Extreme Events and their Impacts
Managing Environmental Risk

By David L Russell, PE, President, Global Environmental Operations, Inc.

Environmental Risk comes in many forms. Sometimes, it's associated with everyday activities and project work. Other times, it's unexpected trouble on a project. With each activity, we can identify and quantify major and minor risk elements. There is a statistical and mathematical, basis for quantifying the risk and associated damage, and the evaluation of the risk items, allows us to improve our planning when we are conducting activities in an emergency response mode. Quantifying the risk and its probabilities enables us to prepare our plans for disaster management.

1. Security vs. Risk: Polar Opposites

Risk and security are polar opposites. What we want is to manage field risk and provide security for our work. So how do we manage risk in field work. Understanding risks and hazards in our field operations tells us what type and kind of security we need. In some places armed guards may be required while a crew is on the job site; in other cases, nothing may be required. We are aware of risk, and make risk decisions many times per day. When you cross the street, scooting ahead of an oncoming car, it's a risk decision. When we meet a stranger on the street in a one on one situation, we also assess risk.

Physical Risk is the likelihood that there will be an event which will damage personnel or equipment on the site due to external sources. Physical risk can be either internal or external.

External Risk can be a vandal on the jobsite, or an errant vehicle destroying equipment, or an electrical storm creating a fire.

Internal Risk often occurs inside the organization from employees' actions or inactions, and it can include bad decisions, sabotage, blunders, fraud, misuse of company facilities, etc. Internal risks are also caused by violation of safety protocols, safety and industrial standards and practices. Sometimes internal risks are attributed to inexperience, ignorance, personnel/policy disagreements and management pressure to skip normal protocols for safety.

Cultural factors may influence our perception and recognition of risks and hazards. We can often recognize and minimize many physical risks such as robbery and other types of personal violence against a working crew—especially in the Third World. Cultural factors in the area of operations must also be considered, and their effect on operations evaluated for sensitivity to the culture in which they operate.

According to safety experts, disasters generally occur when there is a management climate which encourages shortcuts. Specifically, the prevalent theories of accidents and disasters follow a falling domino sequence, Illustrated below

Theories of accidents and causes[i]

BIRD and Loftus Theory of Accidents	Marcum's Theory of Accidents
Lack of control	Inadequate Preparation
Basic and Underlying Causes	Substandard Performance
Immediate Causes	Mis-Understood and Un-recognized Risk and Inadequate Preparation Against Risk
The Incident or Accident	The Incident or Accident
Losses and Casualties of Personal Property	Adverse Reaction to the Incident (Facility Damage and Associated Immediate Losses
	Sustained Losses (direct losses)
	Incurred Costs such as loss of reputation, loss of production, and quality associated or arising from the accident

[ii] *Sometimes: The scramble to assess blame or avoid responsibility follows and that's part of human nature…*

Sometimes we get luck and avoid problems: by way of example, an former academic who started his own air pollution consulting company, lacked industrial experience. But, because he had never dealt with OSHA,

and was not aware of the rules for confined spaces, he did not hesitate to send one of his employees into a manhole (confined space) to collect wastewater samples without proper evaluation of oxygen levels or provision for rescue in the event of a problem. Thankfully there was no harm done but the employee was counseled strongly by another senior engineer for allowing herself to be misused. Neither of them recognized the hazard, and no-one prepared for it.

OSHA does not apply to municipal and governmental entities. The potential for harm and disaster is there, but because government is exempt by statute, they often ignore OSHA and good safety practices, sometimes with fatal consequences. Private contractors working for the government entities must follow OSHA rules and provide "Safe Workplaces".

If a municipality performs the inspections on their facilities, but uses contract labor to facilitate repairs, the question of safety in the workspace arises. In one instance, the municipality operated and inspected lift stations, but subcontracted the maintenance and repairs. When a worker was severely injured due to an preventable equipment failure, the designation of responsibility for providing a "safe workspace" comes into sharp focus. Who is responsible for allowing a workman to enter a lift station which is unsafe? The courts must decide where the responsibility lies.

BP's Deepwater Horizons was at risk because safety protocols were bypassed, and the Chemical Safety Board video reviewed the causes, and found that the causes of this incident followed the accident causes factors (outlined above). Specifically, the operators at Deepwater Horizons were told to ignore safety protocols and were under pressure to cut drilling and exploration costs. The crew frequently shut down the explosive gas alarm because it was always ringing, indicating potential danger. Because of management pressure the drilling continued when it should have been stopped. The fire and explosion resulted in total destruction of the drilling platform, massive oil spill cleanup, ecological damage, and over 20 Billion dollars in cleanup costs and fines.

That is one very specific incident. If you are interested, go on Youtube.com and look up Buncefield, Piper Alpha, and Texas City disasters, along with Bophal, and Chernoby. The results are interesting and prove the point about the accident sequence outlined above. We will discuss them a bit below.

There are many other types of risks. Financial risk is often a major one governing our actions. When we go to the "bank" to get our project financed, or when we await a payment for work performed, those are also project risks—it is just that we often consider them differently. We also face personal risks from our decisions about how we manage our health and properties. Some of these risks are insured: others are "naked" risks, and often go unrecognized.

We beggar trouble when we don't inform ourselves about the consequences of our actions as a whole. When we fail to foresee the intended and unintended consequences of our actions and fail to foresee what the failure modes might be and their unintended consequences, we are inviting risk and potential catastrophe. Not what will go wrong, but what could go wrong?

Not to pick on the chemical industry, but they have some of the most spectacular and well documented accidents which illustrate the consequences of poor risk management[iii]. With good risk management, you may never hear about the collateral damage of an industrial accident.

In Bhopal, India, a Methyl Isocyanate release in 1984 was caused by ignoring good management practices and safety protocols. That release caused 2,259 immediate deaths and 558,125 injuries; many of the injured later died as a result of chemical exposure. Failure to maintain equipment, and the pressures to cut costs overrode the recognition of the need for protection of the community in in Bhopal[iv].

At the BP Refinery Fire and Explosion in Texas City, Texas (2005), careless operating procedures during a startup, poor maintenance, and bad risk assessment which allowed the positioning of a meeting trailer adjacent to a safety flare, caused about 20 fatalities. According to one source, the meeting trailer positioning occurred when someone made a decision that the trailer would be "largely unoccupied".

As a consequence of the Bhopal accident, Union Carbide, one of the US's premier chemical manufacturers, was broken up and sold to Dow Chemical. The chairman of Union Carbide also had an outstanding Criminal Warrant for murder issued by the Government of India. Executives of BP were reassigned.

Hazard release incidents can take place in landfills, drilling operations, construction operations, and anywhere else. How often have you heard of a drilling rig severing a utility line, with unexpected

consequences? In my own experience, I just missed drilling through an 3" diameter optical cable. The cost of repair would have been ruinous. The consequences from the cutting of a utility line depend upon what was being carried in the utility line.

Most major and minor incidents occur, not from a single event, but by a series of small failures which cascaded to produce a much larger incident. The professionals at the incident locations did not seek to create a problem, but the problem occurred because the consequences of the risk went unrecognized. The belief that we are "safe", and that accidents "couldn't happen here" are often at the root of safety failures leading to major incidents.

Almost every incident or accident is caused by multiple failures of safety protocols. Safety and security on job sites and in the office must become a religion which is practiced daily. Some might quarrel with the idea of a religious association to safety—but the basic idea is that consistent, repetitive reinforcement of safe practices and operations is necessary for a modern business. Anyone going into the "field" should be aware of the dangers associated with the work.

One tool which can help reduce accidents is Root Cause Analysis. Asking what can go "wrong" is always good policy before committing to a course of action. Root cause analysis is often applied in accident investigation to get at the fundamental cause of the accident rather than the apparent cause. It is often applied by asking, "What caused that?" 5 or more times in an investigation until the real root cause is identified.

2. WHAT IS RISK?

Risk is defined as the product of three variables:

Risk= Threat * Vulnerability* Assets at Risk

Risk is the effect and it can be monetized – by insurance or reparations for damages. Risk scenarios can be extremely detailed, or overly broad but are measured in relation to a specific set of vulnerabilities, threats, and assets.

Vulnerability is an estimate of the degree of damage or loss, which can be anywhere from zero to 100%. A fire which destroys 20% of the refinery or 40% of a drill rig, would have a vulnerability rating of 0.2 and 0.4 respectively. For humans, an injury associated with an incident might be up to 100% depending upon the injury or disability.

The threat can be location and weather dependent or it can be from sabotage or theft. Every item has some degree of threat associated with it. Threat is the method or area through which an "attack" or a problem can occur.

For environmental projects, you can assess the vulnerability of failure by percentages of goals to be reached, and the baseline cost of the most expensive remedial alternative available. If a remedial project is 75% complete through remedial technique, then the vulnerability is 0.25 when compared to the most expensive and/or most reliable alternative.

Suppose that you have a remedial action where you have a moderately expensive trailer on site. From one source, the risk of vandalism is 50% (ie: it has a 50:50 chance of being attacked), and if the attack is successful, the damage (vulnerability) to the trailer would be 40%, (meaning that we would have to spend about 40% of the replacement cost on the trailer to repair it). Now, the trailer replacement cost is $45,000. The risk due to vandalism --expressed in annual cost terms is:

$R_{vandalism}$ = 0.5*0.4*$45,000 or $9,000.00

Of course, that's for a 40% damage to the trailer. In a worst-case scenario, we might assume that the loss is total, and then the Risk would be $22,500.

Our project might have a Risk/Criticality Matrix which looks something like that shown below, with the exception that the table would be much more detailed and there would be several items and sub-items in each category in the description. This is shown in Figure 1.

In order to use the matrix with a single scenario, we might have to institute some controls or some defensive items into our budget.

The Improper Characterization Risk in Figure 1 should have a cost associated with it for a range of vulnerabilities. Each of the vulnerabilities should have a specific cost of deterrent or defensive items associated with them, so that minimum characterization might cost X, and in order to get it from Very High to High, the cost might increase to 1.5 X. In order to minimize the improper characterization risk the cost might be 4X and could reduce the vulnerabilities from 70% to 15%.

XYZ Remedial Project					
Criticality Ratings					
Description of Risks	**Vulnerability**	**Very High**	**High**	**Medium**	**Low**
Improper Characterization					
Method Failures					
Fire					
Weather/tornado					

Table 1: Typical Risk Management Matrix

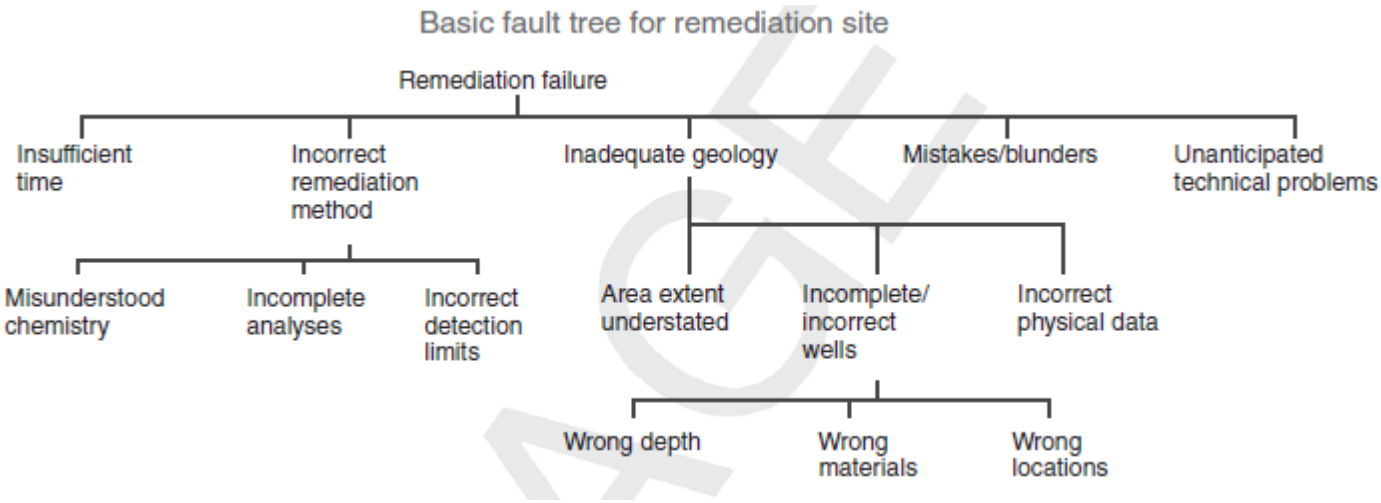

Figure 1: Basic Fault Tree for a remediation site

Other ways we can evaluate risk include Fault Tree Analysis and Risk Informed Decision Making. Fault tree analysis is slightly more mathematically intensive, where we analyze the probability of a failure (event) by analyzing each contributing factor, and making a binary decision on it, level by level, until we get to the top level or main event. Figure 1 illustrates a possible but very broad based Fault Tree for Failure of a Remediation Project. In order to be useful, the fault tree shown in Figure 2 would need substantial refinement before implementation, but it is useful for the purposes of concept illustration. Even for complex projects, Fault Tree Analysis is applicable[v].

The Fault Tree is probalistic. Each element has a numerical probability associated with it, and the probability of a specific event causing failure can be assessed. For example, in the table above, the probabilities for the elements leading into the element "Incorrect Remediation Method" must total 100% (expressed as 1.0) for the sum of the three elements. If there were an additional element such as "Mischaracterized soil type", it would have a probability associated with it as well. However, all the probabilities of the items leading into the "Incorrect Remediation Method" must still only total 1.0 for that branch[vi].

The Fault Tree Analysis is similar to RBCA (Risk Based Corrective Action) which is used by the regulatory community to evaluate public health risks against specific actions. In RBCA you are comparing Public Health Risks against occupational and other health-based exposure standards and criteria. In the skeleton of the FTA analysis shown above, you are looking at the entire project. The form of the equations are identical.

$RISK_{RBCA}$ =Concentration * Toxicity* Exposure

$RISK_{(Project)}$ =, Threat * Vulnerability * Assets

3. RIDM: Risk Informed Decision Management (NASA)

After the failures of *Challenger* and several other spacecraft, NASA developed a procedure for Risk Informed Decision Management. This is a consensus process, as shown in Figure 2.

The detailed level of planning required for RIDM may be uneconomical or impractical for smaller projects because RIDM planning requires boundaries to keep the discussions focused on the issues at hand.

The steps for the RIDM process are: **Identify, Analyze, Planning, Tracking,** and **Control.** It is a continuous process as indicated in Figure 3. Those familiar with the ISO Plan, Do, Act, Check management style will be familiar with RIDM. The RIDM steps are explained in more detail below.

3.1 Identification

The objective of identification is to make the site safer, better, or more environmentally friendly within the bounds of the available project scope and costs, and not to eliminate the last little bit of contamination, as it may be uneconomical to do so. Each element must have an associated risk, and the probability of the success or failure of the project is determined by one or more scenarios. It is the consequences of the risk scenario that defines the outcome. Alternative scenarios and multiple event scenarios may be equally likely, and should be included and identified for consideration.

Multiple inputs and activities are associated with project activity: some are routine, some internal, and some external. Many of these activities are addressed during the project design stage. A project analysis should include the likelihood of mischief and sabotage, and physical or electronic interference with remote locations or communications. It is important to consider the effects of any environmental or other effects from unplanned releases of chemicals, project upsets, or adverse situations.

Development of a complete risk scenario may require the involvement of other groups and departments, and their different perspectives and inputs should be encouraged. If the scenario involves the possibility of notification to, or assistance from outside parties, your group should have a "single entity" to provide contacts and coordination. [An example of this might occur if the scenario anticipates that the local emergency planning committee or the Fire Department or the Hospital may be involved.]

The scenarios considered should be realistic and grounded in practical considerations. If a scenario included weather delays or damage, and if it is located in Miami, it will not be shut down by a snowstorm, but might be affected by a hurricane.

3.2 Analysis

The analysis step requires the estimation of the magnitude and consequences of individual risk elements and working through scenarios to completion, and considering related costs *until the objective is achieved.* Production of a coherent incident analysis report is challenging because the unknowns are unknown and unknowable. The assessment of damage and costs is dependent upon perspective and experience of the analyst or analytical team, and where necessary should

involve equipment vendors to get accurate replacement cost data.

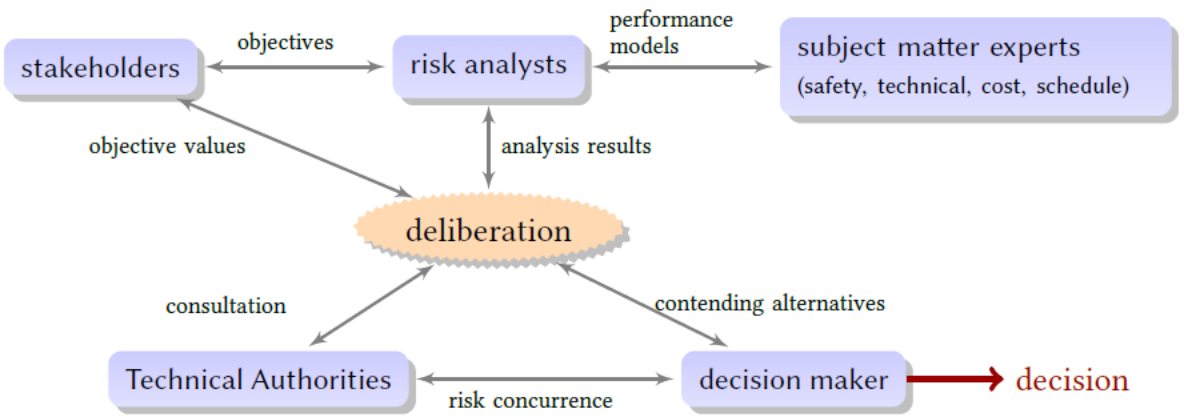

Figure 2: Risk Informed Decision Making Process (from NASA)

Figure 3: RIDM Process. Source: NASA

The preparation of a detailed cost estimate for a large project or installation can require substantial resources and time just to get within 25% of the actual cost, depending upon the level of detail required, the complexity of the or process, the assumptions implicit in the process, and the accuracy of the estimate required. The overall process of analysis includes several important elements:

- What can go wrong – or How can an can things go wrong?
- How big would the incident or problem be?
- What are the security systems to prevent, deter or defeat a specific incident, and
- What is the margin or reserve to prevent an incident or follow up?

3.3 Plan

The planning step is where the response to the incident scenarios is developed. In planning the manpower required for the type of response and should be specific to the scenario. This visualization exercise in requires detailed consideration of options both in response and remedy. Consider detection timing in your response plans and the speed with which an incident can occur or propagate.

Consideration of outside resources and their response times should be factored in the planning for scenario response. Determine what material, personnel and equipment is available for response, and how quickly it can be deployed, as it may be critical to limiting incident damage. Prepositioning resources for response may also be important to project success. Likewise consideration of the likelihood that outside resources (such as an ambulance transporting an injured employee to the hospital) may be contaminated by the employee's exposure to onsite chemicals. Decontamination protocols may be an important part of the scenario planning.

In most cases, the vulnerability or incident probabilities will be low, and the risks are probabilistic rather than actual[vii]. History is not much of a guide in this area. "It hasn't happened in X years," means little to current risk, especially where the procedure has been slightly modified. Disaster and incident probabilities are often very low; deciding between the likelihood of an event with a probability of 0.001% and 0.0001% is very difficult, but sometimes necessary. Make sure that your decision to ignore the low probability occurrence has been sufficiently addressed.[viii] Mother Nature can be a very nasty lady and wreak unexpected damage on a facility. Just make sure that you have proper safeguards in place for the wild event which will never happen.

3.4 Track

All risk decisions must develop a paper trail so that they can be examined and evaluated after an exercise, event or incident. The purpose is not to assess blame but to assess performance response. Planning meetings and documents should be captured and recorded as time stamped files, and documents should include video records and arrest records, invoices, and outside reports and possibly even news reports.

Periodic review and editing of the risk management plans is required. The Risk Management Plan should be documented in a r*isk management manual* which contains procedures and notification protocols. Site Managers, Contract Security, and Key Management Personnel must be trained and familiar with procedures developed. A minimum set of personnel qualifications and skill sets in the planning team should be developed and included in the Risk Management Manual. The *manual* does not need to be highly detailed, but it should be specific enough so that the Manager using it knows what actions to take, and what appropriate levels of force, response, and reserve are required. The procedures manual should also specify the qualifications, responsibilities, duties, and authority for each level of the Response Personnel.

Ideally, the *manual* and the scenarios should be reviewed on a periodic basis. Depending on the size of the plans and the complexity of the facility or the project, review may require monthly Manual review and updating. At a minimum, the Manual and the plans needs to be reviewed -- yearly. The universal limitation of the planning and Manual development is the inability to determine the timing of an incident. We don't know, what we don't know. Eternal vigilance is required for successful operation.

3.5 Control

Project control is more than following the policy Manual. The implementation of good practice and control is a daily exercise and requires commitment from the organization. Control is management, and it implies the use of common sense, and an attempt to meet commitments, even when they might be difficult to attain. Control is watching the project budget, and looking out for employees, and managing equipment and activities. Control also implies that the management will be providing necessary equipment and training to minimize the possibility of accidents and injuries.

3.6 Security

One aspect of managing environmental risk is physical site security. Physical site security extends to employees and equipment. When the workday ends, is the jobsite secure or vulnerable to vandals? Is the site secure from unwanted and unwarranted intruders? Is simple fencing enough to secure the site, or are armed guards necessary to meet the potential external hazard? Are there unauthorized people on the site, and how do you identify them. One chemical plant manager issued bright red hard hats only from his office. In the event of problems all employees were instructed to make sure that the visitors had been removed from the plant.

In the US, physical site security has a relatively low priority except in unusual situations. Recent events from the world-wide terrorist attacks indicate that attacks are often unanticipated. Not all attacks are designed as terrorism events. Where there is a remote possibility of an attack, additional security should be considered, especially if the client or the project is unpopular with the surrounding community[ix]. Situations have occurred where a drilling crew was assaulted and robbed during daylight. Also, if a crew or an employee is working in inside someone else's manufacturing operation of any type, or if it is working in another country, risk considerations should include emergency medical response and treatment, including medical evacuation and hospitalization if required. These precautions should be in place before the employees start work on the customer's site.

Working inside a company's jobsite, can be the equivalent of being in a foreign country, and the company medical staff and employees have no obligation to treat injured or burned contractors unless there is an agreement compelling them to do so[x].

4.0 SITE PHYSICAL SECURITY

Physical security on the jobsite is also a part of environmental risk. Fencing, boundary control, and of physical security are important to employees and project success. A snake under a drill rig can be just as dangerous as an intruder with a gun. A chain link fence is adequate for the perimeter of the work site, but it should have a bottom cable, stout fence posts and wire, a coil of razor wire on the top, and sensors and TV cameras to discourage intruders. Fencing barriers should use the US Army Manual on Physical Security (ATTP 3-39.-32). The Army Manual on Physical Security is very comprehensive, free, and can be downloaded from the Internet[xi].

For remote job sites, or where operations or equipment are unattended, consider communications and power reliability in the planning for site physical security. If cutting the power disables the security system, backup sources of power or other types of alarmed responses may be warranted.

Vehicles can penetrate security areas and create site havoc. Site entrances should be designed to slow speeding cars and trucks. An vehicle containing explosives is a separate security consideration because an explosion can cause concussive injury as well as injury from missiles and fragments. While the incidence of vehicle bombs may be unlikely in the US, political unrest or large public opposition to a specific project should address potential explosives damage and sabotage.

The terrorist or political activist is looking for maximum publicity for his cause, and that means selecting large, highly visible targets. Reduce your site visibility. A remote site is not high on a terrorist's target list unless there is substantial publicity associated with it. Clear definition of your work area, and boundaries with fencing is necessary for legal and safety purposes.

Afterword on Nano Materials and new Technologies

Increasingly nano materials and other new technologies are being introduced into the environmental marketplace. Nano materials are of special interest because they are new and operate at molecular levels. Because of their size, they may not be amenable to removal from waters by conventional technologies—but that remains to be

determined on a case by case basis. The use of nano-materials may pose a specialized risk—which needs to be evaluated prior to their use. Most often, we use nano-materials for a specific purpose, but as with any new technology, we frequently fail to evaluate the downside risks of escaped materials on the environment. The problem is that conventional treatment systems will not remove all the nano-materials, and because of their size, it would require membrane filtration to remove the materials from an effluent. The environment is not a place for experimentation, and we have done enough damage with microfine plastics such as Polyethylene. (Specific gravity 0.93-0.95 for LD and HD PE), and they are finding their way into the gills and flesh of fish, causing damage. The PE is marginally biodegradable and breaks into small particles of around 1-1.5µ M (approximately 0.000039 inches), and it is difficult to remove from the aquatic environment.

A nanometer is 1/1000 of a micrometer and operates on direct manipulation of molecules and atoms. While they cannot, as yet, reproduce by themselves, there is concern for "buckeyballs" and other by-products from nanotechnology. What the future will hold for this technology may represent a risk, as yet unformulated, and just maybe it is time to begin the regulatory control of nano-technology to prevent future incidents. It's better to be safe than sorry.

6.0Summary:

Risk comes in many forms. This presentation has discussed the consideration, calculation, and presentation of types of risk and damage which can occur during all types of normal operations. The components of a good risk management strategy consist of identifying , planning, tracking and controlling Physical, External, and Internal risks to a company or an operation.

Additional Reading for more information:

The subject of disasters and planning for responses is fascinating and complex. The following books should help, although they may not be precisely on the subject material:

1. What Went Wrong, 5th Edition: Case histories of Process Plant Disasters and how they could have been avoided, by Trevor Kletz, Butterworth Publishers 2009
2. The Black Swan: Second Edition: The impact of the highly improbable May, 2010 by Nassim Nicholas Taleb
3. Skin in the Game, by Nassim Nicholas Taleb, March 2018
4. Practical Wastewater Treatment, 2nd Edition, by David L Russell, PE
5. Modern Industrial Security in the 21st Century, by Col. Pieter Arlo, and David Russell

In addition, the UK Department of Labor has well developed tables on accidents and their probabilities Taleb's books are primarily about the stock market and his experiences on the trading floor, but if one can translate his experiences and apply them to real life, they are extremely useful. His last book, Skin in the Game, has a chapter at the end which discusses the mathematical basis for extreme events.

One final book which is very valuable in understanding complex systems and their failures is: Bak's Sand Pile by Ted G. Lewis. (2011) who is the Executive Director of the Center for Homeland Defense and Security at the Naval Postgraduate School in Monterey, California.

Endnotes

[i] Bird, Jr. F. E. and Loftus, R. G. *Loss Control Management* Loganville, GA. Institute Press (1976) and Marcum, C. E. 1978, *Modern Safety Management Practice*, Morgantown, WV, Worldwide Safety Institute

[ii] Not part of either author's original theories, but a practical commentary on the way things seem to work.

[iii] Thanks in part to the Chemical Safety Board and their analysis of accidents

[iv] This is well documented in many videos on http://www.Youtube.com

[v] Deepwater Horizon incident has a complete analysis of the incident in an fault tree. See the following websites:

http://www.bp.com/content/dam/bp/pdf/sustainability/issue-reports/Deepwater_Horizon_Accident_Investigation_Report.pdf

and

https://docs.lib.noaa.gov/noaa_documents/NOAA_related_docs/oil_spills/BP_report/appendices_AA_Z/Appendix%20I.%20Deepwater%20Horizon%20Investigation%20Fault%20Trees.pdf

[vi] Fault Trees are applied before a project is to be performed. An Event Tree is the reverse of a fault tree which is used to assess the problems which occurred where a failure has occurred after the failure event. A very significant event tree was prepared for Deepwater Horizion. It is found on the Internet at the following address:

https://docs.lib.noaa.gov/noaa_documents/NOAA_related_docs/oil_spills/BP_report/appendices_AA_Z/Appendix%20I.%20Deepwater%20Horizon%20Investigation%20Fault%20Trees.pdf

[vii] Examples of the foregoing are, 1) Probabilistic Risk would be a fenced in chemical facility on an remote island. It is reasonably secure from external attack. 2) Actual Risk would be a plant in a run-down, inner-city neighborhood where there is a lot of crime, and a history of vandalism, and organized and random robbery and theft. The risk factors are much much higher for some type of attack or break-in.

[viii] Suggested reading is, "The Black Swan" by Naissem Nicholas Taleb. It is both entertaining and informative, and while it is primarily about financial risk, the application to environmental risk is applicable.

[ix] For example, in areas where there is extreme poverty and in some foreign countries, armed guards may be necessary. The author has worked on sites in South America where armed guards were an absolute necessity due to the possibility of robbery and or kidnapping from FARC Drug Cartel.

[x] The author had an experience in South Georgia inside a paper plant where a co-worker who was also a contractor, was burned and needed medical attention during the swing shift. Fortunately, the paperwork for emergency treatment was in place, but the night medical crew did not get the message, and there was a delay in getting the employee treated.

[xi] The Internet Address is: https://fas.org/irp/doddir/army/attp3-39-32.pdf and it is a public document