Joint Project Workshop on Nuclear Security with Oda Becker – Report

Date: April 24, 2017, 18:00 – 19:30h

Venue: Promenade 37, Room 210, 4020 Linz

Participants: 13 representatives of international NGOs and antinuclear movement

The risk of terrorism is increasing, but especially old nuclear power plants (NPPs) and interim storages for spent fuel have not been designed against possible terrorist attacks. To improve NGO´s know-how concerning nuclear security issues, the Joint Project commissioned the independent nuclear consultant Oda Becker with preparing a working paper. Oda Becker presented key parts of her working paper at the Joint Project Workshop.

The final version of the working paper will be available in June 2017 on the Joint Project's website www.joint-project.org/.

In the first part, Oda Becker presented an introduction into the topic of terror threats on nuclear facilities:

Introduction: While there are numerous potential targets for terrorist attacks (industrial plants, city centers or filled sports stadiums…), an attack on a NPP could be attractive for a terrorist group because of its immediate effect on power generation, its symbolic character (nuclear energy has a civilian/military character) and the global attention it would receive. Countries that are highly dependent on nuclear power could face a real dilemma: 85% of the 449 nuclear reactors in operation were built before the 9/11 attacks and were not designed with sabotage in mind.

Since 9 /11 2001, the public debate tends to concentrate on suicide attacks with a commercial airliner. In fact, the threat is much more diverse and complex. New possible means to support attacks emerge: Drones can be used for the preparation of terror attacks. In autumn 2014 drones flew over French nuclear facilities more than 30 times; until now it has not been possible to find out who is responsible for this action. And those drones pose a security threat to nuclear installations. And on top of this, attention needs to be devoted to one additional attack scenarios: cyber-attacks.

The design-basis threat (DBT) concept is used in security-related regulations. DBTs describe a set of adversary attributes that must be considered in the design of plant security systems. DBT is not designed to be the worst-case threat. It defines the upper limit within the total threat environment against which a nuclear plant licensee is required to ensure protection of the plants. Protecting against beyond-DBT threats falls into the responsibility of federal, state, and local authorities.

However, more formalized processes for identifying and analyzing threats—for example probabilistic risk assessment (PRA)—could help to improve security at nuclear plants. Even then the identification of scenarios may be incomplete, and the estimates developed through expert elicitation are subjective and can have large uncertainties. But nevertheless, risk assessment methods that focus on the risk triplet—scenarios, likelihoods, and consequences—can contribute with useful security insights.

Targets: Old NPPs are particularly vulnerable to external hazards. Their reactor cores are surrounded by a relatively thin-walled building (less than 1 m). If the reactor building is destroyed, it has to be assumed that the reactor's cooling circuit will be damaged and that safety systems will also suffer major damage. Such a case would thus in a short time – within few hours – lead to the meltdown of the reactor core. Radioactive substances will be released from the molten fuel and, since the containment will have been destroyed, they can get into the open basically without any delay or retention inside the building.

The spent fuel storage pool is another vulnerable component with considerable radioactive inventory. In some plants, it can contain several times more fuel than the reactor itself. If a terror attack causes a breach of the concrete walls of a spent fuel pool, the cooling water will pour out. This causes the fuel to heat up due to the decay heat. Once the fuel reaches the temperatures of 900°C, the zirconium cladding starts to burn in air. The resulting fire is very hot and cannot be extinguished with water. Fire could spread to older fuel assemblies. If a spent fuel pool is subjected to an attack leading to loss of cooling water, the caesium inventory of up to 75% could be released.

Not only NPPs (reactor core but also spent fuel pools) are threatened by terror attacks, but also interim storages for spent fuel. Interesting in the workshop was the information that a German interim storage for spent fuel (Brunsbüttel) lost its licence because the operators were not able to prove in court[1] that the facility was protected against possible terror attacks, neither against an airbus crash or an attack with anti-tank guided weapons (DBT).

Consequences: All of the terror attacks discussed below as well as a crash of a commercial airline that causes a major damage of the reactor building would lead to accidents of the most severe category: core melt accident with open containment. The release would be especially high, e. g. in case of cesium-137 between 50 and 90 % of the core inventory. Radioactive substances would be released within a few hours. If an evacuation of the people should go wrong, then, depending upon the weather, hundreds of thousands of people could receive life-threatening doses.

Countermeasures: A decisive problem for reactor safety lies in the fact that although a quick interruption of the nuclear chain reaction can be achieved by a fast shut-down, that does nothing to stop heat developing through the radioactive decay of the fuel. Thus, if the cooling fails, a meltdown of the core can occur within a short period of time. The vulnerability of a NPP to attacks can be generally reduced by a shut-down of the plant. A shut-down conducted as a short-term measure against a terror attack, however, does not accomplish much.

[1]For more information (only in German) see http://www.atommuellreport.de/themen/zwischenlager/einzelansicht/das-brunsbuettel-urteil-und-seine-folgen.html, http://umweltfairaendern.de/wp-content/uploads/2013/06/Stellungnahme-SZL-Brunsbuettel.pdf,

One option for defending against terrorist attacks is to strengthen the facility's protection. This includes measures such as increasing the number and armament of security personnel, extending fencing, erecting barriers on approaches, etc.. Protection against attacks by land are doubtless improved by such measures. But insiders remain a problem. Also these measures do not help against attacks by air like drone overflights as can be seen in France.

In European countries flying over nuclear power plants within a radius of 5 km and at a height below 1,000 m is prohibited. Although no-fly zones around nuclear power plants reduce the risk of accidental crashes, this measure has no effect against a targeted attack. Likewise, air force interceptors can contribute only marginally to the protection of NPPs.

In the second part of the workshop, **three different terror scenarios** were provided by Oda Becker with the request to discuss among the participants if they were plausible and if the NGOs thought they were too detailed for the public. These scenarios included:

- Explosives attack by insiders with the aid of drones: a sleeper attack combined with drones for smuggling explosive devices into the nuclear facility: this seemed totally plausible to the participants, knowing that similar actions already happened (e.g. drones in France flying over NPPs in 2014 which could not be removed, and a Belgian jihadist who worked for three years as a technician with access to the control area of the Doel nuclear power plant).
- Terror attack by an anti-tank guided weapon: Use of anti-tank guided weapons (ATGW) for shooting a hole in the wall, through which the effect of a thermo-baric warhead could enter. In old NPPs, such an ATGW would be able to cause a severe accident, while in new NPPs the walls of the reactor building is be thicker and the safety systems are more separated which would make such an attack much more complicated. There is a black market for ATGWs, but it is more difficult to get a thermo-baric warhead. While being plausible, some participants considered the description of this scenario as too detailed for presenting it to a wider public.
- Terror attack using a helicopter: The group raised the question concerning the time needed to intercept a helicopter, once radar has detected it. However, the high speed of the helicopter (200 km/h) made it seem rather impossible. In Germany, about 15 minutes are needed for take-off and some more minutes to reach the NPP, in Czech Republic perhaps longer – relevant to find out the distance of the next military airbase. All in all, this terror scenario was considered plausible.

The **discussion** circled around the question what should be published – only the information that terror attacks are possible, or should more details be made available to the public?

It should be kept in mind that new scenarios will keep coming up, also for the reasons that new weapons are constantly being developed.

It went undisputed that authorities need to be pressured to make amendments to increase security.

It is important to understand that higher security requirements lead to additional costs – and the nuclear industry is already under severe financial strain – therefore higher security could result in less new-built NPPs.

In upcoming PLEX procedures the information is valuable for confronting operators and authorities with those scenarios and thus in the additional risk of the prolonged operation time.

In the Joint Project, European NGOs and research institutions cooperate since 2003 on safe and sustainable energy issues with a focus on anti-nuclear activities in Central and Eastern Europe. For more information see www.joint-project.org/.

The Joint Project is supported by the Austrian Federal Ministry of Agriculture, Forestry, Environment and Water Management.