models which are limited by linear and cause and

effect chain of events' thinking. These techniques are effective for system designs that have less complex system designs built from the 1950s until approximately 2000.

This new approach to system safety analysis comes from a mental model that uses control theory. It takes the emergent property of safety and analyzes how, when, where, and why safety may be compromised. This mental model can be extended to include security threats. Safety and security have merged with similar characteristics and both properties can be analysed in a similar way. These two emergent properties are different in that security threats are the result of intentional malicious behaviour; whereas, safety hazards are the result of system losses in an environment of well-intentioned behaviour.

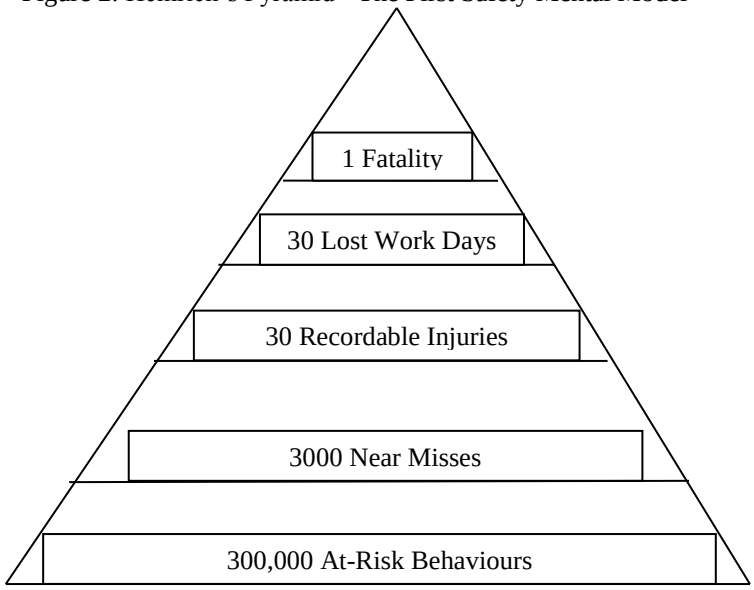
Development in Analysis Approaches

In the past one hundred years, mental models for accident prevention have progressed from counting number of deaths and injuries and applying lessons learned to using control theory and global critical infrastructure analysis. Initiatives to reduce accidents were first motivated by occupational safety and health specialists. As systems became more complex and the need to focus on technical, human, and organizational factors developed, system safety and security analysts became more involved.

A fully Integrated Global Multi-modal Security and Safety management system

The mental model representing the next step, as suggested by the title of this paper must have the perspective of a *fully integrated global multi-modal security and safety* management system. Fully integrated in that all functional aspects of operations, maintenance and engineering of the system must be assessed as one system. Global, in that mental model must be applicable throughout the world. Multi-modal meaning that it applies to all modes of operations, including air, land, sea and rail and to all industries; nuclear, medical, oil and gas, aerospace and aviation, etc.. The mental model must consider both system safety hazards and security threats. No part of the overall system that could lead to loss of life should be excluded.

Figure 2: Heinrich's Pyramid - The First Safety Mental Model



This approach has been practiced by occupational safety, health and environmental specialists for the past one hundred years. Great contributions to loss prevention in terms of preventing accidents, saving lives and reducing damage to expensive equipment have been achieved from using this mindset. However, this mental model does not involve "systems thinking" and is not able to proactively identify deep systemic problems that could lead to losses. It is a reactive approach that deals mostly with the unsatisfactory

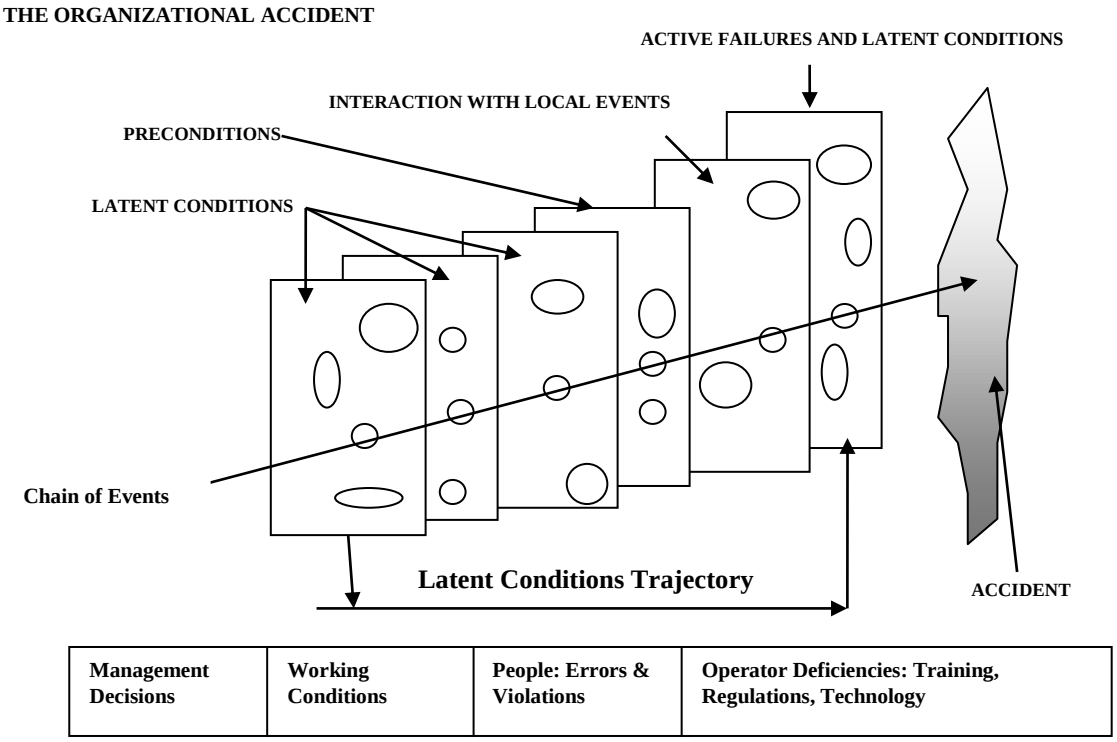
conditions of workplaces. It is a fly-fix-fly approach that gathers statistics and lessons-learned, but it does not identify mitigation for the large complex systems that cause large scale disasters.

Mental Models: Heinrich, Reason, ICAO SMS

Heinrich's depiction of the Domino Model in 1931 helped analysts see that conditions in work places are caused by issues pertaining to more than just the worker himself. This is the first attempt to develop a scientific mental model to describe accident causation.

Reason extended the idea graphically by suggesting that the size and placement of the holes are random and change over time; however, the essence of the mental model remained unchanged. It is a linear sequential chain of events' model. The model indicates that causal factors stem from various sources from the operator through to management.

Figure 3: Dr. James Reason's Concept of Accident Causation



Dr. James Reason's book in the 1990s regarding "organizational accident causation" indicated that any system safety mental model must include all aspects of the hazards within the whole organization responsible for design and operation of a system.

ICAO's SMS Mental Model uses the thinking based on Reason's Swiss Cheese model; however, in addition to looking throughout an organization for accident causation, the SMS approach emphasizes the requirement to be reactive, proactive, and predictive. The most significant contribution to system safety management with the ICAO's use of Reason's Swiss Cheese approach is the way that it is applied. By requiring the safety analyst to focus attention proactively and predictively on what could go wrong, more hazards, issues and concerns can be identified and mitigated prior to operating the system. The analyst is required to consider; What could go wrong?, How severe would it be?, and How likely is it to happen? in situations that only exist prior to operations. Previously, safety was considered retroactively after the accident and hazards and lessons learned were identified during an incident or accident investigation.

The "fly-fix-fly" approach of the 50's was enhanced with improvements in equipment during the *Technical Factors Era* in the 70's, improvements in procedures and equipment from the *Human Factors Era* in the 80's, and most recently improvements from recognizing that people operating complex systems are part of a team during the *Organizational Factors Era* in the 90's. The SMS approach expanded the considerations to include the whole organization and included proactive and predictive perspectives.

Security Threats

After 9/11, security threats became a part of the proactive and predictive scenarios under consideration. The ICAO SMS Mental model with reactive, proactive, and predictive aspects is well suited to include security threats; however, as first conceived, it was intended primarily to help identify and mitigate internal systemic hazards. The greatest improvement in accident prevention introduced by the ICAO SMS Model at this stage in safety management development is the introduction of proactive and predictive thinking. ICAO's Safety Management Manual (SMM), Doc 9859 AN/474 states; "The reactive method responds to events that have already happened, such as incidents and accidents. The proactive method identifies safety risks through the analyses of the organization's activities. The predictive method captures system performance as it happens in real-time normal operations to identify potential future problems. Proactive thinking is based on the notion that system failures can be minimized by identifying safety risks within the system before it fails, and taking the necessary actions to mitigate such safety risks. Mandatory and voluntary reporting systems, safety audits and safety surveys are examples of proactive actions. Predictive thinking is based on the notion that safety management is best accomplished by trying to find trouble, not just waiting for it to show up. Predictive safety data capture systems aggressively seek safety information that may be indicative of emerging safety risks from a variety of sources." An example of predictive analytics is the way the Target enterprise is able to capture the types of purchases that people make and determine if a women is pregnant. Knowing that pregnancy precedes a whole series of standard type purchases, Target will send coupons to the person to encourage the family to purchase all the items from the Target stores. Mature safety management systems must have integrated reactive, proactive and predictive safety data capture systems with mitigation strategies and methods.

Mental Model: STAMP/STPA Based on Control Theory with Safety as an Emergent Property of a System

The STAMP/STPA approach which goes beyond cause and effect chain of event sequences was invented by Dr. Nancy G. Leveson at the Massachusetts Institute of Technology in Boston, USA. It is fully explained in her book entitled; "Engineering a Safer World", 2011. The author of this paper attended a three day workshop at MIT on this mental model, 17-19 April 2012. It was attended by 250 people from 19 different countries. On the first day, Dr. Leveson explained the details of the STAMP/STPA mental model. On the second and third days; there were presentations by people who had applied this analysis technique to a particular safety critical system; for example, automobiles, medical devices, dams, etc. ... Dr. Leveson stated that systems have reached a level of complexity where they are no longer intellectually manageable and certainly too complex for a hierarchical proportional pyramid, the Domino Model, or Reason's Swiss Cheese Model to depict a method of analysis.

Mental Model: Rasmussen/ Svedung

Dr. Leveson refers to the Rasmussen / Svedung model for risk management in her book "Engineering A Safer World", 2011, [6]. This mental model addresses the System Design and Analysis phase as well as the System Operation phase. This mental model has similar elements of the ICAO mental model in that it considers the complete organization and combinations of organizations that contribute to an accident. In addition, when this model is combined with the control theory approach, it is very effective in addressing all sources of potential hazards.

The traditional mental models and techniques have served the system safety community well for many years. It is important to have a very strong argument to recommend that we leave old techniques behind and move to a new way of thinking and analyzing. We were asked to consider as in the book, a comparison of old assumptions and new assumptions.

Figure 4: Dr. Leveson Challenges Several Assumptions [6]

Old Assumptions	New Assumptions
• Safety is increased by increasing system or component reliability. If components or systems do not fail, then accidents will not occur	• High reliability is neither necessary nor sufficient for safety
• Accidents are caused by chains of directly related events. We can understand accidents and assess risk by looking at the chain of events leading to the loss	• Accidents are complex processes involving the entire socio-technical system. Traditional event-chain models cannot describe this process adequately
• Probabilistic risk analysis based on event chains is the best way to assess and communicate safety and risk information	• Risk and safety may be best understood and communicated in ways other than probabilistic risk analysis
• Most accidents are caused by operator error. Rewarding safe behaviour and punishing unsafe behaviour will eliminate or reduce accidents significantly	• Operator behaviour is a product of the environment in which it occurs. To reduce operator "error" we must change the environment in which the operator works
• Highly reliable software is safe	• Highly reliable software is not necessarily safe. Increasing software reliability or reducing implementation errors will have little impact on safety
• Major accidents occur from the chance simultaneous occurrence of random events	• Systems will tend to migrate toward states of higher risk. Such migration is predictable and can be prevented by appropriate system design or detected during operations using leading indicators of increasing risk
• Assigning blame is necessary to learn from and prevent accidents or incidents	• Blame is the enemy of safety. Focus should be on understanding how the system behaviour as a whole contributed to the loss and not on who or what to blame for it

System Safety and Security as an Emergent Properties of a System

In the same way we consider safety as an attribute of a system and an emergent property, we can consider security as an attribute and an emergent property of a system. The consequences resulting from the failure of a system to meet its operational objectives due to a security breach are similar to the consequences resulting from the outcome of a system safety hazard in that all system operations could become shut down. The question is how to build into the analysis of a system the thinking process that will analyze both hazards and threats in a similar manner such that the results can be presented in a report with consistency in process and terminology.

Leveson states [5]; "Safety and security are closely related and their similarities can be used to the advantage of both in terms of borrowing techniques from each to deal with the other. Both qualities deal with threats or risks – one with threats to life and property and the other with threats to privacy or national security. Both involve negative requirements or constraints that may conflict with some important system goals. Both involve protection against losses, although the types of losses involved may be different. Both involve global system properties that are difficult to deal with outside the system context. Both involve requirements that are considered of supreme importance (in relation to other requirements) in deciding whether the system can and should be used. Particularly high levels of assurance may be needed, and testing alone is insufficient to establish those levels. In fact, a higher level of assurance that a system is safe and secure may be needed than that the system performs its intended function. Finally, both qualities involve aspects of a system that are regulated by government agencies and license bureaus where approval is based on factors other than whether the system does anything useful or is economically profitable. These shared characteristics lead to other similarities. Both may benefit from using technologies that are too costly to be applied to the system as a whole, such as formal verification, but that may be cost effective for these limited sub-sets of the requirements. Both also involve problems and techniques that apply specifically to them and not to other more general functional requirements or constraints. If an accident or loss event is defined to include unauthorized disclosure, modification, and withholding of data, then security becomes a subset of safety."

This is not to say that previous *cause and effect chain of event sequence models* do not have value in their analysis of simpler systems. However, the Nancy Leveson Control Theory mental model is an extension of these techniques that capture all hazards associated with the most complex safety critical systems.

Mental Model - Beyond the Next Step: The Critical Infrastructure Protection Approach

Critical Infrastructure Protection is considered going beyond including analysis of both *system safety hazards and security threats* to a fully integrated global security and safety Management System. Critical Infrastructure protection looks at the source of hazards and threats from a national perspective. It assesses all essential elements required to maintain a healthy, prosperous, safe and secure environment within a nation as it pertains to a critical infrastructure sector.

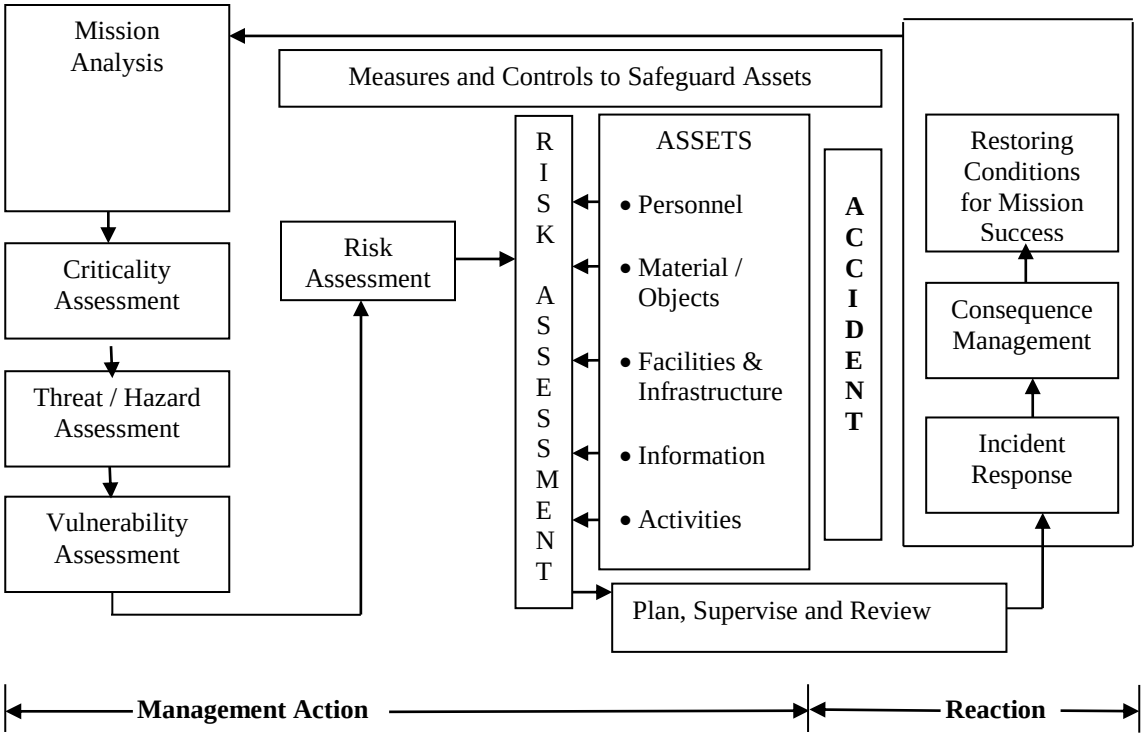
Homeland Security within the USA has identified eighteen critical elements that are considered separate and distinct sectors that must be protected from security threats and system safety hazards including; energy, nuclear reactors, dams, banking and finance, agriculture and food, transportation systems, government facilities, national monuments and icons, postal and shipping, information technology, communications, health care and public health, water, emergency services, critical manufacturing, commercial facilities, defense industrial base, and chemical.

In Canada, the Department of Public Safety has identified ten sectors including; energy and utilities, finance, food, transportation, government, communications and information technology, health care, water, *safety*, and manufacturing. Note that the word "*safety*" in this list pertains more to the general protection of the citizens from harm than from a terrorist intervention or a system safety viewpoint. Critical Infrastructure has been defined as infrastructure so vital that its incapacity or destruction would have a debilitating impact on national security, the economy, public health and safety. [1]

Figure 5: Sub-sectors exist within each sector.

National Sectors	National Sub-sectors
Energy and utilities	• Electrical power generation and transmission • Natural gas production and transmission • Oil production and transmission
Finance	• Banking, • Securities, • Investment, • Insurance
Food	• Agriculture and food industry • Food distribution • Food safety
Transportation	• Air, Rail, • Marine, Surface
Government	• Government services (e.g. weather services)
Communications and information technology	• Telecommunications (voice, fax, video) • Broadcasting (radio, television) • Information Networks (Internet)
Health care	• Hospitals • Clinics • Blood-supply facilities • Laboratories • Pharmaceutical industry
Water	• Drinking water • Wastewater
Safety	• Chemical, biological, radiological, and nuclear • Hazardous materials • Search and rescue • Emergency services (police, fire, ambulance and others) • Dams
Manufacturing	• Chemical industry • Defense industrial base

Figure 6: Critical Infrastructure Protection (CIP) Risk Management Mental Model



The CIP Risk Management model can be applied at the international, national, regional or local level. The components of the model are defined as follows;

- *Mission Analysis*: Planning begins with the conduct of a Mission Analysis to confirm the mission, vision and purpose of the organization.
- *Criticality Assessment:* A Criticality Assessment is performed to identify and prioritize those assets and functions that are essential to accomplishing the mission.
- *Hazard / Threat Assessment*: All threats (deliberately caused events) and hazards (unintentionally caused or natural events) to critical infrastructure must be considered in an all hazard approach. Threats and hazards can be grouped as deliberate, natural, and accidental.
- *Vulnerability Assessment*: Separate Vulnerability Assessments are conducted for each asset identified as critical to accomplishing the mission.
- *Risk Assessment*: The probability and impact of a threat agent or hazard exploiting vulnerability in an asset is assessed, by using the results of the previous four steps.
- *Risk Management*: The impact of the non-provision of mission critical services or the disruption / destruction of mission critical facilities, such that controls and measures must be implemented in order to create the conditions for mission success. The selection of appropriate controls / measures and the assumption of the remaining residual risk by the responsible authorities are required.
- *Incident Response*: In cases where prevention, resiliency and redundancy have not been effective to stop an incident from occurring, effective response capabilities must be planned in advance, tested and maintained.
- *Consequence Management*: Consequence management includes both recovery and restoration of critical facilities and services. Recovery requires resources.
- *Restoring Conditions for Mission Success*: This includes completion of the recovery process and incorporating any lessons learned as a result of the incident.

- *Before an incident occurs, management has the flexibility to act*: During and after an incident, management reacts. Throughout the process management supervises, plans, and reviews risk management measures.

There are several reasons why it may be difficult to implement the CIP risk management process including;

- No clear definition of what is considered critical. It should be possible to determine this by the normal hazard and threat analysis techniques referred to above
- No clear designation of who can determine what constitutes an individual critical system
- No clear delineation of governance responsibilities
- There is a need for owners of critical infrastructure to operate profitable businesses. Since 80% of critical infrastructure is owned and operated by the private sector; this means that gaining access and taking protective measures is not easy.

Four steps that this CIP Risk Management Mental Model incorporates in its risk mitigation process include;

- Must know what is most critical,
- Must understand the risks,
- Must be ready to respond, and
- Must have a recovery plan.

An important characteristic to build into an organization that owns and operates critical infrastructure is resilience. A resilient organization is able to achieve its core objectives in the face of adversity through a combination of measures. Operational resilience is the ability of an organization to adapt to risk that affects its core operational capacities: business processes, systems, technology, and people. Operational resilience combines infrastructure resilience and organizational resilience. The core process of operational resilience is Business Continuity Planning (BCP). BCP identifies what is critical to the operation and what the associated tolerances are in the event of a disaster.

One area of critical infrastructure that has become vulnerable due to modern technology is SCADA (supervisory control and data acquisition) systems. Redmill states; "Security and Access Control. The increasing use of local area networks (LAN) and wide area networks (WAN) to link computer systems is raising the profile of security and access control."

Wikipedia states regarding SCADA systems; "Security issues: The move from proprietary technologies to more standardized and open solutions together with the increased number of connections between SCADA systems and office networks and the Internet has made them more vulnerable to attacks. Consequently, the security of some SCADA systems has come into question as they are seen as potentially vulnerable to cyber attacks."[3]

Security researchers indicate that:

- There is a lack of concern about security and authentication in the design, deployment and operation of some existing SCADA networks
- SCADA systems have the benefit of security through obscurity through the use of specialized protocols and proprietary interfaces
- SCADA networks are secure because they are physically secured
- SCADA networks are secure because they are disconnected from the Internet.

SCADA systems are used to control and monitor physical processes, examples of which are transmission of electricity, transportation of gas and oil in pipelines, water distribution, traffic lights, and other systems used as the basis of modern society. The security of these SCADA systems is important because compromise or destruction of these systems would impact multiple areas of society far removed from the original compromise. A blackout caused by a compromised electrical SCADA system would cause financial losses to all the customers that received electricity from that source. How security will affect legacy SCADA and new deployments remains to be seen. In June 2010, security reported the first detection of malware that attacks SCADA systems running on Windows operating systems. The malware is called

Stuxnet and used four zero-day attacks to install a rootkit which in turn logs into the SCADA's database and steals design and control files. The malware is also capable of changing the control system and hiding those changes. The malware was found on 14 systems, the majority of which were located in Iran. [3]

An example of a combined system safety and security analysis is; "NASA L-Band Digital Aeronautical Communications System Engineering, an initial Safety and Security Risk Assessment and Mitigation by Natalie Zelkin and Stephen Henriksen; ITT Corporation Advanced Engineering & Sciences Division, Herndon, Virginia, January 2011. On page 5 it states; "Two disciplines of specialty engineering (SE), system safety engineering (SSE) and information engineering (ISE), are applied to conduct this analysis. For the purposes of this analysis, safety and security risk identification, assessment, and mitigation are addressed separately. However, similarities between the two types of the analyses are underlined throughout the document. Both are based on functional analysis of the L-band system, and both follow suggested FAA methodology for risk analysis. Furthermore, "From a safety perspective, the threats that concern security are another potential cause of safety hazards, while from a security perspective; the hazards that concern safety are another potential outcome of security threats," Thus, hazard severity levels can be assigned to the safety hazards that could be caused by security threats."

Conclusion

System Safety and Security can and should be analyzed for a complex system by using a common analysis methodology. This paper traces the development of analyses of safety critical systems. It compares the simple Pyramid, Domino, the Swiss Cheese Model as applied by ICAO, Leveson's STAMP/STPA control theory approach, Rasmussen/ Svedung model, and finally a combined System Safety and Security analysis approach in ITT Corporation (Zelkin / Henriksen) example.

References

1. Software Engineering by Ian Sommerville, 1996, p. 24
2. Wikipedia, 1 WTC, Safety and Security, http://en.wikipedia.org/wiki/One_World_Trade_Center
3. Lifecycle Management for Dependability by Felix Redmill and Chris Dale, 1997, p. 146,
4. SCADA Systems: http://en.wikipedia.org/wiki/SCADA#Security_issues, 2012
5. Safeware-System Safety and Computers by Nancy Leveson, 1995, p. 182
6. Engineering a Safer World by Nancy G. Leveson, 2011, p. 32, p. 57, p.82
7. Life Cycle Management for Dependability by Fekix Redmill and Chris Dale, 1997
8. ICAO Safety Management Manual (SMM) Doc 9859 AN/474, 2009
9. Software Assessment–Reliability, Safety, Testability by Michael A. Friedman and Jeffrey M. Voas, 1995
10. Assurance Technologies Principles and Practices-A Product, Process, and System safety Perspective by Dev G. Raheja and Michael Allocco, 2006
12. The Fifth Discipline-The Art & Practice of the Learning Organization by Peter M. Senge, 1990
13. Barriers and Accident prevention by Erik Hollnagel, 2004
14. Organization at the Limit-Lessons from the Columbia Disaster by William H. Starbuck & Moshe Farjoun, 2005

Biography

Robert Ward Fletcher P.Eng.; M.Sc., PMP; PCIP, Consultant, President, Robert Fletcher System Safety, Inc.; Ottawa, Ontario, Canada. Email: rwfletcher@sympatico.ca, Address: 241 Kennedy Lane West, Ottawa, Ontario, Canada, K1E 1G5. Telephone: business 613-837-4128.

Robert is a system safety engineer with many years of experience. He has performed system safety consultancy services work for several clients around the world. He performed System Safety engineering and safety management systems training, auditing and analysis for air traffic control and flight service system applications. Robert has received a M.Sc. from the United States Navy Post Graduate School, a diploma from the Aerospace Systems School, Winnipeg, Manitoba and a Bachelor of Science degree from the Royal Military College. He is a registered professional engineer, a member of the Project Management Institute, and the Critical Infrastructure Institute.