Countering Security Risks to Nuclear Power Plants

F Steinhäusler
Division of Physics and Biophysics,
University of Salzburg, Salzburg, Austria
friedrich.steinhaeusler@sbg.ac.at

ABSTRACT

Between 1972 and 2007 altogether 17 major terror attacks or acts of sabotage have been carried against nuclear power plants (NPP). None of them resulted in an uncontrolled radioactive release. In order to reduce the security risk to NPP due to terrorists in the future, pre-emptive measures are necessary to identify their motivation, incentives, operational and logistical capabilities to implement a successful attack. Physical security has always been a priority for NPP operators, but since 9/11 the global nuclear community has made additional major cooperative efforts to develop a spectrum of measures aimed at countering future security threats to NPP. An Integrated Modular Security System (IMSS) with modular security layers is proposed for new NPP.

1. INTRODUCTION

Long before the terror attacks of 9/11 in the US, nuclear power plants (NPPs) had the most comprehensive security of any industrial facility. Since 9/11, security measures have been increased even further to accommodate for the new threat situation. This paper reviews the new security challenges for nuclear power plant operators and the international achievements in meeting these challenges.

Operators of the 445 NPPs worldwide had the opportunity to gain extensive experience with countering security threats over the past several decades. For example, between 1989 and 1999 there were 235 threats, hoaxes or minor sabotage acts against US nuclear facilities (Nilsson, 2001). Table 1 contains a summary of major security-related events for the period 1972 to 2007 worldwide (NATO, 2004). However, *none* of the past 17 attacks have resulted in radioactive releases to the surroundings.

2. CURRENT SECURITY THREATS TO NUCLEAR INSTALLATIONS

In order to reduce the security risk to NPP due to terrorists it is necessary to identify their motivation, incentives, operational and logistical capabilities to implement a successful attack.

2.1 Terrorist motivation and incentives

Terrorists have two motives for an attack: (1) Diversion of nuclear material in order to misuse the material for criminal purposes; (2) Physical attack or sabotage intended to cause an uncontrolled release of radioactivity. The incentives for terrorists are fourfold: (1) NPPs are associated by the public with high risks. If terrorists should manage to damage an NPP, this will further increase the fear of the public; (2) Any environmental contamination will be symbolic for the capability of terrorists to inflict harm to society; (3) In some countries a relatively small number of NPPs provide a significant contribution to the national energy production (number of NPPs/% of national electricity supply); e.g., Bulgaria (1/ 40%), Lithuania (1/ 78%), Slovenia (1/40%) (European Commission, 2007). Therefore even the temporary loss of such a vital facility could induce a national energy crisis situation; (4) A terror attack on an NPP in *one* country is likely to raise major security concerns in other countries, potentially leading to a temporary shut-down of several such facilities as a precautionary action.

2.2 Operational and logistical capabilities of terrorists

A major terror attack on an industrial installation, such as an NPP, is typically implemented in three *operational phases*:

(1) Conceptual phase: The core terrorist group initiates a terror act or receives a proposal for such an operation from one of its members. Upon positive internal review the action is approved.

(2) Scouting phase: Members of the terror network collect information potentially useful for the implementation of the planned terror act (e.g. construction plans of nuclear facilities, work routines of employees at the plant, schedules of security guards patrolling the site). The actual attack scenario and its options are defined at the end of this scouting phase.

(3) Implementation phase: A group of terrorists prepares the terror attack against an NPP. Shortly before the attack, a top representative of the terror organization will arrive to coordinate the final stages of the attack and will depart prior to the attack.

The *logistical requirements* concerning the acquisition and deployment of conventional weapons can be considered as common knowledge among all those terrorist groups capable of staging an attack on an NPP (Steinhäusler, 2003). Terrorist camps dedicated to training individuals in the manufacture and use of these weapons have been established in several countries. Any military combat training further improves terrorists' attack capabilities, i.e. many "veterans" from previous or current "Jihad" war zones (Afghanistan, Bosnia, Chechnya, Iraq) live in Western countries today.

Table 1: Major security threats due to acts of physical violence to nuclear research- and power reactors for the period 1972 to 2007

Date	Country	Type of facility	Comments
November 1972	USA	Research reactor at Oak Ridge National Laboratory (ORNL)	Hijacking of a DC9 and demand of ransom; ordering the pilot to crash the plane into ORNL; not carried through
March 1973	Argentina	Power reactor at Atucha, 100 km north of Buenos Aires	People's Revolutionary Army (ERP) terrorists raided the construction site
August 1975	France	Power reactor at Brennilis (Brittany)	Two explosions
June 1977	Spain	Power reactor at Lemoniz	ETA terrorists bombed the construction site
October 1977	Spain	Power reactor at Lemoniz	ETA terrorists bombed the construction site
October 1977	USA	Power reactor at Columbia (Oregon)	Bomb was detonated n visitors' centre
December 1977	Spain	Power reactor at Lemoniz	Machine gun- and grenade attack on the guard post by ETA terrorists
March 1978	Spain	Power reactor at Lemoniz	Bomb planted in steam generator by ETA terrorists
June 1979	Spain	Power reactor near Bilbao	Bomb planted in turbine room
December 1982	South Africa	Power reactor	Mercenaries deposit four bombs
July 1982	France	Malville Superphoenix breeder reactor near Lyon	Anti tank rocket fired at construction site
May 1983	Spain	Power reactor in Tafalla near Pamplona	Two people were killed by explosives detonating in their car 1000 meters from facility
June 1985	Philippines	Power reactor	Sabotage campaign by blowing up twenty-six transmission towers within two weeks
August 2000	Australia	Research reactor Lukas Heights near Sydney	Terrorist plot revealed
March 2003	USA	Power reactor	Iraqi terrorists plot revealed
September 2007	Syria	Unspecified reactor	Attack by Israeli Defence Force
November 2007	USA	Power reactor	Pipe bomb discovered on truck of contractor

3. COUNTERMEASURES

Over the past few years the global nuclear community has made major cooperative efforts to develop jointly a spectrum of measures aimed at countering the new security threats to NPPs.

3.1 Vital area concept

To manage security risks to NPPs, major efforts have been undertaken to provide adequate physical protection, in particular to protect *vital areas*. A vital area is defined as any area that contains vital equipment; vital equipment is in turn defined as any equipment system, device, or material the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation (US Code of Federal Regulations, 1993). The US NRC defines Type 1 vital areas as those wherein successful sabotage can be accomplished by compromising or destroying the vital systems or components located within this area. All other vital areas are designated as Type 2 vital areas. Equipment or systems that would be required to function to protect public health and safety following such a failure, destruction, or release are also considered vital.

3.2 Design Basis Threat

The *Design Basis Threat* (DBT) assumes that terrorist acts showed a considerable degree of predictability with regard to their method of attack as well as the scope of their criminal action (Blankenship, 2003). The DBT has been found to be useful in three ways: (1) Providing a basis against which the adequacy of proposed safeguards systems may be measured; (2) Representing an adversary characteristics baseline for use in measuring subsequent changes in those characteristics; (3) Assuring an adequate standardized level of protection at selected nuclear facilities. Some financially disadvantaged countries (e.g., Former Soviet Union, developing countries in Africa and South-east Asia) experienced certain difficulties in applying this concept, unable to allocate adequate financial resources for physical protection of NPPs, based on current DBTs (Kondratov, 2006). Details of a site-specific DBT are classified for security reasons. Therefore only the typical components of a DBT are presented here: (a) Identification of major security threats; (b) Defending against potential attackers; (c) Delaying the attackers until security reinforcements have arrived. Protection against intruders consists of: a series of fences with various sensors; multiple CCTV cameras installed on-site and at the site perimeter; inspection of all persons and vehicles entering the site. In many countries, the basis for the DBT specifies the number of attackers to be assumed, together with the type of vehicle and weapons used in the attack, as well as the kind of assistance provided by a hypothetical collaborating insider. Protection against insiders is based on criminal background checks and psychological tests of employees. Increasingly realistic mock attacks on NPPs are carried out to test the state of readiness of the on-site security forces. With the exception of the aerial terror attacks in the US on 11 September 2001, international terrorism has continued to use *conventional* terror attacks (improvised explosive devices, car- and truck bombs, boats loaded with explosives), increasingly deployed by suicide terrorists. None of these operational and logistical capabilities of terrorists would require a major revision of the current DBT approach.

3.3 Proliferation resistance

The assessment of the proliferation resistance (PR) of NPPs requires the analysis of the motivation and capabilities of the proliferators and the capabilities of the safeguarding system, i.e. the human element is essential in determining the resistance of an NPP to malevolent acts. Over the past five years two systematic approaches have been developed for evaluating the PR. In 2000, the IAEA initiated the *International Project on Innovative Nuclear Reactors and Fuel Cycles* (INPRO) and released the INPRO methodology for evaluating proliferation resistance as the IAEA-TEC-DOC-1362 in 2003. The INPRO approach evaluates a nuclear system with a set of three *Indicators*: Basic principle, User requirements, and Criteria. A further refined concept was published as IAEA-TEC-DOC-1434 (2004); the corresponding *User Manual* was released in 2007. As an alternative approach the *Generation-IV International Proliferation Resistance/Physical Protection Working Group* (GEN-IV PR/PP WG) has been set up by a group established in 2002 with experts from Canada, the European Union, France, IAEA, Japan, South Korea and USA. They jointly developed a proliferation resistance/physical protection evaluation methodology and the corresponding *Implementation Guide*. This methodology evaluates the characteristics of a given nuclear system in terms of several PR variables, accounting for each step of a diversion pathway.

3.4 Operational and technical countermeasures

The following operational and technical countermeasures are currently discussed to provide an advanced degree of protection for an NPP: (1) Preventive shut down of the facility to extend the period available for countermeasures after an attack. Due to the relatively slow cooling of the nuclear fuel, ideally the system should be shut down already at the onset of a significant deterioration of the security situation; (2) Structural strengthening of the facility against a large, fully fuelled aircraft or attacks with explosives by using towers, respectively, protective walls made of steel-reinforced concrete (German Federal Ministry for Environment, 2002); (3) Obstacles preventing the on-site use of vehicles by terrorists, thereby limiting the radius of action of terrorists on the territory of an NPP; (4) Creation of mist to hide the facility from aerial attacks, combined with interference with the GPS-signal in the vicinity of the facility (Baake, 2005); (5) Increase of security staff and improvement of their equipment to provide extended armed resistance until the arrival of additional security forces, combined with highly realistic exercises, state-of-the art access control, stringent evaluation of the security staff, and enforced security procedures for weapon handling and storage (Nucleonics Week, 2006); (6) Protection of the facility by military forces; (7) Physical separation of vital facility components (emergency power supply, emergency control units); (8) Spent fuel storage in a pool preferably located inside the containment building (protected by layers of up to 2 m of heavy concrete and steel).

3.5 Internationally coordinated countermeasures

International organisations developed both voluntary guidance and legally binding documents to protect nuclear facilities and material in peaceful domestic use, storage and transport.

Examples of major international and national achievements over the past few years are listed below.

International Atomic Energy Agency (IAEA):

(1) Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage (IAEA, 2007); safety and security aspects are closely interlinked, when it comes to protecting NPPs against sabotage and standoff attacks. Sabotage protection can work synergistically with the protection against extreme external occurrences of accidental origin and also human-induced events.

(2) Amendment to the Convention on the Physical Protection of Nuclear Material (IAEA, 2006a); this international, legally binding consensus constitutes an important milestone in combating nuclear terrorism.

(3) Assessment of Defence in Depth for Nuclear Power Plants (IAEA, 2005); this tool enables the operator to verify capabilities for implementation of defence in-depth at an existing NPP and to identify its strengths and weaknesses for a given set of predefined objectives.

(4) Advanced Nuclear Power Plant Design Options to Cope with External Events (IAEA, 2006b); state-of-the art design approaches can assist significantly in the protection from extreme external events, including already the phase of siting evaluation.

(5) Effective Nuclear Regulatory Systems: Facing Safety and Security Challenges (IAEA, 2006c); increased threats to the security of nuclear installations require new strategies and approaches to both safety and security.

(6) Nuclear Security Plan 2006-2009; it addresses priorities in nuclear security (needs assessment, analysis and coordination; prevention; detection and response).

(7) International Physical Protection Advisory Service (IPPAS) assists Member States to strengthen and enhance the effectiveness of the physical protection of their nuclear materials and facilities.

(8) International Nuclear Security Advisory Service (INSServ) provides specialized services promoting enhanced nuclear security in order to strengthen the capacity to prevent, detect and respond to nuclear terrorism.

(9) EPREV (Emergency Preparedness REView); EPREV experts review preparedness for nuclear or radiological emergencies in Member States.

(10) Nuclear Security Equipment Laboratory provides support for equipment monitoring, maintenance, procurement and emergency response.

North Atlantic Treaty Organization (NATO):

In June of 2002 at a G-8 summit meeting Britain, Canada, France, Germany, the UK, and the USA, plus Japan and Russia, reached agreement on common goals for efforts to improve security of nuclear materials against terrorists. The declaration establishes broad non-proliferation principles, including the maintenance of "effective physical protection measures" for facilities that house nuclear materials.

European Union (EU):

Pursuant to an agreement with the IAEA, EURATOM has some responsibility to the IAEA for Non Proliferation Treaty-required safeguards inspections and standards for control and accounting for nuclear material at nuclear reactors to prevent diversion of nuclear material to weapons by licensees or other insiders. Each EURATOM member has responsibility to its own citizens for protecting its reactors from sabotage, but, except for the April 2004 UN Security Council resolution (United Nations, 2004), no international measure gives EURATOM members responsibility to the international community to do so. Since the resolution does not provide standards for physical protection, national laws and regulations are the sources for domestic protection standards, provided laws and regulations containing standards have been adopted.

Global Nuclear Energy Partnership (GNEP):

GNEP encompasses nuclear supplier countries who inter alia want to help shape the secure and safe development of nuclear energy worldwide by providing standardized reactors to client states. In addition, they will ensure supplies of nuclear fuel, and that subsequently the used fuel would be returned to a supplier state for reprocessing, recycling of recovered materials, the destruction of some wastes in advanced power reactors, and final disposal. Current members are Australia, Bulgaria, Canada, China, France, Ghana, Hungary, Italy, Japan, Jordan, Kazakhstan, Lithuania, Poland, Romania, Russia, Slovenia, Ukraine and the USA. Canada can join their ranks once it signs the GNEP Statement of Principles, which is likely happen in the USA within weeks (status: 30 Nov. 2007).

3.6 National countermeasures

3.6.1 US approach

After the attack of 11 September 2001, the US Nuclear Regulatory Commission (NRC) reviewed its security program, including an engineering analysis of the consequences of an attack on a nuclear power reactor by a large airliner (US NRC). For protection against aircraft attacks, the NRC relied on the US Federal Aviation Administration (FAA), on airport authorities and on the airlines to provide temporary no-fly zones around some reactors and to keep terrorists off airliners. It relied on the US National Guard and US Air Force to patrol areas near power reactors with military aircraft (Meserve, 2002). Later, the FAA issued a notice to airmen to avoid airspace "above or in proximity to" nuclear power plants (Meserve, 2003). The NRC issued various confidential "Safeguards and Threat Advisories" to strengthen "capabilities and readiness to respond to a potential attack on a nuclear facility", calling for an increase in the stand-off distances from the reactors at which ground vehicles approaching them would be stopped and searched. NRC kept the provisions of these added physical protection requirements secret (NRC, 2002). In April 2003, it issued new DBT requirements for power reactors (NRC News, 2003). NPP sites are divided into three zones: (1) A large "owner-controlled" open buffer region around the plant to provide a viewing distance from the plant of potential attackers; (2) Inside this buffer region is a "protected area" behind fences or other barriers; (3) Inside this protected area is a "vital area" with stronger barriers. By December 2007 NRC

had consolidated its efforts to strengthen physical protection of its 104 nuclear power plants.

3.6.2 British approach

Most of the official UK security requirements for NPP are stated in *Private Security* documents approved by the British Secretary of State for Trade and Development. Plant operators were required to assure that the security of NPPs from sabotage met the standards of an approved security plan for that location (Nuclear Energy Agency, 1999). After 11 September 2001, measures were taken to enable, if possible, intervention by Royal Air Force interceptor aircraft in the event an aircraft attempted to attack a civil nuclear facility (Parliamentary Office of Science and Technology, 2002). In addition, no-fly zones were established around some of the most security-sensitive nuclear facilities (Global Security Newswire, 2001). Later new security regulations for the security of the civilian nuclear industry were issued. The specific requirements that these plans had to satisfy and the provisions of the plans themselves were kept secret. No DBT was made public. It is stated that security plans prepared by operators for approval by the regulatory authority should cover "fencing, closed circuit television and turnstile access; roles of security guards or UK Atomic Energy Authority Constabulary at more sensitive sites, protection of technology (technical secrets) … trustworthiness of individuals…" .

3.6.3 French approach

France has 59 operating nuclear reactors and two spent fuel-reprocessing plants. Specific physical protection requirements were kept largely secret, as were the government's plans for enforcement of them. After 11 September 2001, experts at the French Nuclear Safety Institute agreed that the containment buildings around many of the reactors could give way if a large fuel-laden civilian aircraft crashed into them. But the danger of massive dispersion of radioactive material from aircraft attack on them was not perceived to be as great as that from such an attack on the two reprocessing plants and their large reservoirs for radioactive processing wastes and spent fuel. What specific new French requirements exist to protect NPPs from large aircraft or from the ground-based threats described above are not known.

3.6.4 German approach

Before September 11, 2001, German authorities had not required that its 19 NPPs be protected from a large, crashing, fuel-laden, civilian jet airliner. The oldest plants were strong enough to withstand the crash of a small fighter aircraft. Their walls consisted of reinforced concrete (width: approximately one meter). The ten newest German plants were designed to withstand the crash of a military fighter jet flying at around 770 km/h (German Reactor Safety Commission, 1996). NPP operators took the view that they could not prevent terrorists from hijacking a large airliner and crashing it on an NPP. That, they said, was the responsibility of the government (Riebsamen, 2001). Protection beyond this scenario, i.e. against military-style terrorist attacks with weapons such as bombs, rockets, grenade launchers, etc. is also assumed to be the responsibility of the German government. Investigations carried out by German authorities since 11 September suggest that there would probably be no uncontrolled release of radioactivity resulting from the mechanical impact and subsequent fire at the interim storage facility caused by the crash of a large aircraft.

4. NUCLEAR POWER PLANTS – A LOW PRIORITY TARGET FOR TERRORISTS?

Despite of the large number of terror attacks worldwide, no major terror attacks against NPPs have been implemented since 9/11. One or more of the following main factors may be the reason why: (1) NPP may not be on the target-list of terrorist groups. Conventional modes of attack, -tactics, and -targets are likely to remain the first priority of many terrorist groups in the near-term; (2) Large-scale attacks on hardened components of the national critical infrastructure may not meet the goals of a terrorist group. Low-intensity, conventional terrorism, preferably against "soft targets", may still suffice; (3) Engaging in sophisticated attacks against NPPs will undoubtedly call for a new level of expertise beyond traditional weapon competence. This would not only require additional logistics, training, and possibly new levels of weaponry, it would also increase the risk of failure; (4) There is still a range of other targets that allows terrorists to maintain well-proven tactics, such as telecommunications, electric power- and drinking water supply, and public transport infrastructure; (5) The political "fall-out" from acts of terror against NPPs is hard to predict. Terrorists may prefer less uncertain outcomes of their long-term planning and "investments" in capabilities and manpower.

5. INTEGRATED MODULAR SECURITY SYSTEM (IMSS)

If a security system has a modular structure with appropriate operational and logistical interfaces established between the different modules, future security upgrades will be more cost-effective than current retrofitting practices. It is proposed to implement an Integrated Modular Security System (IMSS) in new NPP, which should address at a minimum the topic areas listed for each module below:

- **Module Threat**

Operational capabilities and tactical approaches of external adversaries, specifying weapons, vehicles, training and skills of attackers; insider sabotage; insider collusion; protection against forced entry into protected areas using divers, 4WD vehicles and truck convoys; protection against aerial attack (deploying alternatively plane, helicopter, parachute, ultra-light plane, remote-controlled parachute and plane, sling shot); protection against sneak-, suicide- and simultaneous cyber attack; protection against attack on first responders rushing to scene.

- **Module Personnel**

Bio-feed back stress management test; reliability- and psychological behavioral test; susceptibility test to corruption and blackmail; 3D-simulated and field exercises; tactical and physical fitness training of security staff; unannounced assessment of access authorization procedures; continuous real-time position control of staff members.

- **Module Access Control**

Integration of different access control technologies (biometrics; electronic locks; card readers; mechanical and opto-electronic locks; portals equipped with metal detectors, vapour detectors, nitrogen quadrupole detectors; instruments based on nuclear

magnetic resonance); security seal technology; advanced control of high-velocity/high impact vehicle access; vehicle search techniques; mobile and stationary barrier technologies; physical protection of security-related equipment and weapons; graded access control to owner-controlled open buffer region, protected areas; and vital areas; enhanced access control during scheduled maintenance and safety-related emergencies; integration of K 9-units.

- **Module Alarm- and Communication Systems**

Electronic perimeter intrusion alarm systems; visual perimeter surveillance; automated mechanical barriers; interior intrusion alarm systems; emergency power supply for security systems; tamper-proof housing of sensors; redundant security lighting; remote supervision of security system signals; physical protection of Central Alarm Station; portal monitors (metal, explosives, nuclear material); protection of on-site computer- and communication systems; redundant duress alarm and emergency communication system; 3D-situation awareness.

- **Module Field-Tests**

High kinetic energy vehicle barrier penetration; vehicle convoy bomb attack; scuba-diver attack; night-time aerial attack; simultaneous computer hacker attack; contingency response in high external radiation field and radioactive smoke plume.

6. CONCLUSIONS

If past events can be indicators of future events, serious violations of physical security of nuclear reactors have a low probability of event with relatively minor consequences so far. However, in view of international terrorism and its capability "to learn", NPP operators must prepare for forever changing terrorist threat scenarios. Such criminal actions have a new dimension in view of the increasing trend to commit acts of suicide terrorism. In order to achieve optimal cost-efficiency of upgrading physical protection systems, it will be advantageous to bring together safety and security specialists. The current high standard in security can be maintained by continuously updated threat-, vulnerability- and risk assessment. New NPPs should consider implementing an *Integrated Modular Security System.* Together, these layers make a formidable defence against present and future security threats posed by international terrorism.

7. REFERENCES

[1] BAAKE R, (2005), *Pilot project nuclear power plant Grohnde* (Lower Saxony),Letter to W. Hohlefelder, E.ON Energie AG, Federal Ministry for Environment, Nature Protection and Reactor Safety (BMU), Bonn, Germany.

[2] BLANKENSHIP J, (2003), *International standard for Design Basis Threat (DBT*), ÖMZ Austrian Military Periodical, *Nuclear Material Protection*, Special Edition.

[3] EUROPEAN COMMISSION (2007), EU Energy and Transport Figures, Statistical Handbook 2006, Directorate-General for Energy and Transport, ISBN 92-79-03598-3, Luxembourg; IAEA website (http://www.iaea.org/cgi-bin/db.page.pl/pris.oprconst.htm)

[4] GERMAN FEDERAL MINISTRY FOR ENVIRONMENT, (2002), Nature protection and reactor safety (BMU), Protection of the German nuclear power plants against the background of the terror attacks in the USA on September 11, 2001 – Results of the GRS-investigation based on the project "Expert assessment of terrorist-induced plane crashes on German nuclear power plants", BMU, Bonn, 27 November 2002 (in German).

[5] GERMAN REACTOR SAFETY COMMISSION, (1996), RSK, *Guidelines for Pressurized Water Reactors*, (as amended in 1996).

[6] GLOBAL SECURITY NEWSWIRE, (2001), 8 Nov. 2001

[7] IAEA Safety Reports series No. 46, STI/PUB/1218 (2005)

[8] IAEA International Law Series No. 2, STI/PUB/1275 (2006**a**)

[9] IAEA TECDOC Series No. 1487, No. 1487 (2006**b**)

[10] IAEA Proceedings Series, STI/PUB/1272 (2006**c**)

[11] IAEA Nuclear Security Series No. 4, STI/PUB/1271 (2007)

[12] KONDRATOV S. and STEINHÄUSLER F., (2006), *Why there is a need to revise the Design Basis Threat concept*, International Journal of Nuclear Law, 1/2, 182-188.

[13] MESERVE R., (2002), NRC Chairman, *Nuclear Security in the Post-September 11 Environment*, Address to the National Press Club: 17 Jan 2002.

[14] MESERVE R., (2003), NRC Statement Submitted to Subcommittee on Oversight and Investigations, House of Representatives Committee, on Energy and Commerce, http://www.nrc.gov/reading-rm/doc-collections/news/2003/

[15] NATO SST.CLG, *Terrorist Attacks on Nuclear Power Plants and Nuclear Material Transports*, Project No. 978964 (2004), updated December 2007.

[16] NILSSON A., (2001), Symposium on International Safeguards - Special Session on *Combating Nuclear Terrorism*, IAEA Material Security Programme, Vienna, Austria.

[17] NRC (2002), Order Modifying Licenses, dated Feb. 25, 2002; NRC Order Modifying Licenses of October 16, 2002; Richard Meserve, NRC Statement, above.

[18] NRC News (2003), *NRC approves changes to Design Basis Threats and issues orders for nuclear power plants*, No. 03-053, April 29, 2003.

[19] NUCLEAR ENERGY AGENCY, (1999), *Nuclear legislation: Analytical study*, (OECD 1999), p. UK-12.

[20] NUCLEONICS WEEK, (2006), 47 / 36.

[21] PARLIAMENTARY OFFICE OF SCIENCE AND TECHNOLOGY, (2002), *Nuclear Terrorism*, Report No. 179.

[22] RIEBSAMEN H., (2001), *Nuclear plants as terrorist targets*, Frankfurter Allgemeine Zeitung, (Frankfurt, Oct. 15, 2001).

[23] STEINHÄUSLER F., (2003), *What it takes to become a nuclear terrorist*, American Behavioral Scientist, 46/6, 782-795.

[24] UN Security Council Resolution 1540 (2004), UN Press Release SC/8076.