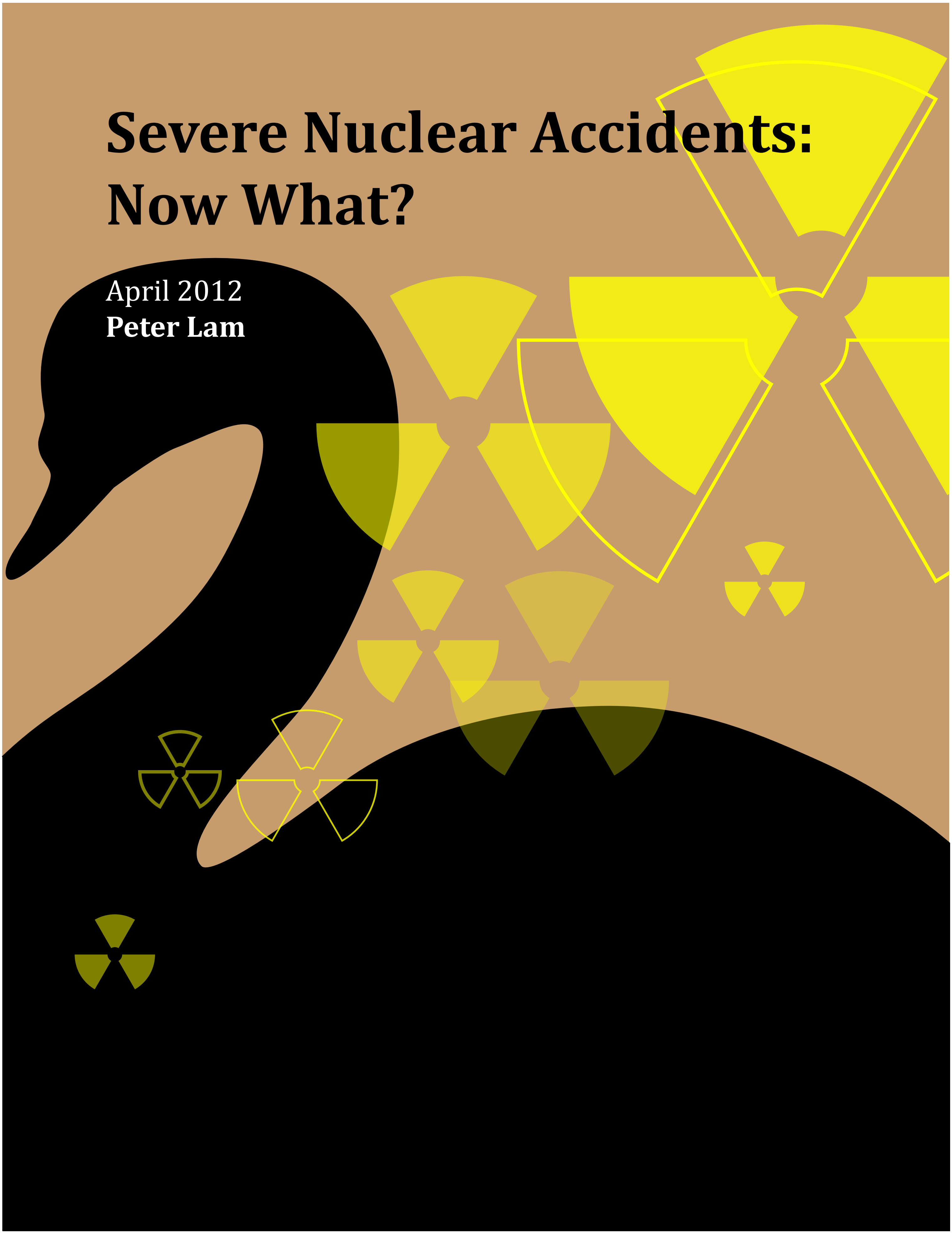
Severe Nuclear Accidents: Now What?

April 2012

Peter Lam



思匯
CIVIC EXCHANGE

About Civic Exchange

Civic Exchange is a Hong Kong-based non-profit public policy think tank that was established in October 2000. It is an independent organization that has access to policy-makers, officials, businesses, media and NGOs - reaching across sectors and borders. Civic Exchange has solid research experience in areas such as air quality, energy, urban planning, climate change, conservation, water, governance, political development, equal opportunities, poverty and gender. For more information about Civic Exchange, visit www.civic-exchange.org.

About the author

Dr. Peter Lam is the Chairman of the Diablo Canyon Independent Safety Committee which conducts chartered safety reviews of the Diablo Canyon nuclear power plant. He was appointed by the California Energy Commission in 2009. He has previously served as an Administrative Judge of the U.S. Nuclear Regulatory Commission for 18 years. Dr. Lam is an international authority on nuclear reactor operating experience, and a leading expert of nuclear reactor safety and risk assessment. In his 18 years of public service as an Administrative Judge, Dr. Lam has presided over numerous public proceedings to decide technical issues of national and international significance involving the use of nuclear energy and materials. Judge Lam’s jurisdiction covered all 104 nuclear power plants, some 21,000 medical and material licensees, and nuclear waste storage in the United States.

Prior to his judicial appointment 21 years ago, Dr. Lam had extensive technical and managerial experience in the nuclear energy business over a period of 20 years. He was a nuclear engineer at General Electric Company, a program manager at Argonne National Laboratory, a manager at Science Applications, Inc., and a consultant at NUS Corporation. Additionally, Dr. Lam managed a group of technical specialists in the U.S. Nuclear Regulatory Commission in the analysis and evaluation of nuclear reactor operating experience. Dr. Lam was also a visiting faculty member at California State University at San Jose, and at George Washington University.

Dr. Lam has published 71 technical papers and reports in national and international journals and in proprietary company publications, which focus on major issues in nuclear transport theory, nuclear reactor fuel design, nuclear reactor operating experience, and nuclear reactor safety. Judge Lam has also issued over 110 published judicial decisions related to some 50 cases of litigations. These judicial decisions resolve a wide range of technical and legal issues regarding nuclear reactor safety, nuclear waste disposal, and other civilian use of nuclear technology.

Dr. Lam has presented lectures at IAEA international conferences in Austria, Korea, and Spain, on significant results in comprehensive analyses of nuclear reactor operating experience. He has chaired an IAEA working group to develop a technical treatise for the analysis and evaluation of operating experience of the world’s nuclear reactors.

Dr. Lam earned a Ph.D. and a M.S., both in nuclear engineering, from Stanford University in 1971, and 1968, respectively. He earned a B.S., in mechanical engineering, from Oregon State University in 1967.

Preface & acknowledgements

Six months ago in Hong Kong I met Christine Loh, the founder and chief executive officer of Civic Exchange, and became aware of Civic Exchange's activities in advancing literacy in nuclear issues for Hong Kong. As I have recently summarized my thoughts on nuclear reactor safety and the future direction of the global nuclear industry, I feel that sharing my thoughts with the Hong Kong readers would be opportune. I am delighted that Civic Exchange has agreed to publish this article on their website.

My deep appreciation to the following individuals of Civic Exchange for their significant contributions to the report: Ms. Christine Loh for her leadership and time; Mr. Andrew Lawson for his editorial comments; Ms. Michelle Wong for her art work and design; and Ms. Veronica Booth for her project management.

Peter Lam, Ph.D.
Administrative Judge Emeritus

The opinions expressed in this article are the author's own and do not represent the official views of the Diablo Canyon Independent Safety Committee.

Table of Contents

1 Introduction

Sighting the Black Swan – the impossible becomes real

The conventional wisdom in the global nuclear industry used to believe that a severe nuclear accident causing devastating consequences is improbable. Hence, among nuclear engineers and scientists, a "nuclear black swan" is an apt expression for a severe nuclear reactor accident with an extremely small likelihood of occurrence, an accident as rare as a European sighting a black swan before the 17th century. How rare is rare? Say, once in ten thousand years. These “black swan” accidents, although deemed unlikely, would cause colossal economic damage as well as enormous health and social consequences. And despite the very small odds calculated by numerous specialists from different technical disciplines in the nuclear industry over many years, three nuclear black swans did occur.

The Big Three:

1.1 Three Mile Island

Thirty some years ago, on March 28, 1979, the first major nuclear reactor accident happened at Three Mile Island (TMI) unit 2 nuclear power plant near Middletown, Pennsylvania. It was the most serious accident in the history of United States commercial nuclear power plant operating history even though it involved no fatality of plant workers or members of the public. The U.S. Nuclear Regulatory Commission (NRC) has determined that the partial meltdown of the unit 2 nuclear reactor was caused by a sequence of events involving equipment malfunctions, design-related problems, and human errors. According to the NRC, the accident brought sweeping changes in how the federal agency and the U.S. nuclear industry perform their emergency response planning, nuclear reactor operator training, human errors prevention, and numerous other areas of nuclear power plant operations.

1.2 Chernobyl

Seven years later, on April 26, 1986, another major accident occurred at the Chernobyl Nuclear Power Plant in the Ukraine, in the former Soviet Union. An explosion and fire in the unit 4 reactor propelled massive amounts of radioactive material into the atmosphere, that then spread over the western former Soviet Union and Europe. Several hundred thousand people were evacuated from the surrounding areas. According to the International Atomic Energy Agency (IAEA), there were 31 immediate fatalities among the reactor staff and emergency responders, while decades later, the effects of radiation contamination continue to be felt. In September 2005, the World Health Organization (WHO), together with the IAEA and six other United Nations agencies, estimated that latent civilian fatalities from cancers caused by radiation exposure had reached about 4,000. The economic damages range in the many billions of 1986 dollars, while the adverse health and social impact has been equally immense. Even now, large geographic areas near the plant remain contaminated. The 25-year old temporary concrete "sarcophagus" which entombs the damaged reactor is now deteriorating, and major additional construction is in progress to remedy the situation.

1.3 Fukushima

On March 11, 2011, a 9.0-magnitude earthquake and a subsequent tsunami hit the Fukushima Daiichi nuclear station in Japan. This double whammy led to a triple nuclear reactor meltdown, the evacuation of more than 100,000 residents from around the nuclear station, and staggering economic and social consequences. The latest estimates of economic damage attributable to the nuclear accident range from US$50 billion to well over US$100 billion, while the political furore generated by the accident has rippled worldwide. After almost a year since the accident, many of the evacuated people have not been allowed to return to their homes and businesses, and the damaged nuclear reactors have yet to be completely stabilized.

Policymaker's dilemma

By now, nuclear power might appear to be economically dubious and environmentally harmful. This appearance is compounded by a common and valid perception that nuclear power is a complex technology and can sometimes be dangerous and unforgiving. Before you label nuclear power as bad or even evil, and before you tally up the actual immense damage and costs caused by the Fukushima Daiichi nuclear accident, and the burgeoning economic and social consequences accumulated at and near Chernobyl, pause to think of the many good features of nuclear power. And ponder why there are more than four hundred of them running in different countries in the world today. Despite the frightening and lingering catastrophic impacts of a major nuclear accident, nuclear power must have some attractive features. Well, yes, it does. Some of these appealing features are described below.

Responding to Fukushima – a global divergence

In this report we'll attempt to address the dilemma: Is nuclear power worth the risk? Some countries like Germany and Switzerland think not after the Fukushima accident, and are planning to phase out nuclear power entirely in the future. Some countries like China, India, and the United States think so, and have plans to continue to build more and bigger nuclear power plants, after evaluating the lessons from the Fukushima accident.

Prevention and mitigation of unlikely events

If nuclear power is worth it, then preventing a nuclear black swan from happening and mitigating its devastating consequences after its unexpected arrival should be an urgent priority. The urgency of this priority should prevail even for the situation that nuclear power is kept as a status-quo source of electricity until alternative energy sources are developed.

2

Nuclear Power: The Good, The Bad, and The Ugly

2.1 The Good

Benefits of nuclear – reliable 24/7, low carbon, low air pollution, and fossil-fuel independence

Nuclear power is becoming an increasingly essential part of the total energy production in the world where the demand for electricity is rapidly increasing. This trend is primarily due to the convergence of several factors. First, nuclear power has compiled a reasonably well-established operational worldwide record in the past 40 years as a reliable base-load supplier of electricity, if you are willing to ignore the three major nuclear reactor accidents. That means it is generating electricity 24 hours a day, seven days a week, regardless whether or not the sun is shining or the wind is blowing. Secondly, nuclear power, in contrast to burning oil, gas or coal, has a very low carbon footprint; i.e. very low emissions of greenhouse gases. Thirdly, nuclear power does not emit toxic air pollutants. Finally, perhaps more importantly, for countries with a large need to import fossil fuels, the use of nuclear power would decrease or even eliminate the dependence on fossil fuels, the price of which can be volatile and the supply of which can be uncertain. Hence, the reduction of oil and gas importation is a major consideration for national security. This consideration is even more critical in countries with little or no petroleum resources.

Push for safety in design and operation

As to the safety of nuclear power, one can also make a plausible argument that the worldwide nuclear power production also has a rather decent safety record as measured by the number of civilian fatality from radiation exposure, despite the occurrence of the three major nuclear reactor accidents. After all, even for these three major nuclear reactor accidents, two out of the three accidents, namely the TMI accident and the Fukushima triple meltdown, had not led to any civilian fatalities from radiation exposure within or outside the site boundary. In other words, the overwhelming majorities of nuclear power plants worldwide, that is the 99% of operating nuclear reactors, have been operating safely. An often repeated pro-nuclear power argument points to the observation that the safety of nuclear power is also bolstered by transparent robust central governments' oversight and enforcement. Furthermore, the extensive application of fundamental safety principles of redundancy, diversity, and physical separation in the areas of design, manufacture, installation, operation, and maintenance of the region's nuclear power reactors is another major contributor to nuclear reactor safety. Additionally, the establishment of world organizations such as the IAEA, the World Association of Nuclear Operators (WANO), and national groups such as the Institute of Nuclear Power Operations (INPO) and Nuclear Energy Institute (NEI), enhances nuclear safety culture and facilitates the adoption of internationally accepted good practices as well as full access to global nuclear power plant operating experience for participants.

Local economy

Regarding nuclear power’s positive contributions to the economy, besides the obvious benefit of producing electricity, the impact of a nuclear power plant on its locale is huge. A nuclear power plant is a big investment as it typically costs several billion dollars. It brings thousands of jobs to the community where it is located while it is being built. While in operation, a nuclear power plant is usually the largest employer, and the largest property tax payer for that location as well.

2.2 The Bad

Even before any one of the three major nuclear reactor accidents ever happened, nuclear power engendered many negative perceptions. Well before any observed immense adverse economic and social consequences from a major nuclear accident, there were always assertions that nuclear power was just bad and risky. These assertions rest upon some very nasty perceptions, real or imaginary. Well, sometimes perception is reality. What are these perceptions?

Perception of radiation

First of all, many people are afraid of radiation. You cannot see it, you cannot smell it, and you cannot feel it. And it causes genetic mutations, which cause cancer. This fear of the hazards of radiation is translated to a strong and negative emotional reaction to nuclear power. This reaction is not entirely irrational, and it runs deep.

Attitudes to involuntary risk

Secondly, all of us do not take involuntary risk well. Put it differently, you and I may accept risk willingly if we think we are in control, and in a position to accept or reject it. Weighing and balancing whether or not the benefits outweigh the penalty comes later. For example, driving a car carries a significant risk from injury, yet the public accepts it more readily, overwhelmingly more than the involuntary risk of injury from nuclear power. In the United States, annual highway fatalities are about 40,000, and annual fatalities from nuclear power plant accidents have been zero. Still, public perception of the risk from nuclear power is certainly higher than the risk from driving a car. One explanation is that the risk from nuclear power is seen as being imposed on those of us who are in the nuclear power plant's vicinity, and on our society in general. This sentiment is particularly common in the United States, as federal laws dictate that only the federal government, and not any other local governments or entities, has the authority in the licensing, inspection, and enforcement of civilian use of nuclear power.

Potential for human error

Thirdly, a very problematic perception for nuclear power is that it is prone to human errors. Human errors are bound to occur when a very technically complex technology is mixed with the need for many levels of human interactions during its design, manufacture, installation, operation, and maintenance. Indeed, in the more than 40 years of commercial nuclear power operation, aside from the three major nuclear accidents, there have been many instances of significant human errors observed in every one of the aforementioned areas of design, manufacture, installation, operation, and maintenance.

A well-known example is the erroneous use of only one set of blue prints (while two mirror-image sets were needed) for seismic structural supports for the two-unit Diablo Canyon nuclear power plant discovered in the early days of construction in 1981. Other common examples are the inadvertent use of wrong materials or wrong procedures in the maintenance of important safety equipment in numerous nuclear power plants. Even though these errors have been expeditiously corrected after they were discovered, their complexity and unpredictable nature help contribute to the public perception of puzzlement and distrust.

Managing and communicating complexity

Fourth, as indicated earlier, nuclear power technology is complex, by design and by necessity. This complexity helps contribute to the difficulty of communication by nuclear companies and governments to effectively explain nuclear power operation and safety. An anecdote regarding the increasing complexity of nuclear power operation is as follows. In the early days of American commercial nuclear power operation, a nuclear power plant's Technical Specifications contained several hundred Limiting Conditions for Operation (LCO), which are well prescribed conditions and actions the plant must follow during different circumstances. A modern nuclear power plant today has several thousand LCOs. To follow and comply with all these LCOs during plant operation requires tremendous efforts by numerous members of the power plant staff. Imagine the difficulty of explaining what these LCOs and their compliance mean to a member of the public.

Technical demands

Another way to get a glimpse of the complex technology of nuclear power is to take a look at how demanding the design functions of the emergency core cooling systems (ECCS) are. These systems, mandated in American nuclear power plants, are required to remove residual heat from the nuclear core in the event of a failure of the normal core cooling system. They are called upon during emergencies. The ECCS have redundancies and diversities, and they are physically separated. They are heavily regulated, meticulously designed, and thoroughly tested. Even though the ECCS are constantly in an idle mode, upon demand they have to automatically deliver a very large amount of water in a hurry. A "very large amount of water" means a few thousand gallons of water per minute. "In a hurry" means about 30 seconds. And then, of course, the ECCS need to operate for a long time, and probably in a hostile environment where temperature, humidity, and radiation may be high. Very briefly stated, the ECCS are large systems with huge capacities, standing idle but have to respond to almost instant demands. And they have to operate in a harsh environment for a prolonged period. The laws of physics are being pushed to their limits here.

Management of radioactive waste

Finally, the public has a rather negative perception about the long-term storage of nuclear waste. It really does not matter whether or not the technical arguments for long-term storage of nuclear waste are valid. The fact that nuclear waste is both chemically toxic and radioactively lethal, and would remain so for a very long time, does not help to promote a positive image for the storage of nuclear waste. Here, a very long time means thousands of years. Witness the difficulty the United States government has in implementing its long-term waste storage policy, particularly the fight for and against the Yucca Mountain facility, and its final cancellation by the Obama administration. The safeguarding of long-life radioactive waste, regardless of the merits of its claimed feasibility, is a controversial issue in many countries, and is expected to remain so for the foreseeable future.

2.3 The Ugly

If you think nuclear power is bad when nothing happens, it quickly becomes ugly when you have a major nuclear reactor accident (The potential for a country to clandestinely divert nuclear power production into producing nuclear weapon materials is another story for another day).

Scale of potential damage

If you have a power plant that burns coal, or oil, or natural gas, a nasty accident may destroy the plant, but usually an accident does not linger for days, months, or years. Literally you can turn off the switch of the fuel supply, and in a relatively short time, after you assess the damage, pay your dues whatever they are, then you can think about rebuilding. Not in a major nuclear reactor accident.

"Decay heat" – a lingering challenge

There are two culprits in any nuclear reactor accident, which contribute to the tremendous difficulty in managing the accident. The first one is the nuclear decay heat. The nuclear chain reaction that produces nuclear power is usually stopped instantaneously in a nuclear reactor accident (except one accident, which we call an Anticipated Transient Without Scram. We will talk more about this later). But the fission products made before the stopping of the chain reaction continue to decay, hence producing what is called the "decay heat". This decay heat lies at the heart of the immense difficulty in managing a severe nuclear reactor accident. The amount of decay heat, at the time the nuclear chain reaction is stopped, is about 10 % of full power. It rapidly diminishes to about 2% of full power in a day, to about 1% in a month, and to about 0.1-0.2% in a year. The problem is that, even at 0.1% of full power, more than a thousand pounds of steam per hour is being produced. This is a massive amount of steam, thus heat, which needs to be removed. The removal of this large amount of heat, when coupled with the second culprit which is radiation release, poses an enormous challenge.

Radioactive Medusa

The second culprit is the huge amount of radioactive materials in a nuclear reactor core and the associated severe radiation lethality, not to mention their chemical toxicity. The LD50 for radiation, which stands for the lethal dose to 50% of the population, is about 500 rems (a rem is unit of measurement of radiation dose). The contact dose of an exposed nuclear reactor fuel bundle residing in a nuclear reactor for about two years, is of the order of a million rems per second. The many tons of radioactive materials residing in a nuclear reactor core represent an inherent danger. A silly but scary argument is that the amount of radioactive material in such a reactor core, if distributed uniformly among the human race, would destroy us all. Rest assured that this scenario is utterly unrealistic as there are no possible means for such distribution and dispersion. Of course there are multiple physical and functional barriers against the release of such lethal radiation, namely the nuclear fuel cladding, the reactor core vessel, the reactor containment, and the many engineered safety features and operational procedures. But in a major nuclear reactor accident with significant radiation releases such as what happened at Chernobyl and Fukushima, some or all of these barriers are breached. Then, the Greek mythological figure of Medusa is fitting to be used here to describe the lethality of molten nuclear fuel. The way the Greek legend goes: anyone who dared to look at Medusa would instantly turn into stone. The hazards of molten nuclear fuel, driven by decay heat and contaminated steam, have been well observed at Chernobyl and Fukushima, and need no further description.

In a very simplistic way, the challenge in a major nuclear reactor accident where radioactive releases are involved is how to contain the radiation release and at the same time deal with the thousands of pounds of steam being produced from a damaged or molten nuclear reactor core for a long time, namely years. As witnessed in Fukushima, to contain radiation releases and to remove decay heat at the same time from a stricken nuclear power plant requires a national effort of Herculean scale.

3

What Are The Severe Nuclear Accidents

The Big Six

What are the severe nuclear reactor accidents that keep us awake at night? Six of them come to mind. Before TMI, Chernobyl or Fukushima, they were treated as if they were purely hypothetical. Things you talk about, but assume would never happen. These six severe nuclear reactor accidents are listed in Table 1. The descriptions here of these severe nuclear accidents are conceptual, hence very brief. A detailed technical discussion of any one of these accidents would involve a great deal of elaboration, and would run to thousands of pages.

Table 1: Nuclear Black Swans: Severe Nuclear Accidents

THE TOP FIVE BLACK SWANS

- Station Blackout
- Anticipated Transient Without Scram (ATWS)
- Reactor Vessel Rupture
- Interfacing Loss of Coolant Accident (Interfacing LOCA)
- Spent Fuel Pool Loss of Cooling

THE RAREST BLACK SWAN

- Multiple Reactor Accidents

3.1 A Station Blackout

Electricity essential to cool reactor

Before the Fukushima nuclear reactor accident, you probably never heard of it. Now it has become somewhat more familiar to the general public. A Station Blackout accident goes like this: Some things happen and cause a nuclear power plant to lose its offsite power. For the same or other reasons the emergency diesel generators do not start, or they start but do not run. Without power, alternating current (ac) power that is, the plant's direct current (dc) battery power is built to last only a few hours. When the dc power runs out, the nuclear reactor loses all means of emergency cooling. In a short time, there would be insufficient cooling water to cover the nuclear reactor, and nuclear fuel would start to melt. This is, of course a very simplistic sketch of the accident scenario as there are many variations in how an actual accident may progress.

All the emergency cooling systems (except steam-driven trains) in a nuclear power plant are dependent on ac power, be it supplied from offsite or from the emergency diesel generators. The dc dependency is related to the throttle or control valves of the steam-driven trains of emergency cooling systems, specific to the type of nuclear reactor and the plant design. For Fukushima, the tsunami caused by the huge earthquake resulted in a loss of all the incoming lines for offsite power, and the same tsunami caused all the diesel generators to fail, and the dc battery banks were depleted after about 8 hours.

3.2 An Anticipated Transient Without Scram (ATWS)

"Scram" = controlled stoppage

An anticipated transient is an event that is expected to occur once in a while during nuclear power plant operation that usually triggers a reactor scram (the rapid insertion of control rods into the reactor core to stop the nuclear chain reaction). The plant is well designed for such an expected event, and plant operators are prepared for it. However, if the reactor does not scram, a major accident would unfold. It is called an Anticipated Transient Without Scram (ATWS). In an ATWS, after the reactor fails to scram, there is about thirty seconds for the reactor operators to act before the reactor core becomes uncontrollable.

An ATWS has fearsome consequences as the reactor continues to produce power at a level where there are no appropriate means for removal. This difficult situation is caused by the fact that the plant has gone into a configuration of decay heat removal assuming that the nuclear chain reactions have been stopped. This accident scenario moves in a fast and furious pace where a nuclear core melt and containment damage are the likely outcome.

3.3 A Reactor Vessel Rupture

An unstoppable projectile?

The third accident is called a Reactor Vessel Rupture. It has something to do with an aging reactor vessel that has experienced significant neutron damage, and may have high copper contents in its vessel bell line, which increases the vulnerability of the reactor vessel to brittle rupture. This event is likely to be triggered by what we call a pressurized thermal shock event (which happens when cold water is inadvertently injected into a hot and pressurized reactor vessel). Key questions to ask are as follows. If or when such a reactor vessel rupture occurs, what would be the worst-case scenario? Would colossal forces released by the vessel rupture propel the top half of a broken reactor vessel into an unstoppable projectile? Would the containment structure restrain and withstand such a heavy projectile?

3.4 An Interfacing Loss of Coolant Accident (Interfacing LOCA)

Defeats containment protection

The fourth accident is what we call an Interfacing Loss of Coolant Accident (Interfacing LOCA). It happens as a result of the simultaneous opening of a check valve and the motor operated valve (MOV) on the injection line of an ECCS system. This single event would bypass containment, disable the involved ECCS system, and precipitate a major nuclear reactor core melt. Here, the containment protection against radiation release is defeated even before a reactor core melt begins. Such a reactor core melt bypassing the containment would lead to the release of a very large amount of radioactive material.

3.5 A Spent Fuel Pool Loss of Cooling or Loss of Inventory

The fifth accident is the Spent Fuel Pool Loss of Cooling or a Loss of Inventory. Again, this one needs no detailed description after the Fukushima accident. Any spent fuel pool accidents are problematic for a variety of reasons: the large amount of radioactive material stored in a spent fuel pool; the lack of containment protection against such a release; and the possibility of the rapid oxidation of the zirconium fuel cladding. Zirconium cladding oxidation in a steam environment, if it were to happen, would release combustible hydrogen gas together with heat, greatly compounding an already difficult situation.

3.6 Multiple Reactor Accidents

Black Swan at Fukushima

Now, the sixth accident is the truest, purest, and rarest black swan: an accident that leads to multiple nuclear reactor core melt. For years, the global nuclear industry and all central governmental regulatory authorities having oversight over their respective nuclear power plants have been saying that a single nuclear reactor core melt was extremely unlikely. This conclusion was drawn from numerous reviews and detailed analyses based on theoretical and experimental models, supported by a long history of global nuclear reactor operating experience. Hence multiple nuclear reactor core melts were deemed impossible, and have never been examined. Until Fukushima, that is.

4

Why Nuclear Black Swans Were Deemed Extremely Unlikely

The six nuclear reactor accidents mentioned before were estimated to be extremely unlikely for many reasons. As will be seen in the discussions below, none of which has to do with recklessness, nor ignorance.

4.1 A Station Blackout

Multiple back-up features supported by operations data …

Take the first accident scenario, a Station Blackout. All of the nuclear power plants in the United States, and probably a majority of the nuclear power plants in the rest of the world, have multiple incoming lines from offsite to supply ac power to the site. How often these incoming lines lose power has been tracked and documented for each site for decades, with details involving the duration, frequency, and cause. Each operating nuclear reactor has at least two emergency generators, only one of which is required to deal with an accident, which are maintained and tested according to rigorous federal standards. These diesel generators, more often than not, have manual cranks, which may be relied upon to start the generator if it does not automatically start. Many nuclear power plant sites also have cross-ties among their diesel generators so that any one of the four generators, say on a two-unit site, can supply emergency power to any one of the two nuclear reactor units. Very quickly one may draw the conclusion that it is extremely unlikely that a nuclear power plant would lose its offsite power and all its onsite emergency diesel generators. Besides, even if this were to occur, the reasoning goes, there are the dc battery banks, which in the United States are designed to run for at least two hours. The dc battery banks would allow the control valves in a steam-driven ECCS train to provide emergency cooling to the nuclear reactor. Hey, the conventional wisdom says, in two hours, we can fix anything that needs to be fixed. The rationale of assigning an extremely low likelihood of occurrence for a Station Blackout has been defended with a great deal of operating data demonstrating the low frequency of the loss of offsite power, together with a long history of successful test starts of emergency diesel generators.

… but Fukushima changed the game

This rationale sounded more than reasonable, until Fukushima, where a 9.0-magnitude earthquake and a subsequent tsunami destroyed all incoming lines together with all onsite diesel generators for all three of the nuclear reactors. The dc batteries lasted for about 8 hours. The level of devastation around the facility prevented any meaningful repair or restoration of equipment for days. By then, a triple nuclear reactor meltdown became inevitable.

4.2 An Anticipated Transient Without Scram (ATWS)

Meticulous design …

As to the second accident scenario, the Anticipated Transient Without Scram, the assignment of extremely low likelihood has to do with the meticulous care employed in how the scram systems are designed, manufactured, installed, operated, and tested. The low likelihood estimates have also been strengthened by the observation that anticipated transients used to occur about ten times a year on a per-site basis, nowadays they happen, perhaps, once a year. Certainly the nuclear engineers who designed the scram system for nuclear reactors knew how critical this system is. The systems developed for both the pressurized water reactors (PWRs) and boiling water reactors (BWRs) are based on the most fundamental principles of safety and reliability. The system has multiple logics, redundant means of insertion of control rods, and very reasonable success criteria. They have also compiled an impeccable operating record. So far, not a single civilian nuclear reactor has failed to scram on demand. But this does not mean the scram system has absolutely no vulnerability. An old story about scram breaker testing comes into mind.

For a popular nuclear reactor vendor, the breakers used to initiate a scram in the scram system are driven by gravity. A breaker has two parts, held together by energizing a magnet. If the current to the magnet is cut, demagnetizing the magnet, gravity will cause a part of the breaker to drop, initiating the scram action. Stated in another way, the breakers will switch position by gravity, from being closed to being open, if the power supplied to maintain its closed position is cut. On first principles, this is an extremely reliable system. Gravity is always there, and the breakers are very heavy, so they would certainly drop when allowed. Coupled this design with independent logics in its actuation, the use of multiple breakers, and exceedingly liberal success criteria, the vendor was confident enough to say that the system is so reliable that the system failure probability is approximately once in a million billion years. This number means nobody should ever worry about a failure to scram.

… but what about circumstances beyond design?

Years ago a routine test was performed on the breakers while a nuclear reactor was not at power. All of the breakers failed to open when power was cut off from the magnets. After an expeditious and extensive examination at that time, the failure of the breakers was attributed to the application of the wrong type of lubricant. Since the breakers were big metallic instruments that needed to change position on demand, they required constant lubrication. Somewhere along the line when the scram breakers were serviced, the wrong lubricant was applied. Instead of lubricating the breaker, the wrong lubricant became sticky after a significant period of time when the lubricant was subjected to heating. So at the time of testing, being stuck together by the wrong lubricant, none of the breakers opened upon demand.

The point of the story here is obvious – one can plan for a lot of things, but it's something that one does not anticipate that causes a lot of trouble. The failure estimate of once in a million billion years was based on test data with the right lubricant. Well, with the wrong lubricant, all bets are off.

4.3 A Reactor Vessel Rupture

In the United States, some of the nuclear reactor vessels had high copper contents in their bell lines. When subjected to high neutron irradiation, as they would be after operating for about twenty years, and depending on the operating history, nuclear reactor vessels become brittle. If cold water is inadvertently injected into the reactor during power operation (when the reactor vessel is hot and pressurized), the thermal forces may cause the embrittled reactor vessel to rupture. This scenario is called a pressurized thermal shock, and is considered to be a possible initiator of a Reactor Vessel Rupture accident.

Changing rules

As most of the people in the United States nuclear industry are aware, the NRC used to have an old rule on pressurized thermal shock, which was developed to protect a nuclear reactor from brittle rupture. After about ten years of intensive research, the NRC now have promulgated and implemented a new rule. Under the old rule there are seven nuclear reactors in this country that would not be eligible for license extension for an additional 20 years, because they do not meet the NRC's old pressurized thermal shock protection criteria. But under the new rule now, all of them would be eligible. The NRC promulgated this new rule by saying no licensee is obligated to adapt the new rule. Yet the essence of the new rule, communicated by the NRC in various ways, is that the NRC has determined after extensive research that the old rule was unnecessarily conservative, and the new rule is more realistic, and at the same time still provides an adequate margin of safety. Perhaps one can also interpret the new NRC rule as an implicit endorsement of the view that a Reactor Vessel Rupture accident is very unlikely, so much so that an additional 20 years of plant operation and embrittlement of the reactor vessel would not pose a credible threat to plant safety.

Opponents of nuclear power attack this new rule as politically motivated, only developed to allow the otherwise ineligible nuclear power plants to apply for a 20-year life extension. Proponents of the nuclear industry hail this new rule as a concrete example of a more realistic and safe federal approach to regulate nuclear power by removing unnecessarily punishing burdens to the nuclear power plant licensees.

4.4 An Interfacing Loss of Coolant Accident (Interfacing LOCA)

Considered unlikely …

In this accident scenario, both the check valve and a normally closed motor operating valve on the injection pipe of an ECCS system (either the low pressure injection system or the high pressure injection system) fail in an open position. This would allow the high-pressure reactor coolant to enter the ECCS system, leading to the destruction of that ECCS system. And if a reactor core melts as a result, the open pathway allows the release of radioactive material outside the containment. The extremely unlikely estimates are based on the observation that a large volume of component failure data indicates that the rupture of the types of check valves and the MOV installed on the ECCS rarely happens. This primarily is attributable to how mechanically robust these valves are designed and built. A long history of nuclear power plant operating experience and component test data also support this claim. Therefore, there was a wide acceptance within the American nuclear industry and the United States government that rupturing of these valves was very unlikely.

… but not impossible

But then, does this mean an Interfacing LOCA will not happen? Could the check valve and the MOV be opened from causes other than ruptures?

An evaluation of American nuclear operating experience by the author while he was at the NRC some 30 years ago indicated that indeed these valves could be opened from causes other than ruptures, and over-pressurization of the ECCS has actually occurred. Over a stretch of about 10 years, several nuclear power plants of the BWR type had their check valve and MOV on one of their ECCS inadvertently opened at the same time. There were many causes for their simultaneous inadvertent openings, but none due to instantaneous rupture. For example, at one plant, a testable check valve was cranked open by a mechanical technician to conform to an erroneous open signal. The erroneous open signal was caused by an electrician who reversed the signaling wires. This lasted for a prolonged period. Then a routine operating test of the MOV led to the complete opening of the injection pathway, and the subsequent over-pressurization of that ECCS system. At another plant, an obstruction by debris of a check valve was not noticed.

Then an online testing of the MOV led to an over-pressurization of that ECCS system. The NRC took these events very seriously, and implemented immediate and appropriate regulatory actions to have the problems expeditiously fixed to prevent their recurrences. One obvious solution was to deactivate the testable check valves, and to tighten the online testing procedures for the ECCS injection MOV.

What saved the BWR ECCS from rupturing was the fact that the BWR reactor operating pressure was relatively low (about a thousand pounds per square inch), as compared to that of a PWR. Therefore the mechanically robust BWR ECCS could withstand that overpressure. Only a few pump seals and gaskets were blown.

A very important question to ask: would the ECCS in a PWR with reactor operating pressure twice that for a BWR be vulnerable to such an over-pressurization?

4.5 A Spent Fuel Pool Loss of Cooling or Loss of Inventory

No conceivable chain of events …

The fifth accident scenario is the loss of cooling or the loss of inventory of the spent fuel pool. This scenario was judged to be very unlikely because of several considerations. First, the cooling system for the spent fuel pool is relatively simple, and requires relatively low heat removal capability, as opposed to the ECCS systems' huge capacity upon instant demand. Second, the spent fuel pool has a massive amount of water, hence upon a rather unlikely loss of its cooling capability, it would take a long time, in the order of days, for the water to evaporate to the level where the spent fuels would be exposed. With the availability of such a long time, many actions could be taken by plant personnel to correct whatever problems causing the initial loss of cooling. Finally, as to the rapid loss of inventory of the spent fuel pool, in contrast to the comparatively slower boiling off of the pool water, the common incidents observed in the past mostly involved inadvertent draining of the pool. The occurrence of these draining events have led to the installation of hydraulic dams and water level alarms which effectively prevent the recurrence of such incidents. Therefore there appeared to be no credible sequence of events which would lead to the uncovering of the spent fuels in a spent fuel pool.

… but Fukushima changed the game … again

This assessment of very low likelihood of occurrence for spent fuel pool accidents remained valid for a long time, until the Fukushima Daiichi accident. There, not only one, but four spent fuel pools (at reactor units 1, 2, 3, and 4) lost their cooling for an extended period of time after the tsunami and explosions. The detailed reasons for the loss of cooling of the spent fuel pools at Fukushima are still being investigated. Water in the spent fuel pools might have been lost due to sloshing of the pools from the 9.0-magnitude earthquake, or from evaporation due to the loss of cooling for an extended period. Hydrogen explosions might have also damaged equipment essential for cooling the spent fuel pools.

4.6 Multiple Reactor Accidents

Unlikely x unlikely = extremely unlikely

The sixth accident scenario is one where multiple reactor units are involved, the truest, purest and rarest of the black swans. If the term "black swan" means extreme rarity, then the truest of the black swans means impossibility. With estimated likelihood of a major nuclear reactor accident in a single reactor deemed very unlikely, the estimated likelihood of multiple units involvement was vanishingly small. Both the Three Mile Island and Chernobyl nuclear accident happened at a single reactor unit, and their occurrences were commonly deemed anomalies. Therefore, before the Fukushima Daiichi accident, the argument that this truest black swan of accidents, namely an accident enveloping multiple units, being extremely rare appeared to be valid. After all, no nuclear accident involving a single reactor unit happened at any of the BWRs or PWRs worldwide with any site-boundary release of radioactive material since and including the TMI accident.

… but then Fukushima …

At Fukushima Daiichi, three nuclear reactors were involved at the same time, and all of them have melted. Additionally, as mentioned earlier, four spent fuel pools at four different reactor units lost their cooling for an extended period of time.

5

The Unlikely Has Happened

Table 2 is most telling.

Table 2: Likelihood Estimates

THE TOP FIVE BLACK SWANS		
Station Blackout	Extremely Unlikely	Occurred
Anticipated Transient Without Scram (ATWS)	Extremely Unlikely	?
Reactor Vessel Rupture	Extremely Unlikely	?
Interfacing Loss of Coolant Accident (Interfacing LOCA)	Extremely Unlikely	?
Spent Fuel Pool Loss of Cooling	Extremely Unlikely	Occurred
THE RAREST BLACK SWAN		
Multiple Reactor Accidents	Absoluted Unlikely	Occurred

Before the Fukushima Daiichi accident, all six nuclear black swans were estimated to be extremely unlikely. As explained earlier, these estimates were based on systematic and extensive studies with seemingly meritorious approaches. For a long time, these estimates seemed to be scientifically defensible.

Then three of the six nuclear black swans happened at Fukushima Daiichi: a Station Blackout, a Spent Fuel Pool accident; and a triple reactor meltdown.

Low likelihood – huge impacts

A compelling observation here is that being assigned a low likelihood of occurrence does not mean a well-studied nuclear reactor accident will not happen. These types of rare events, even when every effort was made to mitigate their impact, if and when they occur, incur staggering damage to property and the environment, not to mention the enormous suffering to the population living within the evacuation zone of the facility. The disastrous consequences, after the Chernobyl accident 25 years ago, are again well evidenced in the Fukushima Daiichi accident.

6

The Way Forward

Abandoning nuclear power – pros and cons

The only sure way to avoid any nuclear reactor accident is to disengage completely from nuclear power production, as Germany and Switzerland are planning to do. This approach requires national will and political consensus, and perhaps more importantly, the development and execution of a realistic plan to replace the significant loss of electricity production from nuclear power. A dramatic adjustment in how electricity is consumed and produced in the transitional period is crucial. The adverse impact on a nation's economy may be substantial. A continuing reliance on fossil fuels and their associated harmful carbon and pollutant emission would have to be tolerated. However, these draconian measures and serious hardships may lead to an acceleration of the development of renewable energy such as wind and solar power.

Retaining nuclear power – three crucial steps

Another approach would be to continue to rely on nuclear power, but take the following three important steps to maintain and improve nuclear reactor safety. The merits of the first two steps are obvious.

Regulatory oversight

First, there should be increased regulatory oversight and enforcement of nuclear reactor safety.

Industry vigilance

Second, there should be increased industry vigilance in all aspects of design, manufacture, installation, operation, and maintenance of nuclear power. A continuing strong focus on good practice and safety culture is equally necessary.

Dismissing rare events is no longer sufficient

Third, take a new look at the rare but high-consequence events with a fundamentally different perspective from the past. Dismissing such rare accidents based on their estimated low likelihood of occurrence, no matter how robust the underlying analyses are, is no longer sufficient to ensure the safety of nuclear power. At Fukushima Daiichi, not only one but three nuclear black swans showed up, while none should be expected. Instead of dismissing rare but high-consequence accidents purely from their estimated low likelihood of occurrence, one should look for additional cost-effective means to prevent their occurrence and to mitigate their impact if they were to occur. A simple dismissal based on seemingly valid analysis should not be relied upon again.

Prevention costs should be measured against scale of disaster

These are difficult endeavors. Especially the third step. Nuclear power technology being complex and unforgiving, the weighing and balancing the costs and benefits of any proposed measures, as well as how to gauge the effectiveness of such measures are exceedingly demanding tasks. For example, in hindsight, designing the Fukushima Daiichi nuclear power plant to protect against a once-in-a-thousand-year tsunami would have been a better idea, albeit more costly. Nevertheless, 40 years ago at Fukushima Daiichi, designing it against a once-in-300-year tsunami, as compared to the American standard of once-in-100-year flood protection, appeared at that time to be adequate. This sense of adequacy was rooted in two notions. First, the likelihood of occurrence of such a big tsunami was thought to be miniscule, and secondly, many means were thought to be available to plant personnel for dealing with a big tsunami. If the actual immense economic damage was used in any cost-benefit analysis, prevention measures against a once-in-a-thousand-year tsunami would have been more than justifiable.

Regarding how to prevent a nuclear black swan, a rare but nasty nuclear reactor accident, one should note that a great deal of effort has already been spent in the past for this purpose. One should not reinvent the wheel here. Rather, the emphasis should be on additional means not considered before, and on the cost-effective nature of the measure. There is not enough money in the world to plan for any and all conceivable things that can go wrong.

Identifying cost-effective "insurance" measures

Take the case of an Anticipated Transient Without Scram. For the BWRs, the automatic depressurization system (ADS) may be activated as a last-ditch effort to mitigate a fast and furiously unfolding accident when the reactor fails to scram. The ADS system, equipped with explosive valves, would dump the water and steam from the reactor vessel into the containment, buying precious time for the reactor operators to take other actions (the reactor vessel and the containment structure would not be useable again, but that is another matter). Questions to ask: Is there more that can be done? More importantly, for the PWRs, which do not have an ADS system, what, if any, additional cost-effective measures should be implemented?

7

Conclusions

A sense of perspective

In any serious debate about nuclear reactor safety, there should always be a delicate balance. On one hand, one should not only speak in apocalyptic tones about how dangerous nuclear power is. Nor should one be an alarmist who insists the sky is falling. On the other hand, one should not rely solely on the prevailing nuclear power plant operational experience nor governmental and nuclear industry analyses or promotional material, if any, to maintain that there is nothing to worry about nuclear reactor safety.

Both proponents and opponents of nuclear power have a host of grievances against each other. These grievances generally follow the lines that nuclear power is fundamentally safe or it is inherently dangerous. The truth is probably somewhere in between. There is no doubt that nuclear power is a complex technology, and can sometimes be dangerous and unforgiving. But nuclear power safety has been heavily regulated and scrutinized for longer than four decades. The global nuclear industry's safety record, though seriously blemished by the accidents at TMI, Chernobyl, and Fukushima, can still claim that 99% of nuclear power plants have been operating safely. More importantly, further improvement in nuclear power safety appears to be feasible.

Safety – a continuous endeavor

In conclusion, if we choose to increase the utilization of nuclear power or choose to keep nuclear power at the current level until alternative energy sources are developed, our urgent priority should be on how to maintain and improve nuclear reactor safety. This means, first and foremost, the prevention of severe nuclear accidents and the mitigation of their enormous consequences upon their unexpected arrivals. A structured, focused and transparent effort is both desirable and necessary for the consideration and debate on how to proceed.

Plan for all six black swans

As an example of what should be debated on preventing and mitigating severe nuclear accidents, take the current approach adopted by the global nuclear industry and many governments on learning from the Fukushima Daiichi accident. The tremendous current worldwide efforts are focusing only on the three severe nuclear accidents previously estimated improbable but had occurred, namely a Station Blackout; a Loss of Spent Fuel Pool Cooling; and a triple core melt. These are commendable and appropriate efforts. However, what about the other three severe nuclear accidents (a Reactor Vessel Rupture; an Interfacing LOCA; and an ATWS) which were also deemed unlikely in the past? Table 2 is most telling. Three of the six nuclear black swans have already shown up at Fukushima Daiichi. It is time to re-examine the other three severe nuclear accidents to ensure they do not happen, and to plan for mitigating their terrible consequences just in case they do.

思匯
CIVIC EXCHANGE

Room 701, Hoseinee House, 69 Wyndham Street, Central, Hong Kong
T (852) 2893 0213   F (852) 3105 9713   www.civic-exchange.org