As of: May 07, 2012
Received: May 04, 2012
Status: Pending_Post
Tracking No. 8100527c
Comments Due: May 04, 2012
Submission Type: Web

38

PUBLIC SUBMISSION

Docket: NRC-2011-0299
Station Blackout Mitigation

Comment On: NRC-2011-0299-0001
Station Blackout

Document: NRC-2011-0299-DRAFT-0035
Comment on FR Doc # 2012-06665

Submitter Information

Name: Anthony Apostolides, Ph.D.
Address: United States,

General Comment

1. Subject: Docket ID NRC-2011-0299

2. The NRC issued the ANPR to begin the process of considering amendments of its regulations that address a condition known as station blackout (SBO). SBO involves the loss of all onsite and offsite alternating current (ac) power at a nuclear power plant.

3. p. 16177 (of the ANRP); GDC-2, #(1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin...

Comment: The past is often not a reliable indication of what may happen in the future. In the future, there may occur random/unexpected events that did not happen in the past. These would be "black swans", as happened in the recent financial collapse. A grim example of this is what happened in Fukushima: the Japanese nuclear authorities thought their nuclear power plants were safe, but they were very wrong; and their country is now paying heavy consequences for their incompetence. The NRC should learn the severe lessons of Fukushima – which are continuing and seem to be worsening over time. The same thing, with different factors/weather conditions, etc., can well happen in the U.S. In that event, the nuclear power plants would have exposed nuclear fuel pools and – more importantly – exposed spent fuel pools.
(See Attachment)

Attachments

COMMENTS-NRC-ANRP-1

Template = SECY-067

DS10

COMMENTS ON NRC ADVANCE NOTICE OF PROPOSED RULEMAKING - Docket ID NRC-2011-0299 [Comments-NRC-ANPR.doc]

1. Subject: Docket ID NRC-2011-0299

2. The NRC issued the ANPR to begin the process of considering amendments of its regulations that address a condition known as station blackout (SBO). SBO involves the loss of all onsite and offsite alternating current (ac) power at a nuclear power plant.

3. p. 16177 (of the ANRP); GDC-2, #(1) Appropriate consideration of the most severe of the natural phenomena that have been historically reported for the site and surrounding area, with sufficient margin...

Comment: The past is often not a reliable indication of what may happen in the future. In the future, there may occur random/unexpected events that did not happen in the past. These would be "black swans", as happened in the recent financial collapse. A grim example of this is what happened in Fukushima: the Japanese nuclear authorities thought their nuclear power plants were safe, but they were very wrong; and their country is now paying heavy consequences for their incompetence. The NRC should learn the severe lessons of Fukushima - which are continuing and seem to be worsening over time. The same thing, with different factors/weather conditions, etc., can well happen in the U.S. In that event, the nuclear power plants would have exposed nuclear fuel pools and - more importantly - exposed spent fuel pools.

In the event of a catastrophic event that takes down the electric grid and a number of transformers, the nuclear power plants will not have electricity (after 7-28 days if they can use their back-up fuel generators - according to information form NRC staff). When/if the nuclear fuel pools and the nuclear spent fuel pools run out of water, the results will be dismal. Radiation will be released - as in Fukushima - from both of these pools, and especially from the spent fuel pools which have many more nuclear rods than the nuclear fuel pools. Radiation of various types will be released in the air, water, and soil. The wind and water will carry radioactive releases to the environment. The distance in which they will be carried in the air will depend on wind power and direction. It is known that rain will bring these releases to the ground, where they will contaminate plants, which will then be eaten by cows, which will be gotten into cows milk and drunk by people, etc.

4. p. 16178 (of the ANRP); second paragraph. "In fact, risk analyses performed for nuclear power plants indicate that the loss of all ac power can be a significant contributor to the risk associated with plant operation, contributing more than 70 percent of the overall risk at some plants."

Comment: The text shows that the NRC has come to recognize the enormous importance of power to a nuclear power plant - which needs power 24 hours a day in order to be prevented from releases nuclear material in the environment. It is of paramount importance to fix this problem soon.

5. p. 16178 (of the ANRP); second column; second paragraph. "The Commission issued the SBO rule based on operating experience suggesting that both onsite emergency ac power systems and offsite power from the transmission network **might be less reliable than originally anticipated**, [emphasis mine] even for plants designed to meet GDC 17 of appendix A to 10 CFR part 50."

Comment: This is a most important point - that the power system might be less reliable than originally anticipated. The NRC has recognized the risks of loss of power of nuclear power plants. It did not do anything about that in the past. Now, it is trying to do something to fix that severe problem.

One wonders why it was the petition of an individual (Mr. Popik) that resulted in this proposed rule activity and not of the NRC itself.

5. p. 16178; third column; first paragraph. ".., it was concluded that there was a sufficiently low likelihood of a LOOP [loss of offsite power] generated by a fire, flood, or seismic activity and that ..."

Comment: This conclusion, of low likelihood, can be very wrong. This was the conclusion reached by the Japanese nuclear regulatory authorities, and the Japanese people are now paying the very heavy price for that mistaken conclusion.

6. p. 16178; third column; third paragraph. "However, the parameters that were used for inputs into both the determination

of the specified duration and the SBO coping analysis are subject to change over time."

Comment: The NRC recognizes that things can change over time. This should lead to changes in regulations of nuclear power plants. Changes have certainly happened in the perception of risks in the cutting of power facing nuclear power plants.

The basic and horrendous problem with nuclear power plants is that they are eternal prisoners to electric power - and with them, the U.S. society is prisoner to electric power. That is, the nuclear power plants require electric power 24 hours a day. Without that power, they can become deadly weapons. To explain: Nuclear power plants require electric power continually, in order to circulate water, in order to: 1) Maintain their nuclear fuel rods at a certain temperature, and 2) Maintain at a certain temperature, their nuclear spent fuel which are typically "stored" in swimming pools, and which are much more than their fuel rods. The accumulation of spent fuel rods is the abysmal result of the government not being able to find a state to accept those tons of radioactive waste.

The nuclear power plants have back-up power from generators, but this power is for only 7 plus 28 days (according to information provided by NRC staff). After 30 some days, the nuclear power plants have no electric power.

When there is no electric power, the water in the fuel rods and the spent fuel pool will evaporate - as in Fukushima. This will result in the release of radioactive material to the environment. There can also be a meltdown of the radioactive rods into the earth. At a minimum that will result in radioactive material being spewed in the soil; it can subsequently go into underground water and travel well beyond the nuclear power plant.

Three Causes of Loss of Electricity of Nuclear Power Plants and Their Fatal Impacts

The three possible causes that can result in long-term loss of electricity to nuclear power plants are: 1) Solar storm, 2) Cyber attack, and 3) Nuclear detonation in the air. The loss of electricity from these causes can last several months - according to one estimate, it can last 1 to 2 years. With that

situation, there will be no food in stores, no water from local water systems, and no medications for the population of the U.S. - for 1 to 2 years (besides other adverse effects). Needless to say, the results of these effects to the U.S. population will be catastrophic: one estimate puts the resultant numbers of fatalities in the U.S. at **200,000,000 people** - a stunning number (2012 Cyber Security Regional Conference, April 2012, Hagerstown, MD).

A main cause of the catastrophic effects is the three causes, noted above, resulting in the knocking down of the transformers of the electric grid of the U.S. Without transformers, there is no electricity. The replacement of the transformers is expected to take 1 to 2 years; the U.S. does not make them, and it takes a long time to produce them. If there is no electricity in the countries that produce them, that would make it even more difficult to eventually replace them in the U.S.

The three potential causes are described below:

1) Solar Storm

A solar storm originates in the sun, and is directed to the earth. If strong enough, it can overload the electric grid, and knock down (melts the windings of) power transformers, an integral part of the U.S. electric grid. Because the electric grid in the U.S. has become interconnected over time, electricity can be lost to the entire U.S. or to a large part of the U.S. (e.g., eastern U.S.). The replacement of the damaged transformers would take 1 to 2 years; thus, the U.S. (or a large part of it) will be without electricity of 1 to 2 years. The catastrophic consequences of this, in terms of lives lost, were described above. Also, if a large part of the U.S. (e.g., eastern U.S.) was without electricity for 2 years, that would result in a chaotic situation in the entire - with respect to water, water, and medications.

According to a 2010 NASA article on solar storms ("Solar Shield-Protecting the North American Power Grid", October 26, 2010;http://science.nasa.gov/science-news/science-at-nasa/2010/26oct_solarshield/):

Excerpt from the article:

"The troublemaker for power grids is the "GIC" – short for geomagnetically induced current. When a coronal mass ejection (a billion-ton solar storm cloud) hits Earth's magnetic field, the impact causes the field to shake and quiver. These magnetic vibrations induce currents almost everywhere, from Earth's upper

atmosphere to the ground beneath our feet. Powerful GICs can overload circuits, trip breakers, and in extreme cases melt the windings of heavy-duty transformers.

This actually happened in Quebec on March 13, 1989, when a geomagnetic storm much less severe than the Carrington Event knocked out power across the entire province for more than nine hours. The storm damaged transformers in Quebec, New Jersey, and Great Britain, and caused more than 200 power anomalies across the USA from the eastern seaboard to the Pacific Northwest. A similar series of "Halloween storms" in October 2003 triggered a regional blackout in southern Sweden and may have damaged transformers in South Africa.

While many utilities have taken steps to fortify their grids, the overall situation has only gotten worse. A 2009 report by the North American Electric Reliability Corporation (NERC) and the US Department of Energy concluded that modern power systems have a "significantly enhance[d] vulnerability and exposure to effects of a severe geomagnetic storm."

That's the surprising conclusion of a NASA-funded study by the National Academy of Sciences entitled Severe Space Weather Events—Understanding Societal and Economic Impacts. In the 132-page report, experts detailed what might happen to our modern, high-tech society in the event of a "super solar flare" followed by an extreme geomagnetic storm. They found that almost nothing is immune from space weather—not even the water in your bathroom."

"The problem begins with the electric power grid. "Electric power is modern society's cornerstone technology on which virtually all other infrastructures and services depend," the report notes. Yet it is particularly vulnerable to bad space weather. Ground currents induced during geomagnetic storms can actually melt the copper windings of transformers at the heart of many power distribution systems. Sprawling power lines act like antennas, picking up the currents and spreading the problem over a wide area. The most famous geomagnetic power outage happened during a space storm in March 1989 when six million people in Quebec lost power for 9 hours:"

"According to the report, power grids may be more vulnerable than ever. The problem is interconnectedness. In recent years, utilities have joined grids together to allow long-distance transmission of low-cost power to areas of sudden demand. On a hot summer day in California, for instance, people in Los Angeles might be running their air conditioners on power routed from Oregon. It makes economic sense—but not necessarily geomagnetic sense. Interconnectedness makes the system susceptible to wide-ranging "cascade failures.""

"To estimate the scale of such a failure, report co-author John Kappenmann of the Metatech Corporation looked at the great geomagnetic storm of May 1921, which produced ground currents as much as ten times stronger than the 1989 Quebec storm, and modeled its effect on the modern power grid. He found more than 350 transformers at risk of permanent damage and 130 million people without power. The loss of electricity would ripple across the social infrastructure with "water distribution affected within several hours; perishable foods and medications lost in 12-24 hours; loss of heating/air conditioning, sewage disposal, phone service, fuel re-supply and so on."

"The concept of interdependency," the report notes, "is evident in the unavailability of water due to long-term outage of electric power–and the inability to restart an electric generator without water on site.""

A large-scale blackout could last a long time, mainly due to transformer damage. As the National Academy report notes, "these multi-ton apparatus cannot be repaired in the field, and if damaged in this manner they need to be replaced with new units which have lead times of 12 months or more."

... Credit: National Academy of Sciences."

2) Cyber Warfare:

Cyber warfare refers to a group of hackers gaining excess, electronically, to the U.S. electric power grid, overloading segments of that grid, and knocking down power transformers. The loss of transformers and other equipment will result in a long time of no electricity in all, or parts, of the U.S. - depending on the extent of the attack. The lack of electricity will result in lack of flowing water in nuclear power plants - in the nuclear fuel pool and in their spent fuel pool. That would result in Fukushima-type catastrophic consequences (Fukushima's situation has been worsening over time). The lack of electricity will also have the dire consequences, on human life, described above.

Cyber Warfare is a serious threat to nuclear power plants. Their control systems include the SCADA (Supervisory Control and Data Acquisition) systems developed by Siemens. SCADA systems control industrial facilities like nuclear power plants, and power grids. It is known that the Stuxnet virus has attacked these SCADA systems in the past; thus, nuclear power plants are most vulnerable to this virus. And, there may well be other electronic viruses in the future.

A CBS news article titled "Cyber War: Sabotaging the System" on June 15, 2010, talks about the threat of cyber warfare on our infrastructure (http://www.cbsnews.com/2100-18560_162-5555565.html). An excerpt of that article is provided below:

"Until February of this year, McConnell was the nation's top spy. As chief of national intelligence, he oversaw the Central Intelligence Agency, the Defense Intelligence Agency and the National Security Agency. Few people know as much about cyber warfare, and our dependency on the power grid, and the computer networks that deliver our oil and gas, pump and purify our water, keep track of our money, and operate our transportation systems.

"If I were an attacker and I wanted to do strategic damage to the United States, I would either take the cold of winter or the heat of summer, I probably would sack electric power on the U.S. East Coast, maybe the West Coast, and attempt to cause a cascading effect. All of those things are in the art of the possible from a sophisticated attacker," McConnell explained.

"Do you believe our adversaries have the capability of bringing down a power grid?" Kroft asked.

"I do," McConnell replied.

Asked if the U.S. is prepared for such an attack, McConnell told Kroft, "No. The United States is not prepared for such an attack."

"It is now clear this cyber threat is one [of] the most serious economic and national security challenges we face as a nation," President Obama said during a speech.

Four months after taking office, Obama made those concerns part of our national defense policy, declaring the country's digital infrastructure a strategic asset, and confirming that cyber warfare had moved beyond theory.

"We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness," the president said.

President Obama didn't say which country had been plunged into darkness, but a half a dozen sources in the military, intelligence, and private security communities have told us the president was referring to Brazil.

Several prominent intelligence sources confirmed that there were a series of cyber attacks in Brazil: one north of Rio de Janeiro in January 2005 that affected three cities and tens of thousands of people, and another, much larger event beginning on Sept. 26, 2007.

That one in the state of Espirito Santo affected more than three million people in dozens of cities over a two-day period, causing major disruptions. In Vitoria, the world's largest iron ore producer had seven plants knocked offline, costing the company $7 million. It is not clear who did it or what the motive was.

But the people who do these sorts of things are no longer teenagers making mischief. They're now likely to be highly trained soldiers with the Chinese army or part of an organized crime group in Russia, Europe or the Americas.

"They can disrupt critical infrastructure, wipe databases. We know they can rob banks. So, it's a much bigger and more serious threat," explained Jim Lewis, director of the Center for Strategic and International Studies.

Lewis led a group that prepared a major report on cyber security for President Obama.

"What was it that made the government begin to take this seriously?" Kroft asked.

"In 2007 we probably had our electronic Pearl Harbor. It was an espionage Pearl Harbor," Lewis said. "Some unknown foreign power, and honestly, we don't know who it is, broke into the Department of Defense, to the Department of State, the Department of Commerce, probably the Department of Energy, probably NASA. They broke into all of the high tech agencies, all of the military agencies, and downloaded terabytes of information."
How much is a terabyte?

"The Library of Congress, which has millions of volumes, is about 12 terabytes. So, we probably lost the equivalent of a Library of Congress worth of government information in 2007," Lewis explained.

"All stolen by foreign countries?" Kroft asked.

"Yeah. This was a serious attack. And that's really what made people wake up and say, 'Hey, we've got to get a grip on this,'" Lewis said."

3) EMP from a Nuclear Detonation

An EMP, or Electromagnetic Pulse, from a nuclear detonation high in the air, is the third major threat to nuclear power plants. Such a detonation can knock down the electric grid (or large portions of it - by knocking down power transformers and other equipment. This EMP will also render useless the vast majority

of vehicles that use modern electronics in their engines. It will also incapacitate airplanes, through their electronics.

The consequences of such an attack are similar to those previously described above. In addition, the transportation system of the U.S. will be useless; this includes airplanes that were airborne at the time of the attack, falling to the ground.

4) Possible Solutions

1]. Harden power transformers so that they can withstand solar storms, cyber attacks, and EMPs from nuclear detonations. This is technically possible and affordable.

2]. Have the nuclear power plants use a number of redundant power systems. Thesw could include propane systems; and alternative energy systems, such as solar and wind systems.

3]. Have the nuclear power plants be not on the electric grod of the U.S. but have their own electrical systems. These could include the systems noted above in #2.

4]. Separate the spent nuclear fuel from the reactor and put that fuel in a separate geographic area. As soon as possible, put the spent fuel in dry casks.

5]. Most risks of solar storms, cyber attacks, and EMPs from nuclear detonations are eliminated if the nuclear power plants are shut down. Risks would remain with the existing spent nuclear fuel - which are considerable - but they would not increase.

Sincerely,

Anthony Apostolides, Ph.D.
Email: Anthonya@pattyapostolides.com

Rulemaking Comments

From: Gallagher, Carol
Sent: Monday, May 07, 2012 12:37 PM
To: Rulemaking Comments
Subject: Comment on Station Blackout ANPR
Attachments: NRC-2011-0299-DRAFT-0035.pdf

Attached for docketing is a comment from Anthony Apostolides on the above noted ANPR (77 FR 16175; March 20, 2012) that I received via the regulations.gov website on May 4, 2012.

Thanks,
Carol