Accidents, "Black Swans" and Risk

John C. Luxat
Professor & NSERC/UNENE Industrial Research Chair In Nuclear Safety Analysis
Department of Engineering Physics, McMaster University
1280 Main Street West, Hamilton, ON, L8S 4L7
luxatj@mcmaster.ca

Abstract

Major accidents and natural disasters with severe consequences have occurred in all sectors of industrial activity with relatively high frequency. The severe consequences of concern involve either significant loss of life or major economic loss, or both loss of life and economic loss. Such events have in the last two years often been referred to as "Black Swan" events following publication of a best-selling book. The events demonstrate limits to the application of Probabilistic Risk Assessment (PRA) that arise from the underlying unquantifiable uncertainty associated with the estimation of the frequency of occurrence of such events. An approach is proposed in this paper that, consistent with the concept of defense in depth employed by the nuclear industry, augments probabilistic risk assessment with a methodology based upon "threat -risk assessment". This approach shifts these very low frequency, high uncertainty, and high consequence "Black Swan" events out of the probabilistic risk assessment domain and into a deterministic emergency response assessment domain.

1. Introduction

Major accidents with severe consequences have occurred in allsectors of industrial activity with relatively high frequency. The severe consequences of concern involve either significant loss of life or major economic loss, or both loss of life and economic loss. Despite the intense scrutiny that occurs following such events, history would indicatethat the occurrence of such accidents may be expected to continue with relatively high frequency. Many of these accidents are initiated by failures in engineered systems or by human actions and are referred to as accidents with man – made origins.The energy sector, in particular, is recognized to be one of the major sources of man-made accidents and disasters [1, 2]. Major accidents have occurred in all areas of the energy sector, including resource extraction, transportation,production anddistribution.

Other accidents are triggered by natural disastersthatoften are compounded by subsequent human actions and errors. Worldwide, natural disaster events are occurring with an apparent increasing magnitude and increasing frequency. This has been attributed by some, particularly in the media and popular press, as evidence that we are currently experiencing an era of significant climate change. Examples which come to mind are, Hurricane Katrina and Hurricane Sandy in the U.S.A. However, not all natural disasters are linked to apparent climate change. Some are random in nature and essentially unpredictable, although their location of occurrence is not. Examples of such events are the 2004Indian Ocean earthquake and tsunami and the 2011 massive Tohoku earthquake and tsunami off the coast of Japan. Both of these events occurred in the seismically active "Ring of Fire" region in the Pacific.

The above observations raise a question: are we merely experiencing a period of "bad luck" or are there inherent technical deficiencies in our risk assessment and accident management response planning methods? This question is addressed in this paper. It is suggested that there are indeed limits in the applicability of Probabilistic Risk Assessment [PRA] to very low frequency, high consequence events. The limits arise from the underlying high, non-quantifiable uncertainty associated with the estimation of frequency of occurrence of such events. Such events have the last few years been increasingly referred to as "black swan" events, following publication ofTaleb's best-selling book [3]. A secondary question is: to what extent are lessons learned from severe accidents in all sectors of industrial activity being used to improve safety in a specific sector, such as nuclear energy?

If indeed, as suggested in this paper, there are fundamental limits to the applicability of probabilistic risk assessment, which is an important tool in supporting nuclear safety and nuclear industry,then what can we do to address the deficiencies? An approach is proposed in this paper that is consistent with the concept of defense-in-depth employed by the nuclear industry and whichaugments probabilistic risk assessment with a methodology based upon "threat–risk assessment". This approach shifts thesevery low frequency, high consequence "black swan" events out of the probabilistic risk assessment domain and places them into a deterministic emergency response assessment domain. The proposed approach is discussed further in this paper.

2. Review of Natural and Man–Made Accidents and Disasters

Over the past 30 – plus years, a series of man-made accidents and natural disasters have been experienced worldwide. The extent and magnitude of such events have been strongly influenced by either human actions or inaction. A representative set of events with high consequences is described in summary form in Tables 1 and 2. As is evident from these tables the accidents and disasters have occurred in a range of industrial activities including: energy transportation (Dona Paz ferry disaster); energy (DeepwaterHorizon [4], BP Texas Refinery fire [5], TMI–2 [6], Chernobyl [7], Fukushima [8]); and aerospace (Challenger [9], Columbia [10]). Other disasters have origins in natural events (2004 Indian Ocean tsunami [11], Hurricane Katrina [12], Hurricane Sandy [13]) and malevolent acts (9/11 [14]) whose consequences were compounded by combinations of human error and deficiencies in design and emergency response planning.

It is interesting to note tha,t even though these events occurred in disparate sectors of economic activity, ranging from public transport, energy transport, space exploration, energy production, and nuclear energy production, they display a significant commonality in terms of the factors that compounded the deleterious consequences of the events. These commonalities are discussed in the following sections.

ACCIDENT	TYPE	DESCRIPTION
Dona Paz, Philippines 1987	Man-made: Oil transportation	The MV Doña Paz, a Philippine-registered passenger ferry, sank after colliding with the oil tanker MT Vector on December 20, 1987. The Vector's cargo ignited and spread to the Doña Paz. The survivors jumped off the ship and swam in shark-infested flaming waters around the ship. The Doña Paz sank within two hours of the collision, and the Vector sank within four hours. It took 8 hours for Philippine maritime authorities to learn of the accident, and another 8 hours before search and rescue operations were undertaken. The collision resulted in the deadliest peacetime maritime disaster in history with >4300 deaths.
BP Texas Oil Refinery Fire 2005	Man-made: Oil production	On March 23, 2005, an explosion occurred at BP's Texas City Refinery, the third-largest refinery in the United States. The explosion occurred in an isomerization unit which was overfilled with liquid that overheated, leading to liquid discharge and formation of a ground level vapor cloud. The cloud was ignited by the running engine of a contractor's pickup truck. 15 workers were killed and more than 170 were injured. At the time, this was considered one of the worst industrial accident in US history.
Deepwater Horizon 2010	Man-made: Oil production	On 20 April 2010, while drilling at the Macondo Prospect in the Gulf of Mexico, an explosion on the rig caused by a blowout killed 11 crewmen and ignited a fireball visible from 56 km away. The fire could not be extinguished and, on 22 April 2010, Deepwater Horizon sank, leaving the well gushing at the seabed and causing the largest offshore oil spill in U.S. history.
Challenger disaster 1986	Man-made: Aerospace	The Space Shuttle Challenger disaster occurred on January 28, 1986, when the vehicle broke apart 73 seconds into its flight. The spacecraft disintegrated over the Atlantic Ocean, off the coast of central Florida. Disintegration of the entire vehicle began after an O-ring seal in its right solid rocket booster failed at liftoff. The seven crew members died.
Columbia disaster 2003	Man-made: Aerospace	The Space Shuttle Columbia disaster occurred on February 1, 2003, when it disintegrated over Texas and Louisiana during re-entry into the Earth's atmosphere. The loss of Columbia was a result of damage sustained during launch when a piece of foam insulation broke off from the Space Shuttle external tank and struck the leading edge of the left wing, damaging the Shuttle's thermal protection system which shields the vehicle from the intense heat generated from atmospheric compression during re-entry. All seven crew members were killed.
9/11 2011	Malevolent act	A series of four coordinated terrorist attacks were launched by the Islamist terrorist group al-Qaeda upon the United States in New York City and the Washington, D.C. areas on September 11, 2001. Two planes, American Airlines Flight 11 and United Airlines Flight 175, were crashed into the North and South towers, respectively, of the World Trade Center complex in New York City. Both towers collapsed within two hours and falling debris, combined with fires that the debris initiated in several surrounding buildings, led to the partial or complete collapse of all the other buildings in the World Trade Center complex. A third plane, American Airlines Flight 77, was crashed into the leading to a partial collapse in its western side.an a fourth plane, United Airlines Flight 93, targeted at the United States Capitol in Washington, D.C., crashed into a field in Pennsylvania after its passengers tried to overcome the hijackers. Almost 3,000 people died in the attacks, including all 227 civilians and 19 hijackers aboard the four planes.

TABLE 1
SOME RELEVANT HIGH CONSEQUENCE MAN-MADE ACCIDENTS AND DISASTERS

ACCIDENT	TYPE	DESCRIPTION
Hurricane Katrina 2005	Natural disaster	Hurricane Katrina made landfall on Monday, August 29, 2005 in southeast Louisiana, causing severe destruction along the Gulf coast from central Florida to Texas. Flooding in in New Orleans, Louisiana, occurred when the levee system catastrophically failed. The hurricane surge protection failures in New Orleans are considered the worst civil engineering disaster in U.S. history. It was the costliest natural disaster, as well as one of the five deadliest hurricanes, in the history of the United States. At least 1,833 people died in the hurricane and subsequent floods, and total property damage was estimated at $81 billion.
Hurricane Sandy 2012	Natural disaster	Hurricane Sandy is the largest Atlantic hurricane on record, with a diameter of 1,800 km, affecting 24 states, including the entire eastern seaboard from Florida to Maine and west across the Appalachian Mountains to Michigan and Wisconsin. Severe damage from the storm surge occurred in New Jersey and New York, where it flooding streets, tunnels and subway lines and cutting power in and around the cites. Damage in the US is estimated at over $100 billion and approximately 285 people were killed along the path of the storm in seven countries.
Indian Ocean tsunami 2004	Natural disaster	The 2004 Indian Ocean earthquake was an undersea subductionmegathrust earthquake that occurred on Sunday, 26 December 2004, with an epicentre off the west coast of Sumatra, Indonesia and a magnitude of 9.1–9.3. The subduction caused a series of massive tsunamis along the coasts of most landmasses bordering the Indian Ocean. Over 230,000 people in fourteen countries were killed, and coastal communities were inundated with waves up to 30 meters.
Three Mile Island - U2 1979	Man-made: Nuclear Power	The Three Mile Island Unit 2accident was a partial core meltdown. The accident which occurred on March 28, 1979, was the worst accident in U.S. commercial nuclear power plant history. The accident was initiated by failures in the non-nuclear secondary system, followed by a stuck-open pilot-operated relief valve (PORV) in the primary system, which allowed large amounts of nuclear reactor coolant to escape. The failures were compounded by the initial failure of plant operators to recognize the situation as a loss-of-coolant accident due to inadequate training and human factors, such as poor ergonomic design of the control room. Small amounts of radioactive gases and radioactive iodine were released into the environment, resulting in insignificant radiation exposure to plant operators and the public.
Chernobyl U4 1986	Man-made: Nuclear Power	On 26 April 1986, reactor Chernobyl Unit 4 experienced a catastrophic power increase, leading to explosions in the core which dispersed large quantities of radioactive fuel and core materials into the atmosphere and ignited the combustible graphite moderator. The burning graphite moderator increased the emission of radioactive particles, carried in a plume, as the reactor had no containment structure. The accident was initiated during an experiment conducted at the start of a scheduled outage to test a potential safety emergency core cooling feature. It is considered to be the worst nuclear power plant accident in history. Over 600,000 people were involved in the clean-up and the estimated cost was 18 billion rubles.
Fukushima	Natural disaster + Man-made: Nuclear Power	The Fukushima accident was initiated by a massive 9.0 magnitude earthquake of the north-east coast of Japan which resulted in a series of massive tsunami waves. The tsunami flooding resulted in loss of all normal and backup electrical power to 3 operating units and 1 shutdown unit. Two other units which were in outages at the time managed to restore backup power because their higher elevation limited the extent of flooding. Meltdown of three reactor cores to an as yet to be determined extent is predicted to have occurred. Severe damage to the outer reactor buildings of 3 units occurred due to hydrogen explosions. There were no fatalities but a large number of people were evacuated from a region to the northwest of the station.

TABLE 2
SOME RELEVANT HIGH CONSEQUENCE NATURAL DISASTERS AND NUCLEAR ACCIDENTS

3 Compounding Factors in Accidents

While the initiating events do not necessarily share unique common factors, the consequences of the events are generally compounded by a number of similar factors that lead to an increase in the severity of the event and/or inadequate emergency response to the event. These compounding factors are briefly discussed below.

3.1 DesignDeficiencies

This factor is common to a wide range of accidents and disasters involving engineered systems. Any system, be it an element of industrial infrastructure or a system engineered to protect members of the public against hazards, is subject to possible deficiencies in design which can result in the failure of the system when subject to challenge and stress. Deficiencies include: failure to specify key design requirements; failure to recognize interactions within and between systems when subjected to conditions that challenge their functioning; common – mode failures of components; and common – cause external events that expose system vulnerabilities following the initiating events. These latter common – mode or common – cause factors are the most difficult to account for in probabilistic risk assessment simply because their probability of occurrence usually cannot be predicted *a–priori* and are accounted for in a general, simplistic manner.Most often, it is only after the failure events have occurred that it is possible to understand the nature of the failure and assign an event frequency value, albeit that this value will retain high uncertainty given the small number of such events that have been experienced.

3.2 ProceduralNon-compliance/Inadequate Training

These factors reflect the contribution of the human operator to compounding the consequences of an event. Systems that are designed to have operator actionsto assure their correct functioning are subject to these compounding factors. Assurance of safe operation requires that operating procedures be developed to regulate the manner in which operators interact with the systems. Failure to either understand (inadequate training) or follow procedures (procedural non-–compliance) can result in operators taking either inappropriate actions (*commission of an action*) or failing to take action(*omission of an action*) during the progression of an event, thereby resulting in more severe consequences.

3.3 InadequateEmergency Preparedness

If an organization fails to adequately prepare for emergencies before an actual emergency occurs, then this failure can diminish the capability of the organization and its stakeholders to respond to the event and, in turn, result in worsening the impact the event. Such failures include: lack of a well-designed emergency response organizational function; lack of training in the application of the response function; inadequate or non-existent support equipment; and an inadequate ability to deploy equipment in a timely manner.

In the nuclear industry specific examples of these compounding factors include: lack of or inadequately developed severe accident mitigation guidelines (SAMG) and lack of preplanned and readily deployed emergency support equipment that does not depend on on-site services, such as electricity and water supplies. Not only must SAMG exist, but they should be developed from a well characterized knowledge base (the technical basis) and they should have a clearly articulated set of candidate high level actions that assist in bringing the accident to a safe terminal state. Contrary to some current beliefs, the SAMG should not be reliant on a high degree of plant instrumentation, since the functioning of the instrumentation cannot be assured with high confidence under the harsh conditions associated with severe accidents. To build such dependency on instrumentation into SAMG renders them susceptible to failure should the instrumentation the lost.

3.4 Institutional Failure

This is a broad category of factors which relate to the functional attributes and capability of operating organizations. It has become a popular term that is used to denote situations where poor organizational design, poor definition of roles and responsibilities, poor communications and organization culture contribute to accidents. Institutional failures include, amongst other elements:

- poor safety culture,
- acceptance of deficiencies,
- a focus on mission imperatives (economic, policy, public relations) at the expense of a safety focus in decision-making,
- poor communication between various groups within an organization or with external stakeholder,
- inadequate regulation, both external or internal

Nearly all major accidents and disasters exhibit some degree of institutional failures. In some instances the failures are stark, such as Chernobyl, the Challenger disaster and the Dona Paz ferry disaster, while in other instances the issues contributing to failure and ultimate outcomes are more complicated, for example the Columbia disaster, Deepwater Horizon, Fukushima and TMI-2.

Some of the key compounding factors associated with the high consequence accidents identified in Tables 1and 2 are listed in Tables 3 and 4.

ACCIDENT	TYPE	INITIATOR	COMPOUNDING FACTORS	CONSEQUENCES
Dona Paz, Philippines 1987	Man-made: Oil transportation	Procedural non-compliance of ferry crew	• Poor ship-to-shore communication • Lack of Emergency Response • Institutional failure	>4300 dead
BP Texas Oil Refinery Fire 2005	Man-made: Oil production	Procedural non-compliance and operator error	• Poor safety culture • Institutional failure (BP) – acceptance of poor plant condition and inadequate procedures • Poor communication • Lack of competent supervision	15 workers killed and more than 170 injured
Deepwater Horizon 2010	Man-made: Oil production	Defective well seal design BOP failure	• Gas explosion • Poor safety culture • Institutional failure (BP)	11 deaths Major environmental pollution of Gulf Coast. >> $10B loss
Challenger disaster 1986	Man-made: Aerospace	Design defect: O-ring seal failure	• Low temperature • Institutional failure – mission imperative	7 deaths, total loss of space shuttle
Columbia disaster 2003	Man-made: Aerospace	Damage to thermal protection system on a wing due to impact of dislodged insulation from external tank during launch	• Institutional failure – poor decision-making and risk management • Poor safety culture • Acceptance of design deviations – insulation breaking free regularly during launces	7 deaths, total loss of space shuttle
9/11 2011	Malevolent act	Multiple crashes of hijacked commercial jet-liners into buildings in New York and Washington D.C.	• Inadequate co-ordination between security and intelligence organizations • Thermal insulation on steel structural members dislodged by aircraft impact	2977 persons killed + 19 hijackers Total loss of the two World Trade Centre (WTC) towers and two other buildings in the WTC complex in New York

TABLE 3
CHARACTERISTICS OF HIGH CONSEQUENCE MAN-MADE ACCIDENTS AND DISASTERS

ACCIDENT	TYPE	INITIATOR	COMPOUNDING FACTORS	CONSEQUENCES
Hurricane Katrina 2005	Natural disaster	Extreme weather event	• Inadequate flood control design. • Lack of Emergency Preparedness	• ~1800 deaths • ~ $200B loss
Hurricane Sandy 2012	Natural disaster	Extreme weather event	• Inadequate flood control design.	• >200 deaths • Major infrastructure damage • > $100B+ loss
Indian Ocean tsunami 2004	Natural disaster	Subduction earthquake	• Lack of Emergency Preparedness • Poor communication • Lack of training – recognition of tsunami behaviour	• >230,000 people killed
Three Mile Island - U2	Man-made: Nuclear Power	Equipment failure: Loss of feed water	• Procedural non-compliance: auxiliary feedwater discharge valves not returned to service • Design deficiencies • OPEX failure • Poor operator training • Inappropriate operator actions • Institutional failure: lack of safety culture	• Radiological: minimal • Economic: major loss – complete loss of unit 2 • 0 deaths
Chernobyl U4	Man-made: Nuclear Power	Operator action: test initiation	• Design vulnerability • Poor operator training • Institutional failure: lack of safety culture • Institutional failure – mission imperative	• Radiological: major release • 28 deaths + 28 over next 20 years • Environmental • Economic: major loss– complete loss of unit 4 • Political: hastened collapse of USSR
Fukushima	Natural disaster + Man-made: Nuclear Power	Massive Earthquake + Massive tsunami waves	• Inadequate flood control design, backup diesels, electrical systems vulnerability • Lack of SAMG and Emergency Preparedness • Institutional failure: inadequate regulation, poor communications between utility and government	• Radiological: major release – multiple units (~ 10% of Chernobyl) • 0 deaths • Environmental contamination • Economic: major loss

TABLE 4
CHARACTERISTICS OF HIGH CONSEQUENCE NATURAL DISASTERS& NUCLEAR ACCIDENTS

4 "Black Swans" and Risk

Following the publicationin 2010 of Taleb's book,*The Black Swan: the Impact of the Highly Improbable*, the term Black Swan has become popular when discussing events with high consequences and perceived low probability of occurrence. A general definition for a Black Swan event is:

> *An event with high consequence which is judged to be incredible until it occurs, at which point the causes become apparent.*

One key aspect of a black swan event is that the frequency of its occurrence cannot be predicted with any level of certainty. Because its frequency is perceived be very low based on historical evidence, it is actually not possible to assign quantitative values to the frequency of occurrence in the future. Another key aspect is that, because of the low perceived frequency of occurrence, the event is considered incredible, thereby "justifying" that the event be given no further consideration (for example, application of a lower bound cut-off frequency used to rule out events in PRA). This causes major difficulties inappropriately treating such events within qualitative risk assessment, such as PRA. This difficulty arises from very definition of riskemployed in such assessments,that is:

Risk = Consequences *Frequency

The necessary conditions for performing a balanced quantitative risk assessment is that quantitative values for both of the two factors in the above equation can be reasonably assigned and, more importantly, the uncertainties in both factors in the above equation are not significantly biased towards one of the two factors. In the case of black swan events neither of these two conditions can be met for the frequency of occurrence.

The above does not imply that probabilistic risk assessment is an ineffective tool for assessing aspects of nuclear reactor safety. It is indeed an effective tool for assessing the robustness of nuclear plant designs and for identifying the risk dominance sequences associated with a well characterized design subject to internal failure events – in particular for evaluating component and system failure frequencies in a level I risk assessment and consequences in a level II risk assessment. The problem lies in the assignment of frequency values to:

- unknown common – cause failures.
- the impact of human operator psychology that can result in unexpected behavior.
- unidentified common – cause vulnerabilities, especially vulnerabilities to external events.

To deal with these limitations it is proposed that probabilistic risk assessment be augmented with threat-risk assessment methods which are not probabilistically based. The application of threat-

risk is applied consistent with the use of defense-in-depth concepts [15]. In particular, threat-risk assessment methods are applied at levels 4 and 5 of the IAEA defense in depth construct shown in Table 5.

Threat - risk assessment is a deterministic assessment process that is often used by police, security and military forces to support emergency preparedness planning. It does not attempt to rank threats by their likelihood. Rather it postulates: "*what if*" a threat occurs then,"*what are*" the range of consequences that may result, and "*what are*" the options to mitigate the consequences and stabilize the event. This assessment is conducted in a systematic and rigorous fashion to ensure that no vulnerabilities are overlooked and that the adequacy of mitigation measures can be evaluated. It is ideally suited for addressing black swan events because the frequency of events does not enter into the assessment. Furthermore, application of this methodology does not lead to a tendency to dismiss events as being incredible solely on the basis of a perceived very low frequency. The outcome of the assessment is focused upon the adequacy and vulnerabilities of emergency preparedness and emergency response actions.

A typical threat-risk assessment involves consideration of single or multiple events which are a threat (hazard) to the successful functioning of systems that are important to safety. This requires consideration of***severity of the threat***, typically using attributes such as:the potential hazard (nature and magnitude); the plant areas, systems and components that are affected by the hazard (extent); vulnerability of plant mitigating systems to common-cause effects of the hazard. Each attribute is assigned a value on an increasing integer scale (e.g. 1 = normally expected, 2 = larger than expected, 3 = extreme). The product of the attribute values yields a **severity index**. Similarly, consideration is given to the ***necessary mitigating actions*** which are characterized by a set of attributes such as: availability; access; deployment complexity; deployment delay; operational complexity. Each attribute is assigned a value on an increasing integer scale (e.g. 1 = mitigation by available in-plant systems, 2 = mitigation by available in-plant and limited ex-plant systems, 3 = mitigation requires multiple ex-plant systems).The product of the attribute values yields a **mitigation index**. The surrogate relative risk measure associated with a potential threat is given by:

Threat-risk = Severity index * mitigation index

Since the severity index is usually determined by factors that are invariably beyond one's control (e.g. common-cause extreme weather events, earthquakes and tsunamis, wide-spread fires), the primary means of risk reduction is through provisions that reduce the mitigation index (i.e provide more robust emergency response capability).

In the case of TMI-2, the risk reduction measures would have included: enhanced procedural compliance (returning blocked valves to their normal unblocked state after a maintenance outage); operator training using simulators (better upset event diagnosis and response); and identification and correction of design deficiencies (e.g. placement of temperature measurement

downstream if the PORV that stuck open). These measures were instituted subsequent to the event as part of the lessons learned.

In the case of Fukushima, the risk reduction measures would have included: recognition that large tsunamis can be generated from earthquakes; recognition of the vulnerability of both in-plant electrical systems and the backup emergency diesel generators to extreme flooding; and provision of easily accessible backup electrical supplies and pumps that could be both readily brought onto site and readily connected. These are the measures that are being pursued world-wide as part of lessons learned activities. However, the effectiveness of such lessons learned may well be limited if they are only focused on seismic and flooding events.

The one aspect of a Black Swan event is that it generates wide-ranging "lessons learned" studies after the event has occurred. Many of the findings from these lesson learned from one event to another are similar in nature (e.g. poor safety culture, institutional failure, design deficiencies and vulnerabilities, poor operator training, etc.). However,although the findings have often lead to safety improvements, they have not lead to an apparent reduction in the risk of high consequence Black Swan events simply because these events are *a-priori* considered "incredible". A systematic and rigorous threat-risk assessment can result in more robust emergency response planning and performance for such events.

5. Conclusions

The characteristics of high consequence and low frequency accidents and disasters have been identified and related to the concept of a Black Swan event. The inherent limitations of quantitative probabilistic risk assessment have been discussed and the problems associated with applying this assessment methodology to Black Swan events is shown to be associated with the large and difficult to quantify uncertainty associated with the frequency factor in the classical risk equation.

An approach is proposed to address these limitations by augmenting probabilistic risk assessment with threat-risk assessment methods applied to the emergency response domain associated with levels 4 and 5 of the IAEA defense-in-depth construct. This approach does not focus on fixed design features that are integral to providing assurance of safety at levels 1 to 3 of defense-in-depth. Rather, it provides a consistent means to assess the relative risk of combinations of events with little or no quantifiable history and to identify relative risk reduction measures that can be achieved through a focus on emergency response measures (defense-in-depth at the levels 4 and 5) [16].

6. Acknowledgments

The financial support of the Natural Sciences and Engineering Research Council of Canada (NSERC) and the University Network of Excellence In Nuclear Engineering (UNENE) is gratefully acknowledged.

References

1. S. Hirschberg, et al," Severe accidents in the energy sector: comparative perspective", J. Hazardous Materials, vol. 111, pp 57-63, 2004.
2. S. Hirshberg, et al, "Severe Accidents in the Energy Sector, 1st Edition", PSI Report No. 98-16, PaulScherrer Institute
3. Nassim Nicholas Taleb, *The Black Swan: the Impact of the Highly Improbable*, 2nd Edition, Random House, 2010
4. United States Coast Guard, "Report of the Investigation into the circumstances surrounding the explosion, fire, sinking and loss of 11 crew members aboard the Mobile Offshore Drilling UnitDeepwater Horizon the Gulf of Mexico".
5. US Chemical Safety and Hazard Investigation Board, Investigation Report; Refinery Explosion and Fire BP Texas, March 23 2005, Report No 2005-04-1-TX, March, 2007.
6. J.G. Kemeny, et.al., "Report of the President's Commission on the Accident at Three Mile Island",Washington D.C., U.S.A., October 10, 1979.
7. Report on the Accident at Chernobyl Unit 4, IAEA, 1986.
8. American Nuclear Society, Fukushima Daiichi: ANS Committee Report, July 2012. Nuclear Society
9. W.P. Rogers, et.al., "Report of the Presidential Commission on the Space Shuttle Challenger Accident", Washington D.C., U.S.A., June 9, 1986.
10. H.W. Gehman, et.al.,"Report of the Columbia Accident Investigation Board", NASA, August 2003.
11. Yoshiaki Kawata, et al, Comprehensive analysis of the damage and its impact on coastal zones by the 2004 Indian Ocean tsunami disaster, Kyoto University, Japan, 2006
12. F.F. Townsend, "The Federal Response To Hurricane Katrina: Lessons Learned", U.S. White House, Washington D.C. U.S.A., February 2006.
13. National Hurricane Center, Tropical Cyclone Report: Hurricane Sandy, 12 February 2013.
14. *National Commission on Terrorist Attacks Upon the UnitedStates* (9/11 Commission), First Edition, W.W.Norton& Company,
15. International Nuclear Safety Advisory Group," Defense in Depth: INSAG-10", IAEA, Vienna, 1996

LEVEL	OBJECTIVE	MEANS
1	Prevent abnormal operation and failures	Conservative design (e.g. redundancy, fail-safe features) High quality construction and operation Equipment maintenance In-service inspections Plant technical surveillance Trained operators
2	Control abnormal operation and detect failures	Control systems Protection systems Trained operators
3	Control of accidents within the design basis	Special safety systems Emergency procedures Trained operators
4	Prevent accident progression to more severe consequences or mitigate their consequences	Severe Accident Management Guidelines (SAMG) Trained operators & staff
5	Mitigate radiological consequences of a significant off-site release	Off-site emergency response Trained staff

TABLE 5
IAEA LEVELS OF DEFENSE IN DEPTH [15]