NUCLEAR POWER PLANT SECURITY CONCERNS AND RECOMMENDATIONS

Nuclear plant security concerns in Ukraine

Concerns

1. Ukraine has 15 civilian nuclear power reactors including six at ZNPP.
2. Deliberate shelling of ZNPP has disconnected it from the power grid multiple times, each time jeopardizing safety systems that cool the reactor cores and the spent fuel storage pools. Shelling damaged the site, disrupting its connection to external power, and "raising fears of a possible meltdown." In addition to posing a risk of a reactor core meltdown, if the water in the pools were to evaporate, the zirconium cladding of the spent fuel assemblies could heat up and ignite, causing a nuclear conflagration that could release large amounts of radioactivity.
3. Ukraine President Zelenskyy warned of a plot to breach a dam near ZNPP. If the dam were breached, the surface water supply to ZNPP would drain away, raising additional risks of losing cooling and possible meltdown.
4. According to the IAEA, Ukraine's Khmelnytskyi (KhNPP) and Rivne (RNPP) nuclear power plants suffered massive Russian shelling on November 15, 2022, causing loss of external power and forcing the reactors to shut down.
5. In an act decried as "nuclear terrorism," on September 19, 2022 a missile came within 1000 feet of hitting Pivdennoukrainsk, Ukraine's second largest nuclear plant, also known as the South Ukraine Nuclear Power Plant (SUNPP). SUNPP is on the front lines of the conflict and remains at risk as Russian missiles and shelling continue to hit the nearby city of Mikholaiv.

Recommendations

1. Support in all political arenas the IAEA's call to establish mandatory de-militarization and targeting zones around all nuclear plants and waste sites, not just in Ukraine, but worldwide.
2. Understanding that power grids feeding operational power to reactors lay largely outside of these proposed Zones, support binding international standards for:
    - Required supply of diesel fuel for onsite emergency generators
    - Creation of mobile emergency response units within all nations operating nuclear power stations
    - Diplomatic immunity for all IAEA staff, allowing them freedom of access to and necessary protection required to any nuclear reactor
    - Amending all international agreements such that any attack on any nuclear facility – intentional or accidental – or use of such facilities for any military purpose would be characterized as a crime against humanity, and a war crime in areas of declared or de facto conflicts

Nuclear plant security concerns in the United States

Vulnerable reactors and radioactive waste

1. The United States currently has 92 operating reactors, two more that are slated to start up in the next year, and 37 that are either closed or undergoing decommissioning. Theese plants are vulnerable to sabotage, terrorism, cyberattack,

dam breaches, and other threats of a deliberate nature. These include small "determined intruder" assaults, and hackers attacking US nuclear plants and/or surrounding infrastructure remotely. Cyberattacks have the potential to hijack key components, cut plants off from the power and water supply required for cooling, and ultimately release large amounts of radioactivity.

2. The US inventory of high-level radioactive waste including highly irradiated nuclear fuel (often called "spent fuel") is also vulnerable to attack.
3. Shipping this waste to/from proposed consolidated interim storage facilities (CISFs) compounds this risk. Regarding spent fuel transport, the National Sierra Club Nuclear Waste Task Force warned that "potential terrorism and national security measures have not been shared with the public. Many emergency responders are volunteers with little training for hazardous materials and even less for radiological incidents. The National Transportation Safety Board (NTSB) should be put in charge of radioactive shipments and require redundant safety measures that protect the public from potential disasters." Beyond Nuclear raised these and other issues concerning spent nuclear fuel transport security in a February 25, 2022 letter to US Department of Transportation Secretary Pete Buttigieg. DOT has yet to respond. In 2018 NTSB Chair Jennifer Homendy provided written testimony to Congress pointing out that even if NTSB's recommended safety measures were implemented (which they aren't) transporting nuclear waste had inherent risks which would not be eliminated.

Downplaying and dismissing security risks

1. Whatever has already happened can happen again. Now that nuclear power plants in Ukraine have actually been attacked, no one can dismiss the threat of attacks on nuclear facilities elsewhere, including in the US, as anything less than credible.
2. After one of the planes that destroyed the World Trade Center on 9/11 flew directly over the Indian Point nuclear plant, Al Qaeda leaders said they planned to attack Indian Point and one other nuclear plant, and reserved the right to do so in the future. At the time, the National Research Council rated the risk of a terrorist attack on US nuclear plants as "high" and civil society called for stronger security measures, including air defense, no-fly zones, and security cordons.
3. A 2013 study conducted by University of Texas at Austin found that all civilian nuclear plants in the U.S. were insufficiently protected from "credible" terrorist threats, including acts of sabotage capable of causing a meltdown, and theft of weapons-grade nuclear material.
4. A 2015 Chatham House report found that nuclear plants are highly vulnerable to cyberattack.
5. Around the time of the independent studies cited above, NRC issued its own assessments based on new, NRC staff-created methodologies that minimized risks and portrayed threats as virtually nonexistent, utterly contradicting previous studies the NRC had commissioned which analyzed the exact same data. Today, even as the threat environment worsens and nuclear plants are attacked in Ukraine, the NRC still treats domestic nuclear plant security as the prerogative of the private plant owner, and fails to take the risk of attack seriously.
6. This is consistent with a pattern of NRC modeling using internally generated algorithms to deny and ignore risks it previously acknowledged. For example, NRC's 2012 "State-of-the-Art Reactor Consequence Analyses" (SOARCA), last updated in 2020, used an algorithm created by NRC staff to conclude that a reactor accident in the U.S. would have "essentially no risk of death during or shortly after the accident, [with] longer term cancer fatality risks…millions of times lower than the general U.S. cancer fatality risk." In 2014 NRC published an updated Spent Fuel Transportation Risk Assessment which reexamined previously assessed data, this time using a

different methodology devised by NRC staff. Although it assessed the same data, the results were utterly different, cutting transportation risks by five orders of magnitude compared to previous reports, effectively reducing the risk to zero.

Security decisions are left up to plant owners

1. Plant owners have an incentive to cut costs and maximize profits. They fund 90% of the NRC's budget and the NRC refers to them as its "clients." Not surprisingly, the NRC has a history of lax regulation, eagerness to comply with owners' requests for regulatory relief, and dismissing as "not credible" threats which would be expensive for owners to redress.
2. Just as inadequate government oversight led to the Boeing 737MAX crashes and the East Palestine, Ohio train derailment, lax regulation of the nuclear industry encourages self-regulation which won't protect the public from security threats. Yet nuclear plant security measures are largely left up to licensees, who have a disincentive to implement adequate ones. Independent analysis shows this approach has failed, and that as a result, US nuclear plants are not secure.
3. In the wake of 9/11 then Homeland Security Director Thomas Ridge asserted that nuclear plant security was the "prerogative" of the nuclear plant owner, and the US government declined to require additional air defense or other security measures beyond what private owners were willing to provide. In theory, the Department of Homeland Security is supposed to play a major role in defending nuclear power plants from attack. In practice, this has yet to be demonstrated, and there is reason to worry that responsibility for nuclear plant security has fallen through the cracks. Delegating security decisions to plant owners will not protect the public.
4. After 9/11 the Ninth Circuit Court did require the US Nuclear Regulatory Commission (NRC) to do a study on enhancing security of spent fuel stored at nuclear power plants. But then as now, security decisions are left up to the licensees.
5. For example, rather than spend money to expand security guard staff after 9/11, plant owners worked their existing staffs harder -- up to 72 hours a week -- to avoid hiring and training new guards. This saved the owners money, but plant security suffered. The NRC treats plant owner's private security guard arrangements as a buyer of a short period of time – perhaps half an hour – until other responders such as police, the military, etc. arrive to defend against the threat. This is unrealistic thinking; it has been shown not to work in many real-world incidents.
6. The NRC leaves it up to licensees to write and file Physical Security Plans which describe security measures they plan to take against terrorism and other threats. The NRC approves the Plans and does not make them public, so the public is unable to know what steps plant owners are and are not willing to take, and how they will or won't get implemented. Such secret NRC agreements with licensees are not a credible way to guarantee US nuclear plant security.

A deficient safety culture which fails to protect public health and safety and the environment

1. NRC's contention that any threats from or to US nuclear plants or waste are negligible or nonexistent reflects its internal culture, which is reactive, not proactive, and tightly connected to the interests of nuclear plant and radioactive waste dump owners. This is a blinkered view which has real-world consequences. It makes for a severely deficient safety culture and endangers Americans.
2. The NRC promises to "to alert its licensees if a specific, credible threat is identified." But if a credible terrorism threat emerged and the NRC alerted licensees, there would be little private plant owners could do to counter it.

3. The NRC takes a 'hands-off' approach to securing spent nuclear fuel. In 2006 the US 9th Circuit Court of Appeals ruled that the NRC was required under federal law to address the security of spent fuel in dry cask storage at Diablo Canyon. Even under court order, the security measures the NRC took to protect the casks were minimal. Its approach is inconsistent as well as inadequate. The NRC only recognizes its obligation to provide security for spent fuel in dry storage within the jurisdiction of the 9th circuit court that issued the order, and does not recognize such obligations in any other part of the country.

Doubling down on nuclear power compounds security threats

1. Increasing US reliance on nuclear power is touted as a climate solution, but it's no such thing. It's a dangerous mistake which would draw resources away from clean energy development and compound security threats.
2. In the U.S. as in the Ukraine, nuclear power plants and spent fuel storage facilities are pre-positioned potential radiological weapons that attackers could exploit. Extending operations of aging, obsolete nuclear plants beyond their design basis through extreme license extension and large subsidies, restarting or re-nuclearizing closed or decommissioned nuclear plants, building new nuclear facilities, and generally increasing reliance on nuclear power are dangerous practices which aggravate the threats described above. Yet they are becoming increasingly commonplace.
3. The Biden administration should therefore reconsider its current policy of seeking to expand the nuclear industry as if it were a clean energy source that could help fight climate change. In fact, it is far from clean; it generates lethal wastes and harmful emissions, makes climate change worse by siphoning resources away from renewables and efficiency, and poses serious security threats which cannot be eliminated.
4. So-called "advanced reactors" will also compound security and other threats. According to a March, 2021 Report, *"*"Advanced" Isn't Always Better,*"* by physicist Edwin Lyman of Union of Concerned Scientists, "advanced" reactors provide no added or enhanced safety value over current reactors, and introduce their own unique sets of operational and safety/security concerns
5. A May 2022 study in the *Proceedings of the National Academy of Sciences* co-authored by former NRC Chair Allison Macfarlane, small modular reactors (SMNRs) generate up to 30 times more lethal radioactive waste than conventional reactors per unit of electricity generated. Nevertheless, they are receiving generous federal funding.
6. SMNRs are being proposed which lack containment structures, reduce or eliminate emergency planning zones, and are exempt from Price Anderson Act coverage. Although proposed as underground/below-grade structures, the depth of bomb craters in Ukraine suggest that this may be totally inadequate to protect them from attack.

Nuclear plant security begins at home

The $35 million the US allocated last year to assist Ukraine with its nuclear plant security is a justified federal expenditure. But nuclear plant security begins at home. The US government must learn the lesson of Zaphorizhzhia -- that attacks on nuclear facilities are a credible threat and could happen here -- and prioritize domestic US nuclear plant security accordingly.

Recommendations

1. The US government must cease viewing nuclear plant security as the prerogative of the licensee and exert leadership to enhance and enforce security measures that make US nuclear plants harder targets, less vulnerable to attack.

2. Instead of siphoning billions of taxpayer dollars to subsidize and expand the nuclear industry, American taxpayers need the federal government to deliver adequate, mandatory security measures for existing nuclear facilities and spent nuclear fuel, the cost of which should be borne by the licensees, not the public.

3. These measures should be mandatory. They should not be left up to plant owners to plan and implement, and not treated as a matter solely for NRC regulation. They must be framed, verified, and implemented by federal agencies whose primary mission is to protect Americans' safety and security, and which are not beholden to the nuclear industry. Cost of implementation should be borne by licensees, not the public.

4. Nuclear plant site monitoring and security should be upgraded and undertaken by appropriate federal security agencies. Among other measures, Hardened Onsite Storage (HOSS) of spent nuclear fuel should be adopted immediately, and transfer of spent fuel from fuel pools to fortified dry storage that meets HOSS criteria should be expedited.

5. The Nuclear Waste Policy Act should be upheld, and not countermanded or modified to allow the US Department of Energy (DOE) to take title to spent nuclear fuel at civilian reactors, which would trigger thousands of vulnerable shipments of spent nuclear fuel by truck, train, and barge across the country to proposed consolidated interim storage facilities (CISFs) in Texas, New Mexico, and elsewhere.

6. Proposed CISFs, whether federal or privately owned, also need robust, mandatory security requirements, because spent nuclear fuel would be concentrated and stored at or barely below grade at these facilities, making them a potential target.

7. Federal funding for SMNRs should be withdrawn and eliminated, and the funds reallocated to effective, available clean, safe, secure alternatives such as renewables, energy efficiency, energy storage and transmission upgrades, so as to ramp up clean energy and phase out nuclear power as quickly as possible.