NUCLEAR SECURITY AND EMERGENCIES IN CASE OF MALEVOLENT ACTS AGAINST NUCLEAR POWER PLANTS

Rafael J. CARO[1] and **Friedrich STEINHÄUSLER**[2]
[1] TECNATOM, Emergency Support, S 28703 Madrid, Spain, Tel. 91 659 88 23, Fax 91 659 86 77, rcaro@tecnatom.es
[2] University of Salzburg, Government Radiological Measurements Laboratory Salzburg, A 5020 Salzburg, Austria

1 Introduction and Background

This paper develops several fundamental aspects of terrorist threats to NPPs. After reviewing the justification, vulnerabilities, and methodological tools to face the threat, the last main paragraph focuses on an overview on the last barrier, Emergency Plan, and the associated training, to analyze the differences with an accident, specific training issues and main recommendations, based on best international practices, to face an emergency caused by a Hostile Act.

Long before the catastrophic attacks that have been occurring since the beginning of the century and that have changed the perception of security at international level, Nuclear Power Plants (NPP) have been considered possible targets for hostile acts [1], [2]. The 09/11 attacks by Al Qaeda, that included the use of technology, the intention to cause a great damage and that the terrorist were inclined to die, added to certain evidences related to the possibility that this group could include an NPP, places this threat in the focus of attention.

2 Vulnerabilities, Threats and Risks

The origin of risk is the accumulation of radioactive materials; inside the reactor, while the reaction chain is maintained, radioactive wastes are produced, and after that they are hold in the spent fuel pools. Nuclear safety principles [3], [4], guarantee a series of protection stages against failure and its detection, which have to be surpassed to lead to an accident. Despite the fact that this does not assure the absolute absence of failures the response of the facility will prevent, in a reasonable way, severe damages. Nevertheless, it is important to reflect the main significant differences amongst facilities in the nuclear security frame: (1) Differences in technologies like Containment structures, Emergency Core Coolant Systems (ECCS), intrinsic stability or fire systems, will have different vulnerabilities. (2) Different locations. Seismic, geological, meteorological, demographic and other characteristics have to be considered. (3) Geopolitical aspects. It is also necessary to take into account the different threats attributable to regions, countries or political regimes. (4) Training in case of emergency; the lack of efficiency can lead to a lack of capacity to mitigate undesired effects in case of a radioactive release. Thus, in addition to nuclear safety principles it is necessary to consider specifically and independently the physical protection of the facilities. Though such protection was explicitly stated in the nuclear safety principles, backgrounds exposed have promoted the attention and modernization of the fundamentals of this activity. In this way the OIEA, in INFCIRC 225**,** [5], [6], proposes a series of principles and measures, based upon which the radiological risks are a function of different factors, among them: (a) The threat, (b) Type and inventory of nuclear materials, (c) Design of the facility, and (d) Security characteristics. This means that each installation must be evaluated independently and, to succeed in preventing sabotage, there has to be: (1) A specific assessment of the facility, (2) a determination of the physical protection level based on the Design Basis Threat, and (3) the adoption of basic measures, like taking into account the physical protection since the design of the facility, limiting the access to nuclear facilities; and the determination of the confidence in anyone to enter the facility.

Threats against NPPs can be classified [7], [8] in the following representative types: (A) Terrestrial attack: Including an assault team or a bomb vehicle, (B) Aquatic attack: In case of sea or rivers as final heat sink.(C) Aerial threats, crashing a big civil airplane [9], or the

installation of explosives by air [8]. (D) Threats to transports, (E) Internal Threats, and (F) Cyber-Threats. The main threat depends on the knowledge the attacker has about the facility.

If the objective is the release of radioactivity, the idea is to provoke a sequence of events that leads to a reactor coolant degradation to make impossible the heat removal, causing damages to the integrity of the first barriers while attacking Contention Building simultaneously, causing the emission of radioactive materials to the environment.

However, this simple description can lead to an error; as it will be seen, the most reliable studies demonstrate that the risk of succeeding in an attack like this is quite low.

Risk is defined as proximity to damage and Security as distance to damage. Both proximity and distance can be expressed as the probability of the occurrence of scenarios that lead to damage. These probabilities can also be expressed as Expected Frequencies, the inverse of which is the Recurrence Interval of the scenario. This approximation is only valid for frequent scenarios and known damages, but not for very safe activities that lead to accidents very infrequent. This problem is tackled in two different ways:

(a) The Deterministic point of view, states the group of accidental scenarios {Ei}, supposed with probability 1, to design the plant in such a way that none of them can lead to unacceptable damages.
(b) Probabilistic Methodology, based on: (1) All predictable accidental scenarios are deduced, (2) The expected frequency is analyzed, and (3) Al associated damages are assessed.

Related to Physical Security, several studies were performed internationally after the terror attacks in the US on 11 September 2001. The following illustrates the situation in the US. After the terror attacks on 09/11, two [9] studies ordered by the Nuclear Energy Institute (NEI), and Nuclear Regulatory Commission (NRC) to Electrical Power Research Institute, EPRI, with the following results:

The first one [9] analyzes the risk associated to an attack against a NPP with a large commercial airplane; the study used a deterministic methodology and concluded that:

a. The containment structure will not be seriously affected,
b. The spent fuel pools would not become drilled, spent fuel would remain protected and there would not be release of radioactive materials to the environment, and
c. The dry storage structures had not serious damages, so there would not be any release of radioactive materials.

The second one [10] is focused on the risk of a terrestrial attack to a nuclear facility; the study uses a probabilistic methodology with approximations. The main conclusions of this study are the following:

a. The risk for the public due to a terrestrial terrorist attack to a commercial nuclear plant is low ($1 \cdot 10^{-8}$ immediate casualties/year or $1 \cdot 10^{-9}$ future death/year).
b. In case of attack, the probability of damage is low while severe release probability is lower.
c. In the improbable case of core damage and radioactive release, the consequences are not catastrophic.

The US Energy Policy Act of 2005 [11] imposed specific criteria for the US Nuclear Regulatory Commission (NRC) to take into account for a revision of the Design Basis Threat (DBT; for details, see section below) against terrorism. Subsequently NRC revised the DBT (10 C.F.R. art 73.1) on April 18, 2007. Among other changes, the revisions expanded the assumed a more realistic mode of attack, i.e., capabilities of adversaries to operate as one or more teams and attack from multiple entry points. Altogether 112 force-on-force inspections were conducted between 2007 and 2009, with each inspection typically including three mock attacks by the adversary force. Eight mock attacks resulted in the simulated destruction of complete target sets, indicating inadequate protection against the DBT, necessitating the implementation of additional security measures [12]. Nuclear power plants were designed to withstand hurricanes, earthquakes, and other extreme events. But deliberate attacks by large airliners loaded with fuel, such as those that crashed into the World Trade Center and Pentagon, were not analyzed when design requirements for today's reactors were determined [13]. In particular the impact of a

large, fully fuelled civilian plane crash on spent fuel pool area remains as a controversial issue; analyses differ as to the damage that could result. The US National Academy of Sciences (NAS) found that "successful terrorist attacks on spent fuel pools, though difficult, are possible," and that "if an attack leads to a propagating zirconium cladding fire, it could result in the release of large amounts of radioactive material" [14]. At present NRC has determined that commercial aircraft crashes are beyond the DBT - guidelines on how to meet requirements to properly face those threatening situations were submitted[1] to licensees [15]- and published regulations in June 2009 to require that new reactor designs have to be able to withstand such crashes without releasing radioactivity. The new advanced reactors are now designed to withstand this threat, even though some[2] like Westinghouse AP-1000, had published in 2007, 2 years before the rule, that modifications to successfully withstand aircraft crashes, had already been done [12].

3 Design Basis Threat (DBT)

DBT is a description of attributes and characteristics of internal and external potential adversaries that could try to execute a malicious act, as not authorized movement or sabotage against which it has been designed and assessed [10] a physical protection system of nuclear or radioactive materials or related facilities. The objective of DBT [17] is to establish a tool that creates a common basis, furthermore a precise and detailed technical basis, to allow the operator the creation of a physical protection plan and its approval by the competent authority in nuclear security. General onus for the development, use and maintenance of DBT is on State, see Figure 1. The summarized description of how to develop, maintain and use the DBT is based upon three stages: Threat assessment, DBT development and use and maintenance.

- **Threat Assessment** is a multidisciplinary activity for which the State has to bring together the necessary experts on each discipline to analyze all relevant information in order to produce the Threat Assessment Document (TAD) that generally describes all the threats the State has to consider.
- **DBT development**, based on TAD assessment, the aim is the generation of typical adversaries and the application of political considerations to produce the DBT Document containing the threat to protect and Beyond DBT Document with threats not appropriate to be included in the DBT, but the State obliges to guarantee a reasonable level of protection.
- **DBT use and maintenance,** to determine the responsibilities in design, implementation, assessment, use and revision of physical protection against DBT. The regulator has to evaluate physical protection systems to guarantee their efficiency against DBT. The global environment of threat is dynamic, so a revision process has to be stated.

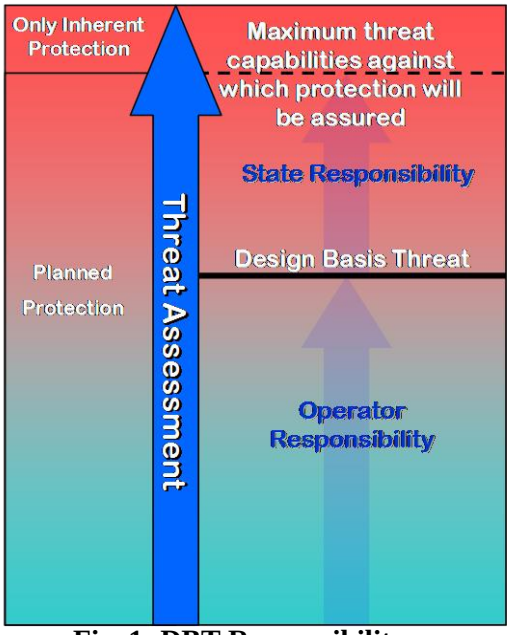

Fig. 1- DBT Responsibility

Once the BDT is defined, the next step is to use it to define and evaluate the Physical Protection System (PPS) that has to prevent from the successful completion of BDT [17].
Two aspects have to be considered to carry out an evaluation that provides a reasonable confidence in protection: The multidisciplinary character of these activities and the need to have the adequate specialists for each task and the criteria definition of adequate response against the threat.

[1] Initially classified as confidential but released after Fukushima's earthquake, now is taken as reference to face this kind of BDT.
[2] EPR Finland, VBER-300 FNPP, VVER 91/99, IRIS, PHWR-540, ACR-700, SWR 1000, VK-300, BN-800, AHWR (see ref [16])

The methodology of PPS Evaluation classifies the threats in two main types: (a) TT-1, threats that include the necessity of penetration in the facility by the enemies, and (b) TT-2, threats that start outside and do not need the presence of enemies in the facility. The evaluation process of the PPS can be described sequentially through the following stages:

1. Necessary entry information, in terms of DBT and BDBT, classified in TT1 and TT2.
2. Selection of scenarios, adapted to the specific characteristics of Plant.
3. Extreme Loads evaluation. After translating the scenarios in their Extreme Loads associated, the capability of SSC to face them is evaluated.
4. PPS and Vital Areas Definition. Generally PPS are set as successive barriers with a progressive increase of security requirements; the most protected areas are called Vital Areas.
5. Evaluation Methodology. The process performed up till now permits the definition of the two fundamental aspects to consider:
   - The threats and its translation to engineering parameters to the extreme loads associated
   - The SSC to protect the plant against the threat and their inclusion in areas to protect.

The next step is the effective performance of the evaluation of protective technical aspects against events TT-1 and TT-2 previously stated. This evaluation includes analysis of the impact on vital areas, the protection provided by the system of physical protection and extreme load analysis. If the evaluation is positive - i.e. the current system can face the threat - then it should be considered other layers of defence in depth, and mitigation of the consequences in hostile environments. Otherwise, the threat must be re-evaluated once the necessary improvements have been implemented.

After considering the response of emergency, including actions by state agencies to address the situation in an environment of aggression and the contribution of state security threats beyond the DBT, the state must decide whether or not, after the application of all available layers of defence in depth, the risk of a threat has been reduced to an acceptable level.

4 Extended Damage Mitigation Guidelines, EDMGs

After 9/11 Terrorist Attack the readiness of NPPs in USA to manage challenges to core cooling, containment and spent fuel pool cooling (SFP) following large explosions or fires was enhanced through a series of new legal requirements which resulted in 10 CFR 50.54(hh)(2). NEI 06-12 Rev.2 [15] provides acceptable guidance about mitigating strategies to fulfill those requirements, it was considered classified until the Fukushima Accident, when the USA Government released it; now it is a major reference in coping Hostile Acts against NPP.

Nuclear power plant licensees are responsible for overcoming design basis security threats and for using available resources to face beyond design basis threats. It is not feasible to define a "bounding" scenario because the wide range of beyond design basis terrorist threats so it was determined that a critical feature of the response should be flexibility to facilitate actions, over a wide range of potential scenarios. There are two critical elements of an improved response:

- Command and control enhancements aimed at improving initial site operational response before the Emergency Response Organization (ERO) is fully activated, and
- A specific set of mitigation strategies for all BWRs and PWRs to implement.

In this way it was identified a set of flexible, deployable generic enhancement strategies that could be beneficial in responding to a broad spectrum of damage states and they included:

- Procedure/guidance enhancements,
- Minimal procurement, and/or
- Minor plant modifications to non-safety related systems and portable equipment.

4.1 Command and Control Enhancements

Command and control is a key factor to mitigation success but it may be affected, avoiding procedurally required actions, proper communications, and other actions related with the Emergency Response.

To enhance command and control for these beyond design basis conditions there are provided the Extensive Damage Mitigation Guidelines (EDMGs), so called taking into account that the damage could affect equipment, plant operators and access to wide areas of the plant, with combinations of failures which might be considered of negligible probability in traditional severe accident analysis. The scope of the Initial Response EDMGs would include:

- An assessment of on-site and off-site communication.
- Methods for notifications and activation.
- Basic initial response actions, including key mitigation strategies.
- Initial damage assessment.

For developing the EDMGs, there were utilized, among others, the following assumptions:

- Imminent threat warning does not occur.
- Loss of access to the control room building and any content.
- Loss of all AC and DC power required for operation of plant systems.
- Minimum site staffing levels and a level of training in EDMG as in SAMG.

The initial response EDMGs are intended to provide a bridge between normal operational command and control and the normal command and control. The relationship between the initial response EDMGs, and other long-term response actions is shown below in Figure 2.

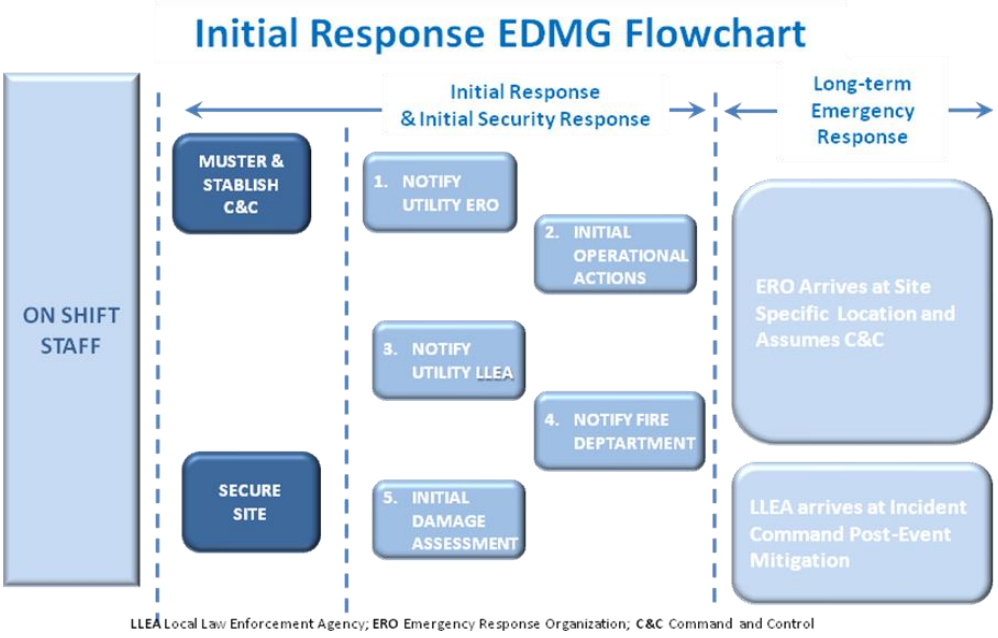

Fig. 2- Initial Response EDMG Flowchart

5 Training on Emergencies caused by NPP Attacks

Despite the low probability that the emissions produced by an attack on a commercial NPP are able to produce great damage, it is defined the Emergency Plan that acts as the last layer of the defence in depth. This Plan has the purpose to mitigate the consequences of a potential event that is supposed to happen, without analyzing its likelihood.

The aim here is to analyze the training that must have the personnel involved in responding to a NPP Emergency, caused by a security incident. It is considered that the fundamentals of emergency preparedness remain valid, but acknowledging that there are some relevant differences that recommend the development of specific training, including drills and exercises. These drills and exercises must be independent and be integrated into the general Emergency Preparedness Program.

Therefore, it is going to be reviewed the main characteristics of potential emergencies resulting from hostile action, studying the differences with accidental emergencies, throughout the main issues in the Emergency Plan. Once the differences have been defined, it will be analyzed the characteristics of specific training to deal with those emergencies, by two ways:

- By defining the main aspects on which it is considered that training should be approached, and
- Analyzing the characteristics associated with specific exercises and drills.

5.1 Differences between Accidental Emergencies and Attack Caused Emergencies.

Despite the fact that historically it is not true[3], there is a wide agreement that the most severe potential consequences of a security emergency at a NPP are associated with damages that can lead to big releases of radioactive material to health, nature or property. In this sense, there is no difference between accidental and other emergencies caused by a malicious act. However, it can be discerned important differences such as the different [19] need to share information or different ways to protect people. From a general point of view, the main differences in the characteristics of physical security emergencies from accidental emergencies could be summarized [20] as the following:

1. The media impact.
2. The potential medical consequences (in magnitude, mix of radiological and conventional weapons caused injuries).
3. The impact could be "directed" to maximize the consequences.
4. There may be secondary threats.
5. The potential sequence for the event is less predictable.

And, also from a general point of view, related with the response there can be found significant differences from the response to accidents, which can be summarized in the following points:

a) Many agencies, response forces and jurisdictions may be affected.
b) Intelligence, tactical response force and crime-of-scene procedures are critical issues.
c) There is an increased need for coordination: Of medical capabilities, of specialized response services, and of a large number of organizations, at all levels.
d) The lead organization may be a security or law-enforcement agency.
e) Protective measures.
f) Emergency timing.

As the worst consequences of attacks are similar to accidental emergencies, with some particular differences, and the basis for Emergency Preparedness (EP) remains valid, the aim of training should be focusing on the special aspects of the EP that are related to these situations, and drills and exercises should be defined to train and test those aspects most specifically related to de special characteristics of the emergencies originated by physical security events.

5.2 Operational and Logistical Challenges for First Responders

The following analysis of challenges to first responder (FR) is based on the practical experience gained in the three major nuclear accidents at Harrisburg (1979, USA; INES Scale 5), Chernobyl (1986, Ukraine; INES Scale 7) and Fukushima (2011, Japan; INES Scale 7), as analyzed in the CAST Database DERMI, and the terror threat scenarios developed in the CAST Project.

All of the above listed accident sites were power reactors, i.e., currently there is only limited practical experience of first responders for INES Scale accidents larger than 5 in a fuel fabrication facility, research reactor or reprocessing plant. The following scenario assumes that terrorist have staged a successful attack on a nuclear facility, resulting in an uncontrolled release of radioactivity into the environment, and on-site and off-site FR are responding to the attack. It is noted that both groups of FR face similar challenges in the immediate aftermath of such an event.

5.2.1 Environmental Boundary Conditions

Depending on the actual weather situation at the time of the accident, FR may be facing low night-time temperatures during winter or excessive day time heat in the summer. Either climatic

[3] Until now, the most severe consequences caused by terrorist attacks have happened through killing people shooting them with conventional weapons.

condition will pose technical challenges, ranging from: (a) Maintaining fire extinguishing water supply-lines and collection of radioactive contaminated run-off in subzero-temperatures, to (b) Search & rescue operations in personal protection equipment (PPE) in a hot and humid radioactive environment, whilst potentially facing terrorists on site. FR operations on site can be aggravated further by strong winds or floods.

5.2.2 Fire Fighters

Fire Fighters are likely to face difficulties reaching areas on site with their large and heavy trucks. The nuclear facility is likely to have been subject to extensive physical damage from the terror attack, resulting in large amounts of debris from damaged buildings on the access roads at the nuclear facility. Similarly, probable lack of electric power due to power outages and collapsed structures will impede initial access of fire fighters to victims trapped inside as well as hinder orientation indoors. Visibility can be further limited by heavy, potentially radioactive smoke from smoldering fires. Extinguishing fires will have to be carried out in the simultaneous presence of potential gun fire from terrorists remaining on site, increased radiation fields, as well as atmospheric emissions of toxic and possibly explosive gases. Under these circumstances rescue of injured and search operations for missing persons will be limited in time and space, whilst recovery of the dead will most likely have to be postponed to a later stage.

Workers are routinely operating in many locations on a nuclear site. In order to avoid direct confrontation with terrorists on site, fire fighters will need data on the current location of each individual in order to rescue staff trapped inside collapsed buildings. This necessitates that fire fighters are moving in their PPE in multiple confined spaces, which can be either radioactively contaminated or subjected to high dose rates. At the same time, fire fighters are likely to be exposed to electric hazard from damaged power supply lines. A topical issue will be to ensure that FR are also able to gain access to areas with enhanced physical access control, such as the control room area, with the staff inside potentially incapacitated or under the control of terrorists

5.2.3 Police

Police activities will focus on two topic areas: (a) Criminal events on scene at the nuclear facility; (b) Off site emergency support procedures. Due to the radioactive contamination all security operations will have carried out either wearing respiratory protection or additional PPE.

At the foreground of police actions will be the provision of physical protection for the staff and the nuclear facility, ultimately apprehending armed terrorists on site and safeguarding criminal evidence. Throughout the police operations additional victims and damage to the facility due to armed conflict cannot be excluded. At all times police units will have to provide site protection against unauthorized access to the nuclear site, which will include traffic regulation for large number of FR vehicles and personnel entering and leaving the facility.

A special task for police units will include assistance in evacuation procedures with the added complexity of a simultaneously ongoing counterterrorist operation. This will encompass traffic regulation for the anticipated large number of evacuees and self-evacuees, whilst preventing the escape of the terrorists on site and the potential covert attempt of additional terrorists to stage a secondary attack on the facility itself or on FR responding to the incident. Special attention will have to be paid to the transport of inmates from prisons.

5.2.4 Paramedics

Medical FR will not be able to attend to the victims on site until the security forces have declared the nuclear facility as secure. Therefore, the staging area for ambulances and associated staff will have to be guarded until the counterterrorism operation has been declared as completed. Paramedics will require police assistance in discriminating between injured staff members and potential terrorists, attempting to escape amongst the other injured victims. In this regard particularly the expected large number of the walking-wounded will pose a problem for the paramedics and the hospital staff to identify potential terrorists escaping from the scene as wounded victims.

5.3 Training focuses

Specific training to face emergencies originated by hostile attacks should focus on the following aspects or objectives of learning:

1. **Detection and Threat Assessment**. Both on-site and off-site Responders must be trained in the assessment of security threats, including decision-making on possible precautionary measures of protection and the Interface between Operation and Physical Security Organizations.
2. **Classification** must be trained specifically.
3. **Notification**, seen as some regulators have adopted a kind of short notice and prompt notification.
4. **Protective actions**. (On-Site). The training objective is to maximize protection of personnel during the emergency and it must consider situations in which the type of threat alters the usual response. Some measures that are specific and should be trained are:
    a. *Activation of the ERO* to Alternative Emergency Facilities and the initial response.
    b. *Evacuation* of threatened buildings as well as escape routes available.
    c. *Sheltering*, confining the staff in facilities away from potential targets.
    d. *Counting*, considering the planned dispersal of operators and supervisors.
5. **Initial Operation Actions**. The Emergency Response Organization, ERO must train the diagnosis of plant status and plan and mitigation actions implementation in emergencies caused by hostile actions, i.e., defined and directed from alternatives emergency facilities. It should be trained repairing actions. The objectives of the operating personnel will prevent and mitigate damage to the core and maintain the integrity of the containment. It must be trained the support to Operation staff both from ERO, including Logistics, as from off-site organizations.
6. **Off-Site Response**. The staff must be trained on Initial Response Actions, prioritizing and allocating resources and support to the site in response to the emergency.
7. **Mitigation** must be trained in case of great damage, training for it, at least:
    a. Using alternative resources to replace and/or support damaged equipments.
    b. Using physical security Site team and Off-Site Security Forces in an integrated way in the Command Post (local, on-scene) to allow coordinated movement of response resources.
8. **Communications**:
    a. Must be trained to use communications equipment, including alternative equipment and responding to malicious efforts to produce malfunctioning on them.
    b. Initial communications with local police and ORO (Off-site Response Organization).
    c. Coordination of resources to address the response to damage, including the coordination of off-site support and the Access Control.
    d. Specific training in the management coordination of victims in several ways:
        i. For a large number of victims, (e. g. by air attack).
        ii. Injuries combined by radiation and characteristic of the terrorist attack.
        iii. Evacuation of casualties to appropriate hospitals in each case.
        iv. Physical protection of healthcare workers.
        v. Use of protective equipment and communications.

5.4 Drills and exercises

Seeing as the main foundations of the EP are still valid, it is important to recognize that one of the most important aspects related to the training, if not the most important one, is the practical training on the particular characteristics of an emergency caused by a hostile act.

It is going to be reviewed the main points to be included in the exercises ranged in three levels; in the first level with generic points and more management related aspects; in the second level there are more concrete aspects but still perfect to discuss in exercises type Table Top, and in the third level where it can be found aspects more related to the field deployment. Based on well known references, it is recommended [20] that such exercises should have the following training and test general and high level targets:

a) To increase Coordination capabilities:
    a. Between organizations that are not normally involved in the response to Nuclear / Radiological Emergencies.
    b. Between intelligence agencies, response forces with law enforcement agencies and first responders, specialized radiological emergency response units and facility management.
    c. With the Media Communications in a situation of public fear and media survey.
    d. With medical arrangements to respond to an event with mass casualties, possibly contaminated and with medical consequences in a security threat scenario.
b) To increase the capabilities of specialized services to properly respond at the NPP and Off-Site.
c) The ability of all FR to work in this kind of stressful emergencies, considering for example that there may be secondary threats, and to work under the leadership of a security or law-enforcement agency.

At the second level, it could be defined a specific area to train in the Emergency Response in case of hostile actions against NPP; the assessment of the threat and to define properly the response. In this level, the main objectives to train in order to be well prepared to face these emergencies could be summarized [20], [21], [22] as follows:

a) Assess the threat in terms of credibility and potential impacts.
b) Effectively communicate the threat level to emergency response organizations and, when appropriate, the public.
c) Develop an appropriate plan for precautionary protective actions in case of a credible threat.
d) Implement appropriate precautionary protective actions to protect people and workers.
e) Activate medical services and support facilities.

Finally the third level of training issues, more related to in-field response to emergencies caused by attacks, could be summarized as follows:

a) Establishing an effective command and control system with many FR organizations.
b) Implementing appropriate defensive/precautionary actions to properly protect.
c) Rapidly field deployment of FR, including medical teams, dealing with a large number of casualties, and fire fighters dealing with big fires.
d) Deploying triage areas properly provided, managed and protected.
e) Protecting FR on the field of operations, and handling of potential evidences.

5.5 Conclusions and recommendations

The main finding is that, even though the basis of nuclear emergencies remains valid in these situations, there are specific characteristics that recommend:

1. To review the Emergency Plan in order to define the changes, improvements and adaptations needed to better face the specific aspects related to hostile attacks. In this way, and based on well known references it can be recommended to develop:
    a. Specific arrangements and procedures.
    b. Specific emergency equipment and facilities (i.e. alternate facilities properly equipped) and specific support software to face these situations.
2. To develop a systematic approach to train in order to define the specific training needed in some particular aspects of the Emergency Plan, taking account the different groups of responders and the different threats, to guarantee with a reasonable confidence that, even in the worst case, the staff in charge of face the emergency have been trained properly.

6 Acknowledgments

Except paragraph 4, which has been included after the related documents have been released, the rest of the paper has been developed in the CAST project, Comparative Assessment of Security-centred curricula for Training First Responders on disaster management in the EU, funded by the European Commission, through the Seventh European Framework Programme Security Area, CAST, GA No.: 218070, Call FP7-SEC-2007-1.

7 References

[1] Nuclear Reactor Hazards. A. Frogatt Nuclear Power: Myth and Reality. Nº2, Dec. 2005.Nuclear Issues Paper No. 2
[2] Attacks on Nuclear Reactors: The Implications of Israel's Strike on Osiraq. Bennett Ramberg. Political Science Quarterly, Vol. 97, No. 4 (Winter, 1982-1983), pp. 653-669. The Academy of Political Science.
[3] Principios Fundamentales de Seguridad, Nociones fundamentales de seguridad, SF-1, IAEA, 2007. STI/PUB/1273, ISBN 978–92–0–308707–0, ISSN 1020–5837
[4] Defense in depth in nuclear safety: INSAG-10. IAEA, 1996., ISSN 1025-2169.
[5] The Physical Protection of Nuclear Material and Nuclear Facilities. INFCIRC/225/Rev.4
[6] Guidance and considerations for implementation of INFCIRC/225/Rev.4, the physical protection of nuclear material and nuclear facilities. IAEA-TECDOC-967 (Rev.1). IAEA, 2000.
[7] Nuclear Renaissance, Human Security And Political Risk, Rajesh M. Basrur, S. Rajaratnam School of International Studies Nan yang Technological University, Singapore, Paper presented at the Second Annual Convention of the Consortium of Non-Traditional Security Studies in Asia (NTS-Asia), Beijing, November 10-11, 2008
[8] Terrorismo Nuclear, Tnte. Ing. de Armamento C. Martín. La Energía y su relación con la Seguridad y la Defensa. Monografía 98 del CESEDEN. Ministerio de Defensa, España.
[9] Deterring Terrorism: Aircraft crash impact analyses demonstrate Nuclear Power Plant's structural strength, EPRI-NEI, 2002.
[10] Risk Characterization of the potential consequences of an armed terrorist ground attack on a U.S. Nuclear Power Plant. EPRI, 2003.
[11] EPACT05, P.L. 109-58
[12] Mark Holt & Anthony Andrews, Nuclear Power Plant Security and Vulnerabilities, US Congressional Research Service, 7-5700, RL34331, 2010
[13] Meserve, Richard A., NRC Chairman, Research: Strengthening the Foundation of the Nuclear Industry, Speech to Nuclear Safety Research Conference, October 29, 2002
[14] National Academy of Sciences, Board on Radioactive Waste Management, Safety and Security of Commercial Spent Nuclear Fuel Storage, Public Report (online version), 2005.
[15] NEI 06-12 B.5.b Phase 2&3 Submittal Guideline. Rev, 2 NEI, 2006
[16] Advanced nuclear plant design options to cope with external events. IAEA-TECDOC-1487, 2006
[17] Development, use and maintenance of the design basis threat. IAEA nuclear security series no. 10; STI/PUB/1386 ISBN 978–92–0–102509–8
[18] Engineering safety aspects of the protection of nuclear power plants against sabotage. IAEA Nuclear Security Series no.4, Technical Guidance. IAEA 2007.
[19] Bulletin 2005-02: Emergency Preparedness and Response Actions for Security-Based Events. USNRC–NSIR. WASHINGTON, D.C. 20555-0001. July 18, 2005.
[20] Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency. IAEA, VIENNA, 2003. EPR-METHOD (2003). IAEA 2003.
[21] Guideline for the Development of EP Drill and Exercise Threat-Based Scenarios. NEI 06-04, Revision 0. Nuclear Energy Institute. Washington, 2006. (202.739.8000)
[22] Conducting a Hostile Action-Based Emergency Response Drill. NEI 06-04, Revision 1. Nuclear Energy Institute. Washington, 2007. (202.739.8000)