

Nuclear Power Plants and Terrorism

Some remarks on a sensitive topic

Dr. Christoph Pistner

Tokyo, 14.06.2016

Nuclear Power Plants and Risks

- Nuclear Power Plants have a huge radioactive inventory
- Confinement of radioactive inventory is fundamental safety function
- Risk is a function of the hazard potential (radioactive inventory) and the possible causes for releases
- Causes for releases may stem from
 - Accidents but also
 - Incidental Attacks

Nuclear Power Plants and Terrorism – Is there a Threat?

- Sweden 2012: civil protesters enter nuclear power plant – remain undetected for several hours
- France: over months, drones fly over nuclear power plants – counter measures do not help, no responsible person identified yet
- Belgium:
 - August 2014: possible sabotage of steam turbine in nuclear power plant
 - 2014: known islamic fundamentalist identified working in high security area in nuclear power plant since 2012
 - After Paris attacks: nuclear power plants being evacuated, videos of director of nuclear research facility found in terrorists houses

Nuclear Power Plants and Terrorism – Is there a Threat?

- Ukraine:
 - May 2014: approx. 20 armed activists enter nuclear facility – to protect it against hostile forces
 - November 2015: transmission towers of national grid attacked – loss of external grid at nuclear power plant
- Germany April 2016: computer virus „Conficker“ and comparable viruses located in safety relevant computer systems in operating BWR plant

Nuclear Power Plants and Terrorism – Kinds of Threats

Different kinds of threat to be taken into account

- War-like situations with direct or indirect consequences for nuclear power plants
- Terror attacks from the outside (who, how many, what capabilities?)
- Terror attacks from insiders (permanent staff, temporary workers?)
- Cyber attacks

- Different threats require different approaches
- Threats might change over (relatively short) timeframes

Regulatory Requirements

- IAEA:
 - “Nuclear Security: The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.”
- Western European Nuclear Regulators Association:
 - “O5. Safety and security interfaces ensuring that safety measures and security measures are designed and implemented in an integrated manner. Synergies between safety and security enhancements should be sought”
- German Atomic Energy Act:
 - Ensure that “the necessary protection has been provided against disruptive action or other interference by third parties”

„Design Basis Threat“ – How to define?

- Ministry of the Interior and Ministries responsible for nuclear safety are in charge to define DBTs and corresponding responsibilities of the operator
- Protection has to be provided
 - By the operator: ensure protection of facilities for a certain time
 - By the state: ensure police forces engage after a certain time
- In Germany, DBTs and corresponding responsibilities are defined with respect to disruptive action or other interference by third parties (SEWD)
- Details about DBTs and corresponding responsibilities are not public

SEWD – Nuclear Facilities, IT-Safety, Interim Storages

3-99
Stand 05/13

RS-Handbuch

Bekanntmachung zu der „Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherheitskategorie I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT)“, zu den „Lastnahmen zur Ausbesserung kerntechnischer Anlagen und Einrichtungen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter mittels IT-Angriffen (IT-Lastnahmen)“ und zu den „Erläuterungen für die Zuordnung der IT-Systeme von Kernkraftwerken zu IT-Schutzbedarfsklassen (Erläuterungen)“

vom 8. Juli 2013 (BMBF, 2013, Nr. 36, S. 711)

– Bek. d. BMBF v. 8.7.2013 – RS 14 – 13151 – 813 –

Genehmigungen nach §§ 8, 7 und 9 des Atomgesetzes (AGG) in der Fassung der Bekanntmachung vom 10. Juli 1990 (BGBl. I S. 1595), zuletzt geändert durch Artikel 1 des Gesetzes vom 20. April 2013 (BGBl. I S. 621) genehmigt worden ist, dürfen unter anderem nur erstellt werden, wenn der erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter gewährleistet ist. Dieser Schutz umfasst auch den erforderlichen Schutz gegen IT-Angriffe.

Zur Gewährleistung eines einheitlichen Sicherungsstandards der kerntechnischen Anlagen und Einrichtungen der Sicherheitskategorie I und II gegen IT-Angriffe wurden einheitliche Vorgaben hinsichtlich der zu umzusetzenden Angriffsszenarien sowie hinsichtlich der zu ergreifenden Schutzmaßnahmen aufgestellt und in den IT-Lastnahmen bzw. der SEWD-Richtlinie IT niedergelegt. Die für den Vollzug des Atomgesetzes zuständigen Genehmigungs- und Aufsichtsbehörden der Länder und das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit sind am 12. Juni 2013 im Länderausschuss für Atomenergie – Hauptausschuss – übergeben worden, die IT-Lastnahmen, die SEWD-Richtlinie IT sowie die Erläuterungen für alle kerntechnischen Anlagen und Einrichtungen der Sicherheitskategorie I und II einheitlich anzuwenden.

Die Genehmigungsinhaber sind zu den Entwürfen dieser Dokumente gehört worden; die Entfassungen (Stand 12. Juni 2013) sind ihnen über die atomrechtlichen Genehmigungs- und Aufsichtsbehörden der Länder zugänglich gemacht worden.

Die IT-Lastnahmen, die SEWD-Richtlinie IT sowie die Erläuterungen, die ab dem Tage ihrer Bekanntmachung gültig sind, geben sich hiermit bekannt. Auf die Übergangsbestimmungen in Kapitel 8 der SEWD-Richtlinie IT wird hingewiesen. Der Wortlaut der Dokumente wird aufgrund ihrer Einlassung als Verschlusssache nicht veröffentlicht.

Redaktioneller Hinweis:
BfS bemüht sich, fehlerfreie Texte zur Verfügung zu stellen, übernimmt jedoch keine Haftung. Bei Rechtsfragen sind die in den amtlichen Publikationsorganen des Bundes auf Papier veröffentlichten Fassungen verbindlich.

Seite 1 von 1

SI

Der Text der Richtlinie wird aufgrund der Einschlussfrage nicht veröffentlicht.

Die Antragsteller/Genehmigungsinhaber sind dieser Richtlinie bekannt worden; die Entfassungen (Stand 5. Dezember 2012) sind ihnen über die sie vertretenden Verbände (VÖB/BVE) zugänglich gemacht worden.

Der Text der Richtlinie wird aufgrund der Einschlussfrage nicht veröffentlicht.

Die Antragsteller/Genehmigungsinhaber sind dieser Richtlinie bekannt worden; die Entfassungen (Stand 5. Dezember 2012) sind ihnen über die sie vertretenden Verbände (VÖB/BVE) zugänglich gemacht worden.

Redaktioneller Hinweis:
BfS bemüht sich, fehlerfreie Texte zur Verfügung zu stellen, übernimmt jedoch keine Haftung. Bei Rechtsfragen sind die in den amtlichen Publikationsorganen auf Papier veröffentlichten Fassungen verbindlich.

Seite

Actual Text is classified

3-76
Stand 04/13

RS-Handbuch

Bekanntmachung zu der Richtlinie zur Sicherung von Zwischenlagern gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD) (SEWD-Richtlinie Zwischenlager)

vom 4. Februar 2013 (BMBF, 2013, Nr. 17, S. 375)

– Bek. d. BMBF vom 4.2.2013 – RS 14 – 13151-622 –

Eine Genehmigung nach § 8 des Atomgesetzes (AGG) in der Fassung der Bekanntmachung vom 10. Juli 1990 (BGBl. I S. 1595), zuletzt geändert durch das Gesetz vom 31. Juli 2012 (BGBl. I S. 1704) darf unter anderem nur erteilt werden, wenn der nach § 6 Abs. 2 Nr. 4 AGG erforderliche Schutz gegen Störmaßnahmen oder sonstige Einwirkungen Dritter gewährleistet ist. Zur Gewährleistung dieses erforderlichen Schutzes hat der Antragsteller/Genehmigungsinhaber der jeweiligen kerntechnischen Anlage Schutzmaßnahmen zu treffen, die mit den Schutzmaßnahmen der Polizei abzustimmen und zu verzahnen sind.

Als Grundlage für die Beurteilung der vom Antragsteller nachzuweisenden baulichen und sonstigen technischen, personellen und organisatorischen Schutzmaßnahmen bei Zwischenlagern hatten die zuständigen Behörden des Bundes und der Länder am 24. Oktober 2001 die Richtlinie „Sicherung von Zwischenlagern für bestrahlte Brennelemente aus Leichtwasserreaktoren an Kernkraftwerksstandorten in Transport- und Lagerbehältern gegen Störmaßnahmen oder sonstige Einwirkungen Dritter“ verabschiedet. Dann wurden die Schutzzeile, die zu sichernden Gebäude und sonstigen Anlagen sowie die Sicherungsanforderungen und die erforderlichen Schutzmaßnahmen festgelegt.

Eine Neufassung dieser Richtlinie wurde nach den Beschlüssen zur Nachrüstung der Zwischenlager, die aufgrund einer veränderten Effizienztabelle im Jahr 2011 getroffen wurden, notwendig.

Die für den Vollzug des Atomgesetzes zuständigen Genehmigungs- und Aufsichtsbehörden der Länder und das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit sind am 14./15. Juni 2012 im Länderausschuss für Atomenergie – Hauptausschuss – übergeben worden, die überarbeitete Richtlinie für alle deutschen Zwischenlager einheitlich anzuwenden.

Die zuständigen Gremien der Ständigen Konferenz der Innenminister und -senatoren der Länder wurden beteiligt.

Die Antragsteller/Genehmigungsinhaber sind zum Entwurf dieser Richtlinie gehört worden; die Entfassungen (Stand 10. Mai 2012) sind ihnen über die sie vertretenden Verbände (VÖB/BVE) zugänglich gemacht worden.

Die Neufassung der Richtlinie, die ab 1. Februar 2013 gültig ist, geben sich hiermit bekannt. Sie ersetzt die Richtlinie „Sicherung von Zwischenlagern für bestrahlte Brennelemente aus Leichtwasserreaktoren an Kernkraftwerksstandorten in Transport- und Lagerbehältern gegen Störmaßnahmen oder sonstige Einwirkungen Dritter“ vom 24. Oktober 2001 sowie die Uranlage „Sicherung von Zwischenlagern – relevante Einwirkungsmöglichkeiten unter Berücksichtigung neuer Erkenntnisse und resultierende Schutzmaßnahmen“ vom 15. April 2011.

Der Text der Richtlinie wird aufgrund der Einschlussfrage als Verschlusssache nicht veröffentlicht.

Redaktioneller Hinweis:
BfS bemüht sich, fehlerfreie Texte zur Verfügung zu stellen, übernimmt jedoch keine Haftung. Bei Rechtsfragen sind die in den amtlichen Publikationsorganen des Bundes auf Papier veröffentlichten Fassungen verbindlich.

Seite 1 von 1

General Protective Measures

Two Pillars

- Robust systems, structures and components
 - See example of airplane crash in the following
 - Threat is evolving (external attack with modern weapons: need for reinforcements in German Interim Storage Facilities and Power Plants)!
- Administrative measures
 - Access restrictions to facilities (inner and outer perimeter)
 - Physical protection services (guards)
 - Background checks for workers in nuclear facilities (three different levels of checks)
 - ...

Robustness: The Example of Aircraft Crash Impacts

- In German nuclear power plants, accidental aircraft crashes were initially not taken into account
- Starting in 1974, accidental aircraft crash of military aircrafts had to be taken into account, detailed requirements (mass, size and speed of airplane, amount of fuel ...) in regulation
 - Protection by robustness of buildings OR spatial separation
- After 09.11.2001: Public discussions of consequences of intentional aircraft attack on nuclear facilities
 - Evaluations of resistance of buildings against consequences of aircraft attacks are performed but detailed assumptions and results are not publicly available

Robustness: The example of Aircraft Crash Impacts

- In 2011: Plant-specific safety review (RSK-SÜ) of German nuclear power plants in the light of the events in Fukushima-1 (Japan)
 - Mechanical impact (impact of the aircraft) and thermal impact (kerosene fire) considered
 - Three degrees of protection defined for each impact categories
 - Degree 1: Military aircraft (Starfighter)
 - Degree 2: Military aircraft (Phantom) or medium sized commercial aircraft
 - Degree 3: Large commercial aircraft
 - Plants not fulfilling Degree 1 have been shut down 2011
 - All plants still in operation in Germany today fulfill degree 2 with respect to Phantom, but questions remain with respect to commercial aircraft
 - Investigations with respect to degree 2/3 still ongoing but not public

Robustness: The example of Aircraft Crash Impacts

- Robustness of safety related buildings (concrete thickness)
- Robustness of cooling water supply
 - Spatially separated buildings, protected pipings
 - More recently also mobile equipment as backup
- Robustness of electricity supply
 - Two independant and divers emergency power supply systems (two diesel generator groups)
 - Three independant connections of the plant to the external grid, one of those specifically protected (underground)
 - More recently also mobile electricity supply, accesspoints

Cyber Security

- Remember: Stuxnet 2010 (continuous development of the capabilities to attack since then)
- Relatively new threat:
 - Protection not as well developed as physical protection?
 - Awareness not as high as with other threats?
 - Details of threats still evolving!
- Strongly increasing rate of cyber attacks against industry in general
- Small risk for attacker
- Infection pathways via: Internet, USB, mobile Disks ...

Cyber Security

- Important parts of the response (in Germany):
 - no software-based systems are in use in the reactor protection systems of German nuclear power plants
 - separation of safety and security related computer systems from external net, access controls to computer systems
 - (Law on IT-Safety of 25. Juli 2015)
- Dilemma:
 - Air gap can (easily) be overcome (see Stuxnet)
 - Separation of computer systems from external net hinders continuous updates: Virus found in Germany in 2016 dated back several years and would have easily been identified, but no up to date virus protection was installed

Openness vs. Classification

- Some information must be protected, because of security concerns
- But:
 - Interface between safety and security is difficult:
 - By learning from operational experience in nuclear power plants (analysing and discussing safety incident), insiders might learn how to sabotage the plant
 - By discussing incidents with the public, security aspects might become public
 - Engagement of public is difficult
 - How to check adequateness of Design Basis Threats?
 - How to check whether protection against DBTs is adequate?
- Example of Interim Storage Facilities in Germany:
 - Lawsuits against licences for interim storage facilities due to deficiencies in security → Loss of licence of operating interim storage facilities!

Vielen Dank für Ihre Aufmerksamkeit!
Thank you for your attention!

Haben Sie noch Fragen?
Do you have any questions?

