Safety Shortcomings in Tankers, related Marine Terminals and Tank Farms

Submission to the Tanker Safety Expert Panel

James Ronback, P.Eng, System Safety Engineer (retired), Delta, B.C., June 18, 2013

Executive Summary:

In spite of the questionable financial viability [56, 57, 58] and promised economic gains to the oil and natural gas industries owned by foreigners like the Chinese, Malays and Americans exploiting the Canadian tar sands and fracking our natural gas reserves, and due to our federal government's indifference to climate change, I am adamantly opposed to the resultant increased hazardous tanker traffic that has inadequate safeguards for transporting dangerous and noxious cargoes. This increased hazardous tanker traffic demands excessively high societal and environmental risks [39, 40, and 55] that are not tolerable in the event of a major spill, fire or explosion.

With the ever increasing size of supertankers and LNG (liquefied natural gas) carriers and their reduced manoeuverability, the greater amount of hazardous stored energy within them, increases the impact of undesired consequences during a major incident. With a single engine these ships are only one failure away from a major catastrophic event due to loss of power and steering, especially in heavy seas.

If an explosive condensate or natural gas air fuel vapour cloud spill ignited [76] on a large tanker or a LNG carrier, the conflagration would be horrific. With a LNG carrier with 266,000 cubic meters of LNG, or at a LNG tank farm at a liquefaction station, the worst case explosion [75] of all the stored energy at 5.9 PJ (Petajoules) ($5.9 * 10^{15}$ joules) would be significantly more than the Hiroshima atom bomb [74] that had 0.06 PJ of stored energy released in its potential devastation [72, 73]. So it behooves me, that even though I do not approve of these hazardous tankers and their dangerous cargoes, as an engineer wearing an iron ring, I must warn our national regulators and the oil and gas, and tanker industry operators of their System Safety shortcomings.

The people of BC and elsewhere in Canada are faced with pushy and arrogant oil and natural gas production and transportation industry leaders who are out to conquer our three coasts, come hell or high water, deploying hazardous supertankers and LNG carriers. Notwithstanding that, I offer, without prejudice, my observations and ten recommendations, for your consideration on the System Safety aspects of Tanker Safety and the related marine terminals and tank farms.

These recommendations address: System Safety Policy and Management; Safety Plan Guidelines; Capability to withstand Rogue Waves; Fail-safe and Resilient Design; Mandatory twin screws with

Independent engines for ships with hazardous cargoes; Backup navigational systems on LNG carriers; tankers and tugs in case of loss of GPS; Risk Based Marine and Land use Studies; Functional Safety Integrity level; Risk Informed Safety Case; and Increased Separation for hazardous ships.

Overall, an enhanced and more comprehensive System Safety Management by ship owners and terminal operators that addresses the above concerns would make the transport of hazardous and dangerous goods less risky within Canada's coastal waters. The related tanker and LNG carrier traffic, and offloading and storage at the marine terminals and tank farms implementing these recommendations would make it less risky for the vulnerable human communities and the coastal and estuary environments that are potentially impacted by tanker or LNG carrier spill, fire or explosion incidents.

1.0 Introduction

Safety is freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment [38].

Whereas: **"Risk is a consequence of dependence**. Because of shared dependence, aggregate societal dependence on the fossil fuels is not estimable. If dependencies are not estimable, then they will be underestimated. If they are underestimated, then they will not be made secure over the long run, only over the short. As the risks become increasingly unlikely to appear, the interval between events will grow longer. As the latency between events grows, the assumption that safety has been achieved will also grow, thus fueling increased dependence in what is now a positive feedback loop. Accommodating rejectionists preserves alternative, less complex, more durable means and therefore bounds dependence. **Bounding dependence is the core of rational risk management." (**Paraphrasing Dan Gear [63]).

From a safety perspective, one must always try to look for alternative solutions that minimize the worst case consequences. Also one needs to take a long term view to see what solutions to our world-wide energy demand will result in fewer deaths. For example, large-scale expansion of unconstrained natural gas use would not mitigate the greenhouse gas emissions and would cause far more deaths than expansion of nuclear power [68].

Effective safety management is almost non-existent amongst the marine terminal operators and ship owners that provide carriers and super tankers for transporting hazardous cargo like LNG, dilbit and condensate/ naptha and jet fuel. There is a distinct lack of a clear Safety Policy, Safety Management System and quantifiable Safety Goals required by Canadian regulations. For example, these safety aspects are not found in the Enbridge or Kinder Morgan proposals for tanker traffic despite their constant media blitz campaign assuring the public that everything is under control.

The shipping industry and terminal operators need to show us how they behave when no one is watching [4, 38].

> **<u>Recommendation 1</u>: LNG carrier and tanker owners and operators must provide a comprehensive Safety Policy, Safety Management System and a System Safety Plan with demonstrable Safety Goals that are available for public comment.**

Unfortunately, Transport Canada only provides limited guidance in their Safety Plan guidelines. It is incomplete, in that it is mainly geared to workplace safety and it does not address designing for safety. It gives guidance on providing protection against hazards by invoking workplace safety and health

standards and regulations but it does not attempt to show how to quantify the risks in order to make risk informed decisions on safety.

Probabilistic risk studies are required for natural and marine[1] hazards, e.g., monster freak waves [69], earthquakes and landslides, etc. In the case of earthquakes and related landslides and tsunamis, these studies may be suspect since: "Hazard maps tend to underestimate the likelihood of quakes in areas where they haven't occurred previously" [25]. The accuracy of freak wave prediction is still very limited as to their likely occurrence [79]. These rogue waves that come out of nowhere can be more than 30 meters high. Are the super tankers and LNG carriers designed to handle this massive wave load?

Severe weather has sunk more than 200 supertankers and container ships exceeding 200 metres in length during the last two decades. Rogue waves are believed to be the major cause in many such cases [70]. Rogue-wave prone sea states can actually occur more often than once in the 25-yr period, which is currently used as a return period for ship design [71].

There seems to be an aversion by tanker owners and operators of marine terminals and tank farms to conducting quantitative risk assessments for industrial hazards on land. For example, the marine terminal and tank farm at the Kitimat Terminal contains 243,000,000 liters of highly volatile, flammable and toxic condensate in three tanks. Thus the "experts" are severely underestimating the consequences of the critical hazards of their project.[2] The vulnerability of a supertanker unloading condensate near this tank farm is immense in the event of a major incident. You do not want any other ships within 5 kilometers.

I strongly advise that the Tanker Safety Expert Panel recommend that Transport Canada and the National Energy Board (NEB) both diligently make use of the NASA System Safety Handbook [38]. It goes beyond looking only at hazard analysis techniques. It includes probabilistic risk analyses as well. The goal of the analysis is to develop a scenario based understanding of the system's safety performance in order to:

1. Identify the most critical scenarios that can lead to undesired consequences.
2. Identify the items that increase risk to make the scenarios critical.

[1] See the probabilistic studies as recommended by the voluntary TERMPOL team [48] for the marine environment, for which extensive probabilistic studies done by Det Norske Veritas on navigational (Technical Data Report, Marine Shipping Quantitative Risk Analysis, 2010) [49] and spill risks (TERMPOL Study 3.15: General Risk Analysis and Intended Methods of Reducing Risk, April 2010) [50] and by the Bercha Group on explosive vapour cloud modeling [51].

[2] More people have been killed by tank farm and pipeline accidents than by North American nuclear power station accidents. No one was killed by radiation in the Fukushima nuclear power tsunami incident.

3. Ensure that the controls (barriers or active controls) are directed towards the risk contributors.

Hazards refer to the causal factors of accident scenarios, whether direct or indirect, primary or contributory, or latent.

As such, the proponent's system safety activities should not duplicate those system engineering processes that have the potential to affect safety [38]. They should be done at arm's length.

> **<u>Recommendation 2</u>: The lack of adequate Safety Plan Guidelines from Transport Canada for tankers, including LNG carriers, marine terminals and related tank farms needs to be rectified and go beyond hazard-centric thinking, as soon as possible, before any project is allowed to proceed.**

2.0 Reliability versus Safety

One must not confuse reliability goals with safety goals. You can easily have a very reliable system that is not safe. When it does fail rarely, the consequences can be catastrophic. Conversely, one can have a very safe system that is unreliable but it always fails safe and causes no harm.

To make a system more reliable you can increase the design margins of the hardware components to withstand more physical stress, such as monster wave heights and earthquakes. But increased design margins alone will not make the system fail-safe.[3] Extraordinary development and verification effort is required to provide the evidence that shows that the entire system, including management, and the computer control system is sufficiently robust, resilient and tolerant to system failures, including human errors, to satisfy the safety claims.

> **<u>Recommendation 3</u>: Ships carrying hazardous cargo, such as tankers and LNG carriers, must be designed to withstand several worst case 10,000 year rogue, TBD (30) meter, waves and wave load that can occur in their 25 year design life.**

Navigation of the jet fuel/ dilbit/ condensate/ LPG tankers and barges to the marine terminal aided by tugboats is extremely tricky. It is subject to the vagaries of the tides, swift river currents, winds, fog, floating debris, loss of propulsion by the tugs or other river traffic and the potential loss of GPS signals [64, 65] due to interference suggests that serious collisions will occur in the operational lifetime of this

[3]While controlling the system by using computers, sensors and safety critical software in the control loop you cannot rely alone on increased hardware design margins, especially with digital processing in the safety critical hardware and software control loop together with man-machine interfaces [22],

project. The marine safety aspects of the loss of GPS for navigation and on board machinery such as single engines or steering need attention by the regulators.

For example, if there is a collision on the river with a LNG carrier, jet fuel tanker or barge, or an accident at the loading dock, e.g., hose/ pipe/ connection failure or a lightning strike [66] or a small plane crashing into the tank farm, or a disgruntled anti-pipeline radical using dynamite as a backhoe; and the highly flammable fuel catches fire and spills onto the water and land, what can be done to control the spreading of the fuel fire and prevent any secondary fires [67]?

3.0 Critical Safety Goals

A **critical safety goal that is missing** is the requirement that all catastrophic failures must be at least two failures away from happening. By catastrophic, I mean - loss of human life or permanent disability; loss of a major system; loss of ship or supertanker; major spillage; loss of LNG, oil or condensate storage facility; loss of a system control center; severe environmental damage.

A glaring example of a missing critical safety goal is the fact that most of the current worldwide oil and condensate supertanker fleet typically have only one engine. Thus each one is only one failure away from being adrift or floundering.

> **<u>Recommendation 4</u>: The control system for the LNG carriers, tankers, tank farm, marine terminal and control room should be designed to fail safe. They must be at least two failures away from a catastrophic hazard, and tolerate loss of an external electrical power and communications for at least two weeks.**

Machinery failures are an important cause of tanker spillages.

Worldwide we are experiencing over 5000 total loss of power casualties per year. If the single engine is disabled, a tanker without power and steering will become a drifting hazard and may eventually run aground or collide with other ships or tankers, resulting in a major spill.[4]

[4] "Worldwide we are experiencing over 5000 total loss of power casualties per year." [2008 Tanker Loss of Power Casualties, Jack Devanney, www.c4tx.org] [33]. "The current large (over 10,000 tonne deadweight) worldwide tanker fleet is experiencing at least two full losses of power or steering per day, and probably more than ten. If this fleet were twin screw, properly implemented, this number would be cut by a factor of one thousand." [The Argument for Twin Screw Tankers, Jack Devanney, Center for Tankship Excellence, USA, djw1@c4tx.org, September 20-21, 2007 http://www.martrans.org:8093/symposium/papers/Track%20A/A11%20devanney.pdf] [34].

For example, the Enbridge Tanker Acceptance Program (TAP) does not address the need for twin screws/ propellers to mitigate the ships from floundering, colliding or grounding due to machinery failures [35, 36, 37 and 52]

> **<u>Recommendation 5</u>: To increase tanker safety on Canada's coasts and waterways, the Transport Canada and NEB must require that all ships carrying hazardous cargo such as, but not limited to, LNG, jet fuel, crude oil and condensate in carriers or tankers or supertankers sailing in Canadian waters or visiting Canadian ports must be of twin screw design with two independent engines**
>
> **<u>Recommendation 6:</u> Ships carrying hazardous cargo must have an effective backup navigational system in case of loss of GPS**

4.0 When is it safe enough?

To conclude that a system is adequately safe [41], it is necessary to consider a set of safety claims that derive from the safety objectives of the organization. The safety claims are developed from a hierarchy of safety objectives and are therefore hierarchical themselves. Assurance that all the claims are true within acceptable risk tolerance limits implies that all of the safety objectives have been satisfied, and therefore that the system is safe. The acceptable risk tolerance limits are provided by the regulatory authorities, e.g., NEB, Transport Canada, who must make the decision whether or not to proceed to the next step in the life cycle. These tolerances are known as the decision maker's risk tolerances.

"In general, the safety claims address two fundamental facets of safety:

1) Whether the required safety thresholds or goals have been achieved, and

2) Whether the safety risk is as low as possible within reasonable impacts on cost, schedule, and performance.

The latter facet also includes consideration of hazard and controls (barriers and active controls) that are collective in nature (i.e., they apply generically to broad categories of risks) and thereby provide protection against unidentified or uncharacterized risks.

The demonstration that all the claims[5] are true within the decision maker's risk tolerance comprises what is referred to as a Risk-Informed Safety Case (RISC)" [38].

[5] "To avoid confirmation bias and compliance-only exercises, assurance (safety) cases should focus not on showing that the system is safe but in attempting to show that it is unsafe [62]. It is the emphasis and focus on identifying hazards and flaws in

5.0 Lack of risk based planning for industrial hazards

The appropriate use of land is an enormously effective way of reducing the impact of hazards on communities. That is why for industrial hazards we must require Risk Based Land Use Assessments to be done to control or eliminate incidents with societal risks [7, 8] that have very high consequences on the surrounding communities like Hartley Bay and its ecosystem.

For example, the marine terminal and its tank farm at the Kitimat terminal will have 11 tanks for oil and three tanks for condensate. Condensate is similar to naphtha, e.g., the white gas used in Coleman stoves and lamps. Each tank can store 78,000 cubic meters or 78,000,000 liters. The volatile condensate or naphtha has a flash point below minus 5 degrees Celsius. It can be as low as minus 20 degrees Celsius.

Methane, which is the main component of LNG, has a flash point of minus 187.8 degrees Celsius [76].

Considering that many storage tank accidents are found worldwide [14, 40, 77], it is very disturbing that NEB or Transport Canada does not require companies, like Enbridge or Kinder Morgan, to use any risk based land use assessments or vapour cloud modelling or leak prediction to determine the impact of the critical hazards on their tank farms and terminals and their surroundings. In particular, it is not being done for the three giant tanks containing highly volatile, flammable and toxic condensate that is unloaded at the Kitimat terminal via condensate supertankers and stored in a large 200+ million liter condensate tank farm. This facility is near a fragile marine environment and a heavily used marine waterway. Nowhere in the federal CEAA's or NEB's, Transport Canada's environmental review processes, is the risk of a fuel air vapour explosion blast and fire on the tank farm being properly evaluated for these proposed projects.[6]

Unfortunately explosive fuel vapor cloud modelling has not been done for the condensate tank farm since NEB has not invoked such a requirement. This is a serious omission since a tank farm fuel air vapour explosion blast puts a supertanker at risk, especially one that is transferring condensate or LNG.

Looking at the horrific tank farm explosions, fires and pollution that have recently occurred in Miami, Florida (19); Lamesa, Texas (20); Buncefield, UK (12); Jaipur, India (21) and elsewhere (24), I find it

---

the system that provides the "value-added" of system safety engineering. The system engineers have already created arguments for why their design is safe. The effectiveness in finding safety flaws by system safety engineers has usually resulted from the application of an opposite mindset from that of the developers." [61].

[6] A condensate vapour cloud blast modeling [51] was done for the Kitimat marine terminal and in the narrow channel for condensate supertanker grounding and collision incidents because it was recommended by TERMPOL.

unbelievable that a risk based land use planning and assessment and vapour cloud modelling for this critically hazardous tank terminal has not been done.

Risk based land use planning must go beyond natural hazards, e.g., landslides, earthquakes, floods, etc., and tackle the related industrial hazards as currently done in the UK, EU and California in Los Angeles [9, 19, 20, 21, 28]. Current practices used for health and safety on industrial sites are typically limited to protection against the hazards or the consequences without necessarily assessing the risk.

It is not safe to ignore the enormous impact of an explosion of a critical mixture of condensate fuel vapour and air, that can flash and explode at a temperature below -5°C and as low as -20°C depending on the condensate mixture. In this case, deliberate ignorance is potentially a crime [16].

The combined stored combustible and explosive energy in the 200 million liter condensate tank farm and a supertanker unloading condensate at the marine terminal is equivalent to **more than two million tons of TNT.** [7]

The impact of an uncontrolled fuel-air vapour explosion like the one that occurred at the tank farm in Buncefield, UK in 2005 was horrific [3, 4, 6].

The fuel in a vapour cloud mixes with atmospheric oxygen. The huge cloud of fuel flows around objects and into structures. When ignited the blast wave destroys unreinforced buildings and equipment and kills and injures personnel.

Fuel-air blast explosions kill or injure in several ways: with the blast wave; with flying debris or by collapsing buildings; and by the blast wind throwing bodies against the ground, equipment, structures, berthed supertankers and other stationary objects.[8]

[7] The nearby area surrounding an exploding and burning tank farm and condensate supertanker, would be devastated by the searing radiant heat, flammable gas cloud, blast overpressure and flying debris [28]. The recent horrific fuel air explosions and fires in tank farms worldwide and the use of Hellfire weapons [15] are a testament to the awesome power resulting from accidental unconfined condensate vapour cloud explosion and fire.

[8] The fuel-air blast's fatal mechanism against living targets is unpleasant. The pressure wave, and especially the subsequent vacuum, that ruptures the lungs will kill people [1]. If the fuel burns violently but does not detonate, victims will be severely burned and may also inhale the burning fuel [15]. People near the ignition point are almost always obliterated. Those at the fringe are likely to suffer many internal injuries, including burst eardrums and crushed inner ear organs, severe concussions, ruptured lungs and internal organs, and possibly blindness. Some may suffer for several seconds or minutes while they suffocate.

This kind of horrific explosion and conflagration is an unacceptable risk for human and ecological communities along Canada's coasts and waterways.

Providing buffers between the tanker, the tank farm and marine terminal may not be enough. A condensate vapour cloud can result from any number of one or more causes, e.g., an operator error, hardware [59] or software [60] failure, or leak during an earthquake. Its ignition will result in a very powerful explosion that can rupture many other tanks. The blast wave, fire and the oil and condensate spill will spread over land and water and greatly extend its zone of risk to the surrounding workers, population and ecosystem.

> **Recommendation 7: A risk-based marine and land use study that examines the possible worst case impact of a fuel air vapour cloud explosion's blast wave and fire on a LNG carrier, tanker, marine terminal and tank farm must be done for each project [8].**

Given their susceptibility of being hacked, using the Internet for remote control has no place for safety critical infrastructures [63].

> **Recommendation 8: The tanker, tank farm and marine unloading facility's control system and instrumentation must be built and operate at the highest IEC Safety Integrity Level (SIL 4) or its equivalent for its functional safety [45, 46].**

> **Recommendation 9: A Risk Informed Safety Case must be provided before any risk informed decision can be made by the regulatory agencies, the public needs to know what level of risk of fatalities, injuries and damage to the ecosystem is deemed acceptable by the regulators and to the surrounding communities [41].**

> **Recommendation 10: Ships carrying hazardous cargo with more than TBD (2) Petajoules of stored energy must maintain a separation of TBD (5) kilometers from all other ships at sea and communities on land.**

The Halifax explosion, on December 6, 1917, was equivalent to roughly three kilotons of TNT. Over 1,500 people were killed instantly while 9,000 were injured. Over 12,000 buildings within a 16-mile radius were destroyed or badly damaged [23]. The energy Enbridge proposes to store in the three condensate storage tanks of the Terminal is over 800 times the energy released in Halifax.

7.0 Conclusion

The requirements for the tanker owners' and operators' and marine terminal and tank farm facility operators' System Safety and Risk Management System must go beyond the normal accident and high reliability mentality [17, 32]. Individual components of the system may be very reliable but their interactions may cause harm. The regulations must also deal with the complex man-machine computer interfaces and interactions used for this remotely controlled and safety critical hazardous cargo, e.g., LNG, condensate, jet fuel, etc., and their transport and storage system.

The Tanker Safety Expert Panel needs to ensure that the risk of accidents and operator errors causing fatalities and injuries anywhere on any project and to the surrounding communities is reduced to a level as low as reasonably practicable. The extremely high consequences of a fuel vapor cloud explosion demands that working or living near the condensate tank farm while a condensate supertanker is unloading, should be as safe as living or working next to a nuclear power station [18]. So far, it is not.

The above recommendations are designed to address some tanker safety shortcomings but even if they are addressed by the Tanker Safety Expert Panel, I feel this review exposes the world's environment to the impacts of society's exploitation of yet more fossil fuel in the long run. It will incrementally damage our environment. That will of course include the health of the very ocean the LNG carriers and supertankers pass over, as well as the rising temperatures of the waters in the streams and rivers. Oil and Gas companies claim that they can protect them from tanker and LNG incidents and spills. But I do not trust them.

I do not want to see our coastlines, rivers and estuaries deteriorate for salmon populations as a result of our fossil fuel exploitation and transportation to new Asian markets. The overall cumulative environmental and societal impacts of the related project still are not addressed in the environmental assessments. It is not a question of -- are accidents going to happen? --- But when the accidents do happen, can we and our ecosystem survive with these additional risks and inevitable cumulative impacts to our rivers and coastal ocean environment? Its wealth of natural renewable resources must be available for future generations to enjoy and above all to continue make life possible on this planet.

"Large-scale expansion of unconstrained natural gas use would not mitigate the climate problem and would cause far more deaths than expansion of nuclear power."[68]

Alternately, in addition to promoting carbon free renewable energy solutions, such as solar energy, wind and tidal power, we also need to develop the use of nuclear power within all provinces and territories in

Canada to satisfy our 24/7 base load demand. This diversity of energy sources will help to mitigate the consequences of global warming reduce future mortalities and eliminate the unintended consequences of exporting LNG and dilbit and its concomitant rise of greenhouse gas emissions.

It is up the Tanker Safety Expert Panel to propose to the Government of Canada sufficient and necessary changes needed by the Canadian regulators, to ensure that the ship and terminal owners and their crews and pilots provide due diligence and compliance required for the system safety of tankers and LNG carriers and the protection of human lives and the environment.

Yours safely,

Jim Ronback, P. Eng. (retired System Safety Engineer)

1530 Kirkwood Road,
Delta, BC
V4L 1G1
Home: (604) 948 1589, Cell: (778) 668 1589, Jim_Ronback@dccnet.com

Biography

Jim Ronback, B.A.Sc., E.E. (University of Waterloo) P. Eng. (retired), lives in Delta, BC. He has worked as a software developer for flight simulators at CAE Electronics Ltd.; Product Assurance engineer for digital telephony at Bell Northern Research; Software Quality Assurance manager at Northern Telecom HQ, Advisory Product Assurance Engineer at IBM Don Mills Lab. He served as the Canadian representative on the International Electrotechnical Committee, TC 56 on Reliability and Maintainability, and was the founding Secretary of WG 10 on Software Reliability Aspects. As a System Software Safety Engineer, he provided safety and hazard analyses and mitigation on several safety critical projects including: the Ontario Hydro's Darlington Nuclear Power Station's Safety Shutdown System (consultant); Canada Arm II used on the International Space Station (SPAR Aerospace); the Brake Assurance Monitor for the Kuala Lumpur light rail train (consultant); and the comprehensive Safety Cases for Canadian Advanced Air Traffic Control System (CAATS) and MAATS, the military version (Raytheon). Jim is a Director of VAPOR, www.vaporbc.ca , Delta Naturalists Society and Boundary Bay Conservation Committee.

Ronback & Associates,
1530 Kirkwood Road,
Delta, BC
V4L 1G1 Tel: +1 604 948 1589 Jim_Ronback@dccnet.com

References

1) Lung injuries are particularly difficult to diagnose and treat.
http://www.hrw.org/en/reports/2000/02/01/backgrounder-russian-fuel-air-explosives-vacuum-bombs

2) "The cause of the (Buncefield) explosion seems to have been a fuel-air explosion of unusually high strength. The British Geological Survey monitored the event, which measured 2.4 on the Richter scale."
http://en.wikipedia.org/wiki/Buncefield_fire

3) "It blew out huge office blocks which would have held hundreds of workers, had the accident not happened at 0600 GMT on a Sunday.
... More than 600 firefighters fought the inferno which lasted for three days.
... At the time, the oil industry insisted its safety record was excellent."
http://en.wikipedia.org/wiki/Buncefield_fire

4) "A report published in February 2011 concluded that fundamental safety management failings were the root cause of the disaster."
http://www.hse.gov.uk/news/buncefield/index.htm .

5) Buncefield: Why did it happen?
http://www.hse.gov.uk/comah/buncefield/buncefield-report.pdf

6) Buncefield Investigation Board publishes Final Report, 11th December 2008
http://www.buncefieldinvestigation.gov.uk/

7) This report sets out recommendations concerned with land use planning around high-hazard industrial facilities regulated under the Control of Major Accident Hazards Regulations 1999 (COMAH) and addresses the related concept of societal risk. The recommendations are made by the independent Investigation Board, chaired by Lord Newton of Braintree, set up to supervise the investigation into the explosions and fires at the Buncefield oil storage depot, Hemel Hempstead, Hertfordshire on 11 December 2005. AN IMPORTANT DOCUMENT
http://www.buncefieldinvestigation.gov.uk/reports/comahreport3.pdf

8) Illustrative model of a risk based land use planning system around petroleum storage sites:
Buncefield Major Incident Investigation Board, Rev 0, 6 June 2008 by DNV Energy
http://www.buncefieldinvestigation.gov.uk/reports/dnvenergy.pdf

9) THE UK APPROACH TO LAND USE PLANNING IN THE VICINITY OF CHEMICAL MAJOR HAZARD INSTALLATIONS, TOM MADDISON, Health and Safety Executive (HSE) 2010
http://www20.gencat.cat/docs/interior/Home/MS%20-%20Institut%20de%20Seguretat%20Publica%20de%20Catalunya/03%20ambits%20dactuacio/Recerca/Grups%20de%20recerca/2010/Grup%20de%20recerca%20sobre%20risc%20i%20territori/HSElup.pdf .

10) MIA Fuel Farm Explosion Exposed, April 14, 2011 11:22 PM
http://miami.cbslocal.com/2011/04/14/i-team-mia-fuel-farm-explosion-exposed/ .

11) Slow motion of tank farm explosion in Lamesa, Texas.
http://www.youtube.com/watch?feature=player_embedded&v=6qcrwNM74sg
http://daviddrummond.com/blog/2009/05/15/lamesa-tx-tank-battery-fire-explosion/

12) Half a million people evacuated as deadly fire rages through Jaipur oil depot
By Mail Foreign Service - UPDATED: 09:57 GMT, 1 November 2009
http://www.dailymail.co.uk/news/article-1224018/Five-killed-150-injured-massive-rages-Indian-oil-depot.html .

13) Environmental impacts of the fire in Indian Oil Corporation Depot, Sitapura, Jaipur
http://210.212.96.131/rpcb/ReportsAndPaper/Report_on_Environmental_Impacts.pdf .

14) A study of storage tank accidents
James I. Changa, Cheng-Chung Lin, Journal of Loss Prevention in the Process Industries 19 (2006) 51–59
http://xa.yimg.com/kq/groups/3862917/1523127472/name/%2525EE%252580%252580StorageTank%2525EE%252580%252581FiresStudy.pdf .

15) British Military Using Hellfire Weapons in Afghanistan
Posted by Paul Fiddian on 23/06/2008 - 17:51:18
http://www.armedforces-int.com/news/british-military-using-hellfire-weapons-in-afghanistan.html .

16) Legal definition of DELIBERATE IGNORANCE
http://www.lectlaw.com/def/d036.htm

17) Beyond Normal Accidents and High Reliability Organizations:
The Need for an Alternative Approach to Safety in Complex Systems
Karen Marais, Nicolas Dulac, and Nancy Leveson, MIT, March 24, 2004
http://www.cs.st-andrews.ac.uk/~ifs/Teaching/Socio-tech-systems(LSCITS)/Reading/BeyondNormal%20AccidentsAndHROs.pdf .

18) "Enhancing Reactor Safety in the 21st Century - U.S. Nuclear Regulatory Commission" July 12, 2011
http://pbadupws.nrc.gov/docs/ML1118/ML111861807.pdf page 2.

19) Policy & Approach of the Health & Safety Authority to COMAH Risk-based Land-use Planning (19 March 2010), HSA
http://www.hsa.ie/eng/Your_Industry/Chemicals/Control_of_Major_Accident_Hazards/Approach_to_LUP_under_Comah_Regs.pdf

20) Land-use planning guideline - European Commission
http://ec.europa.eu/environment/seveso/pdf/landuseplanning_guidance_en.pdf .

21) GUIDANCE ON LAND USE PLANNING AS REQUIRED BY COUNCIL DIRECTIVE 96/82/EC (SEVESO II).
http://ipsc.jrc.ec.europa.eu/fileadmin/repository/sta/mahb/docs/LandUsePlanning/EUR18695EN_LandUsePlanningGuidance.pdf .

22) A. L. Juarez-Dominguez, J. J. Joyce and R. Debouk, Feature Interaction as a Source of Risk in Complex Software-intensive Systems, 25th International System Safety Conference, Baltimore, 13-17 August 2007.
http://www.criticalsystemslabs.com/docs/JuarezFinal_ISSC2007.pdf .

23) "The energy released was equivalent to roughly three kilotons of TNT (about 1.26 × 10^13 joules). ... Over 1,500 people were killed instantly while 9,000 were injured.
Every building within a 16-mile radius, over 12,000 in total, was destroyed or badly damaged."
Halifax Explosion
http://en.wikipedia.org/wiki/Halifax_Explosion .

24) British Military Using Hellfire Weapons in Afghanistan
Posted by Paul Fiddian on 23/06/2008 - 17:51:18
http://www.armedforces-int.com/news/british-military-using-hellfire-weapons-in-afghanistan.html .

25) "Hazard maps tend to underestimate the likelihood of quakes in areas where they haven't occurred previously. … Although bad luck can mean that quakes occur in places with a genuinely low probability, what we see are too many 'black swans,' or too many exceptions to the presumed patterns."
“Why earthquake hazard maps often fail and what to do about it”, by: Seth Stein et al, Tectonophysics (July 2012), doi:10.1016/j.tecto.2012.06.047.
http://www.earth.northwestern.edu/people/seth/Texts/mapfailure.pdf
http://phys.org/news/2012-08-earthquake-hazards-deadly-flaws.html

26) "Enhancing Reactor Safety in the 21st Century - U.S. Nuclear Regulatory Commission" July 12, 2011
http://pbadupws.nrc.gov/docs/ML1118/ML111861807.pdf page 2.

27) Kerosene type BP Jet A-1 has 43.15 MJ/kg and a density at 15 C is 804 kg/m3.
http://en.wikipedia.org/wiki/Aviation_fuel .

28) RISK ANALYSIS OF LADWP MARINE TANK FARM
http://www.portoflosangeles.org/EIR/WilmWaterfront/DEIR/Appendix_G.pdf .

29) "Flammability depends on many factors: Ignition source (energy, temperature); Fuel state (vapor versus mist, mass loading); Turbulence; Temperature; Pressure
... Flash point is not a useful characterization of explosion hazard" page 20
EXPLOSION OF AVIATION KEROSENE (JET A) VAPORS
http://www2.galcit.caltech.edu/EDL/projects/JetA/reports/EX_20F.PDF .

30) Videos of Miami Jet Fuel Tank Farm Fire on March 24, 2011
http://www.youtube.com/watch?v=m7Mu4fJaLUo&feature=player_embedded .
http://www.youtube.com/watch?v=sXYBsuhB6u0&feature=player_embedded .
http://www.youtube.com/watch?feature=player_detailpage&v=2uiSIQHkLEU .

31) Recommendations on the design and operation of fuel storage sites
http://www.endress.com/eh/central/info/resource.nsf/imgref/Download_Buncefield_Investigation_DO-Recommendations.pdf/$FILE/Buncefield_Investigation_DO-Recommendations.pdf .

32) Engineering a Safer World - Systems Thinking Applied to Safety, Nancy Leveson, MIT Press 2011
http://sunnyday.mit.edu/safer-world/index.html (free), http://mitpress.mit.edu/0262016621 .

33) "Almost every tanker in existence is one failure away from being adrift has not penetrated the public consciousness. A body politic that is obsessed with single skin hulls has not even noticed that all but a handful of the 3600 odd large tankers in existence have a single engine.
... many casualties ... resulted from lack of machinery redundancy are listed as groundings ... or collisions..."
An obvious mitigation for a single point failure, e.g., the loss of engine power, is to have redundancy by doubling the number of engines and screws.
http://www.c4tx.org/ctx/job/twin/summary.html .

34) "... Machinery failures are an important cause of tanker oil spillage. This paper argues that the current large (over 10,000 deadweight) tanker fleet is experiencing at least two full losses of power or steering per day, and probably more than ten. If this fleet were twin screw, properly implemented, this number would be cut by a factor of one thousand."

The Argument for Twin Screw Tankers, Jack Devanney, Sep 20-21, 2007.
Center for Tankship Excellence, USA, djw1@c4tx.org
http://www.c4tx.org/ctx/pub/twin_screw.pdf .
http://www.martrans.org:8093/symposium/papers/Track%20A/A11%20devanney.pdf .

35) "A significant change that is occurring in commercial tanker is the increasing adoption of twin screw designs. **The introduction of twin screws is a response to increasing concern of oil pollution through loss of steerage** and the increasing number of Special Areas and Particularly Sensitive Sea Area (PSSA) defined through IMO".
Future naval tankers - bridging the environmental gap - the cost effective solution
Andy Kimber, BEng, CEng, MRINA, BMT Defence Services Limited, UK
Arne Magne Vik, Skipskonsulent A/S, Norway, March 2006
http://media.bmt.org/bmt_media/resources/33/AEGIRPresentedatWMTCMarch06.pdf .

36) 20000 DWT PRODUCT/CHEMICAL TANKER - TWIN SCREW
+ Bow Thruster & Stern Thruster, ICE CLASS 1A
Volume Cargo Tanks - about 21000 cbm, built 2008
http://www.mes.it/reference.html?id=50
http://www.mediterraneanav.it/fleet/ship-details/id/20 . owner of SARACENA

37) "Twin Screw and more power redundancy would additionally help to drastically improve low speed maneuverability and the pilot's ability to correct a mistake" p. 118
Second International Workshop on Risk-Based Approaches in the Maritime Industry, 5-8 May 2008
http://www.safedor.org/resources/SAFEDOR-P-2009-02-19_Workshop_Risk_Based_Approaches-rev-1.pdf .
http://www.safedor.org/resources/SAFEDOR-P-2009-04-27_Final-Conference-Proceedings-rev-1.pdf

38) NASA System Safety Handbook
Volume 1, System Safety Framework and Concepts for Implementation
NASA/SP-2010-580, Version 1.0, November 2011
http://www.hq.nasa.gov/office/codeq/doctree/NASASP2010580.pdf

39) "Kerosene 4000' upstream from water plant intake. Versar states at 180 ppb [parts per billion] kerosene people won't drink water because of bad taste".
On-Scene Coordinator's Report: Battle of Bull Run, Manassas, Virginia, March, 1980
http://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=9100CIY1.txt .

40) A study of storage tank accidents
http://www.sciencedirect.com/science/article/pii/S0950423005000641
http://www.youtube.com/watch?v=S40RcLsar-g .

41) Risk Acceptance Criteria or "How Safe Is Safe Enough"
http://www.questconsult.com/resources/papers/pdf/paper48.pdf .

42) Esler, D., Trust, K., Ballachey, B., Inverson, S., Lewis, T., Riszzolo, D., Mulcahy, D., Miles, K., Woodin, B., Stegeman, J., Henderson, J., Wilson, B., *Cytochrome P4501A Biomarker Indication of Oil Exposure in Harlequin Ducks up to 20 Years After the Exxon Valdez Oil Spill.',* Wiley-Blackwell, April 2010: DOI: 10.1002/etc.129
http://www.sfu.ca/biology/wildberg/papers/Esler%20et%20al%202010%20ETC1.pdf

43) We Don't Quite Know What We Are Talking About When We Talk About Volatility
Daniel G. Goldstein, Nassim Nicholas Taleb
http://www-stat.wharton.upenn.edu/~steele/Courses/434/434Context/Volatility/ConfusedVolatility.pdf

44) Why We Don't Know What We Talk About When We Talk About Probability,
Nassim N. Taleb
http://www.fooledbyrandomness.com/probability.pdf

45) Developments in Flammable Liquid Storage Tank Fire Protection
Robert Zalosh, 2007
http://www.energy.org.il/info/m-energy/matzagot-9/nrg.200.pdf

46) Safety Integrity Level
http://en.wikipedia.org/wiki/Safety_Integrity_Level

47) Written Reply Evidence of Northern Gateway Pipelines Limited Partnership, July 20, 2012
http://www.ceaa.gc.ca/050/documents_staticpost/cearref_21799/4234/NGP_Written_Reply_Evidence.pdf

48) TERMPOL Process Report on the Enbridge Northern Gateway Project, 20/02/2012.
http://www.ceaa.gc.ca/050/documents/57633/57633E.pdf

49) Technical Data Report, Marine Shipping Quantitative Risk Analysis, 2010
www.ceaa.gc.ca/050/documents_staticpost/.../marine_shipping.pdf

50) TERMPOL Study 3.15: General Risk Analysis and Intended Methods of Reducing Risk, April 2010
http://www.ceaa.gc.ca/050/documents_staticpost/cearref_21799/2559/section3_15.pdf

51) TERMPOL Vapour Cloud Modelling and Conditional Quantitative Risk Analysis, 2010
www.ceaa.gc.ca/050/documents_staticpost/.../vapour_cloud.pdf

52) Section 2.9: Ship Specifications, TERMPOL Survey and Studies, January 20, 2010.
http://www.ceaa.gc.ca/050/documents_staticpost/cearref_21799/2559/section3_09.pdf

53) Northern Gateway's response to JRP IR 12
http://www.ceaa-acee.gc.ca/050/documents/p21799/81508E.pdf

54) Safety Plan Guidelines, March 31, 2011
http://publications.gc.ca/collections/collection_2011/one-neb/NE23-163-2011-eng.pdf

55) Enbridge Incorporated
Hazardous Liquid Pipeline Rupture and Release
Marshall, Michigan, July 25, 2010
http://www.ntsb.gov/doclib/reports/2012/par1201.pdf

56) Oil Sands Development–What the Industry Doesn't Want Us to Know
http://www.robynallan.com/2013/01/15/oil-sands-development-what-the-industry-doesnt-want-us-to-know/

57) Northern gateway and risk
http://www.robynallan.com/2012/07/10/northern-gateway-and-risk/

58) Gateway Oil-Spill Insurance
http://thetyee.ca/News/2012/06/05/Gateway-Oil-Spill-Insurance/

59) DRAM Errors in the Wild: A Large-Scale Field Study
http://www.cs.utoronto.ca/~bianca/papers/sigmetrics09.pdf

60) Understanding latent sector errors and how to protect against them
http://www.usenix.org/event/fast10/tech/full_papers/schroeder.pdf

61) The Use of Safety Cases in Certification and Regulation, Prof. Nancy Leveson,
Aeronautics and Astronautics/ Engineering Systems, MIT
http://sunnyday.mit.edu/SafetyCases.pdf

62) Jeffrey J. Joyce and Ken Wong, Hazard-driven testing of safety-related software, 21st International System Safety Conference, Ottawa, Ontario, 2003
http://www.criticalsystemslabs.com/docs/2003OttawaSafetyTesting.pdf

63) Dan Geer, Resolved: The Internet is no place for critical infrastructure
http://queue.acm.org/detail.cfm?id=2479677

64) World's first automatic back up for GPS successfully demonstrated in jamming trial
http://www.accseas.eu/news-and-events/news/worlds-first-automatic-back-up-for-gps-successfully-demonstrated-in-jamming-trial

65) UK Focuses on GPS Jamming & Interference
http://www.insidegnss.com/node/1934

66) Lightning sparks gas tank farm - Posted: June 13, 2010
http://www.wral.com/news/news_briefs/story/7773524/

67) March 14, 2011 Report to the General Purposes Committee (City of Richmond website) - Richmond Fire Department response to the VAFFC's proposal. See GP - 22 (Special) - section 18.6.3 Existing Fire Response Capacity and Evaluation of Adequacy: "The inference that RFR has at present the resources to service this increased risk to the City of Richmond is simply incorrect and unfounded."
http://www.richmond.ca/cityhall/council/agendas/gp/2011/032811s_minutes.htm .
http://www.richmond.ca/__shared/assets/Vancouver_Airport_Fuel_Delivery_GP_SP_03281130111.pdf .

68) Prevented Mortality and Greenhouse Gas Emissions from Historical
and Projected Nuclear Power
Pushker A. Kharecha and James E. Hansen
NASA Goddard Institute for Space Studies and Columbia University Earth Institute,
http://pubs.acs.org/doi/pdf/10.1021/es3051197
http://pubs.acs.org/doi/suppl/10.1021/es3051197/suppl_file/es3051197_si_001.pdf .

69) Rogue wave
https://en.wikipedia.org/wiki/Rogue_wave .

70) Severe weather has sunk more than 200 supertankers and container ships exceeding 200 metres in length during the last two decades. Rogue waves are believed to be the major cause in many such cases.
http://www.esa.int/Our_Activities/Observing_the_Earth/Ship-sinking_monster_waves_revealed_by_ESA_satellites .

71) On the probability of occurrence of rogue waves
E. M. Bitner-Gregersen1 and A. Toffoli2
http://www.nat-hazards-earth-syst-sci.net/12/751/2012/nhess-12-751-2012.pdf

72) Breach and Safety Analysis of Spills over Water from Large Liquefied Natural Gas Carriers
Anay Luketa, M. Michael Hightower, Steve Attaway
http://www.energy.ca.gov/lng/documents/2008-09-11_SANDIA_2008_Report.PDF

73) Algerian Explosion Stirs Foes of U.S. Gas Projects
http://www.nytimes.com/2004/02/12/business/algerian-explosion-stirs-foes-of-us-gas-projects.html

74) Joule
http://en.wikipedia.org/wiki/Joule

75) 1998 St. Cloud explosion
http://en.wikipedia.org/wiki/1998_St._Cloud_explosion

76) Methane MSDS
http://avogadro.chem.iastate.edu/MSDS/methane.pdf Flash point is -187.8 degrees C

77) LNG Safety and Security
http://www.beg.utexas.edu/energyecon/lng/documents/CEE_LNG_Safety_and_Security.pdf

Definitions:

Catastrophic (scenario) is the loss of human life or permanent disability; loss of major system; loss of vehicle; loss of ground facility; severe environmental damage.

Catastrophic Hazard is any hazard that, when uncontrolled, results in a catastrophic event.

Critical is the condition where failure to comply with prescribed contract requirements can potentially result in loss of life, serious personal injury, loss of mission, or loss of a significant mission resource. Common uses of the term include critical work, critical processes, critical attributes, and critical items.

Fault is an undesired system state and/or the immediate cause of failure (e.g., maladjustment, misalignment, defect, or other). The definition of the term "fault" envelopes the word "failure" since faults include other undesired events such as software anomalies and operational anomalies.

Failure is:[1] Inability of a system, subsystem, component, or part to perform its required function within specified limits.
[2] Non-performance or incorrect performance of an intended function of a product. A failure is often the manifestation of one or more faults.

Fail-Safe is the ability to sustain a failure and retain the capability to safely terminate or control the operation.

Failure Tolerance is the ability to sustain a certain number of failures and still retain capability.

Hazard is:
[1] A state or a set of conditions, internal or external to a system that has the potential to cause harm.
[2] A state or condition that could potentially lead to an undesirable consequence (i.e., casualty or property damage).
[3] Existing or potential condition that can result in, or contribute to, a mishap or accident.
[4] Any real or potential condition that can cause injury or death to personnel, or damage to or loss of equipment or property.
[5] A state or a set of conditions, internal or external to a system that can cause injury or death to personnel, or damage to or loss of equipment or property or the environment

Critical Hazard is damage to equipment, non-disabling injury, requires unscheduled shutdown, affects operations

Note: No single failure should result in a critical hazard
==> 2 controls (i.e., redundant) to prevent critical hazard.

Catastrophic Hazard is a disabling / fatal personal injury, loss of control or facility.

No combination of two failures should result in a catastrophic hazard
==> 3 controls (i.e., dual redundant) to prevent critical hazard.

Failure Tolerance is a basic safety requirement; tolerate minimum number of CREDIBLE failures

Single failure tolerant = 2 independent controls.

Risk {Programmatic} is the combination of following:
(1) The probability (qualitative or quantitative) of experiencing an undesired event,
(2) The consequences, impact, or severity that would occur if the undesired event were to occur and
(3) The uncertainties associated with the probability and consequences.

Design for Minimum Operational Risk provides adequate factors of safety: structures, pressure vessels, pressure lines, fittings, fire/ explosion suppression, mechanisms, materials compatibility, flammability,

Design for Minimum Societal Risk utilizes a risk-based land use planning to minimize health and economic impact.

Safety is [1] In a risk-informed context, safety is an overall condition that provides sufficient assurance that mishaps will not result from the mission execution or program implementation, or, if they occur, their consequences will be mitigated. This assurance is established by means of the satisfaction of a combination of deterministic criteria and risk-informed criteria. The term "safety" broadly includes human safety (public and workforce), environmental safety, and asset safety.
[2] Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.

Safety Culture is the value placed on safety as demonstrated by people's behavior. It is the way safety is perceived, valued and prioritized in an organization. It reflects the commitment to safety at all levels in the organization. It is "how an organization behaves when no one is watching". Safety culture is expressed and observed via individual and group attitudes and behavior; and organizational processes.

Safety Assurance provides confidence that acceptable risk for the safety of personnel, equipment, facilities, and the public during and from the performance of operations is being achieved.

Safety Program is the implementation of a formal comprehensive set of safety procedures, tasks, and activities to meet safety requirements, goals, and objectives.

System is the combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose.

System Safety Engineering is the application of engineering and management principles, criteria, and techniques to achieve acceptable mishap risk, within the constraints of operational effectiveness and suitability, time, and cost, throughout all phases of the system life cycle.

System Safety Plan is a written plan defining the approach to accomplish the project safety activities, including safety management, identification of safety tasks, roles and responsibilities, and the coordination and communication with project/ systems/ software engineers and approving authorities.

Safety Integrity Level - according to IEC 61508, Functional Safety, the Safety Integrity Level (SIL) must be related to the dangerous failure rate of the system electrical control system, not just its failure rate or the failure rate of a component part, such as the software. Definition of the dangerous failure modes by safety analysis is intrinsic to the proper determination of the system failure rate.

Reliability is the probability that a given item will perform its intended function for a given period of time under a given set of conditions.

Notes:

Large LNG carrier carries 266,000 cubic meters = 266,000,000 liters
http://en.wikipedia.org/wiki/LNG_carrier

Energy density of LNG = 22.2 MJ/L = 22,200,000 joules per liter
http://en.wikipedia.org/wiki/Energy_density

Energy stored on LNG carrier = 22,200,000 x 266,000,000 = 5.9 10^15 = 5.9 Petajoules (PJ)

The Hiroshima atom bomb had 63 Terajoules (TJ) = 0.063 PJ
http://en.wikipedia.org/wiki/Joule