Engineering solutions to ensure protection of nuclear power plants against sabotage.

Dimitar Dimitrov
Bulgarian Academy of Sciences - Institute of Metal Science Equipment and Technologies with Hydroaerodynamics Centre "Acad. A Balevski", Sofia, Bulgaria
E-mail: ddimitrov@ims.bas.bg

Abstract: *The protection of nuclear installations against malicious acts can take a number of different forms. This report addresses only issues related to the sabotage of nuclear facilities - prevention or mitigation of sequences initiated by malicious acts that may have potential radiological consequences. Nuclear power plants have good physical protection systems (PPSs) and procedures, and they are designed to minimize the likelihood of an accident and in the event of an accident, not to release radioactive material in an uncontrolled manner. The objective of this report is to provide methods for evaluating and for proposing corrective actions aimed at reducing the risk related to any malicious act that, directed against a nuclear power plant, could endanger the health and safety of plant personnel, the public and the environment.*
KEYWORDS: *NUCLEAR FACILITIES, PROTECTION OF NUCLEAR INSTALLATIONS, MALICIOUS PURPOSES, MALICIOUS ACTS, SABOTAGE OF NUCLEAR FACILITIES, PHYSICAL PROTECTION SYSTEMS, CORRECTIVE ACTIONS.*

1. Introduction

Since the attacks of 11 September 2001, the perception of the potential terrorist threat to nuclear installations has changed significantly. Within the nuclear industry, the immediate international response was to enhance security by augmenting the forces guarding installations, increasing physical protection by installing additional security devices, enhancing protection procedures, tightening access control, increasing standoff distances for surface vehicles, reviewing and updating emergency preparedness, and generally increasing awareness of the need for close cooperation, at all levels, between government and private sector entities concerning warning and response.

It was less clear what additional analyses could and should be performed to determine whether the structures, systems and components important to safety at nuclear power plants provide optimum physical protection against potential terrorist attacks and to identify any cost beneficial changes in the form of back fits

Many licensees of nuclear power plants around the world, in some cases mandated by their regulatory agencies, carried out calculations of the robustness of plant structures when subjected to aircraft impacts, taking into account dynamic and resulting fire effects. These calculations were generally limited to the performance of passive structures and systems.

In any terrorist attack or act of sabotage, the overarching concern is to achieve and maintain a safe shutdown condition, including continued availability of heat sinks and containment of radioactive material until the incident has been brought under control. This publication provides guidelines for the assessment of the engineering safety aspects of the protection of nuclear power plants against sabotage, including standoff attacks.

The Nuclear Security Fundamentals publication [1] provides the objective and essential elements for the entire nuclear security regime. Recommendations indicate what a nuclear security regime should address for the physical protection of nuclear material and nuclear facilities [2], radioactive material and associated facilities [3], and nuclear and other radioactive material out of regulatory control [4]. These publications recognize the particular threats that could be posed by insiders, as well as the need to implement specific measures against insider threats and to evaluate those measures accordingly.

2. Objective

In the light of the current threat environment, the overall objective of this report is to provide methods for evaluating - and, if necessary, for proposing corrective actions aimed at reducing (mainly through upgrades) - the risk related to any malicious act that, directed against a nuclear power plant, could endanger the health and safety of plant personnel, the public and the environment through exposure to radiation or the release of radioactive substances [5].

This report describes a methodology for assessing the capacity of a selected subset of a nuclear power plant's safety related structures, systems and components (SSCs) to withstand sabotage induced events. The proposed methodology, which includes screening, applies existing safety margin assessment techniques in an integrated manner. Specifically, the aims of this report are to:

(a) Provide a link between the information in The Physical Protection of Nuclear Material and Nuclear Facilities [6], general guidance on the physical protection of nuclear material and nuclear facilities against sabotage, and engineering safety aspects of protection against sabotage;

(b) Provide a link with general guidance on the identification of vital areas within nuclear facilities and on the development and maintenance of the design basis threat (DBT);

(c) Provide general guidelines for the assessment of nuclear facilities in relation to sabotage induced sequences;

(d) Use common terminology drawn from established (i.e. consensus) definitions or define new terms, when necessary, to clarify joint safety/ security concepts;

(e) Propose a safety margin assessment approach that allows for the use of different acceptance criteria from the design process (e.g. best estimate versus design allowable);

(f) Provide for an assessment process so that decisions can be made by the operator (or regulator) of an installation concerning the need to enhance or upgrade the safety related SSCs, the physical protection measures or on- or off-site emergency procedures;

This report covers all nuclear facilities, including nuclear power plants, research reactors, and fuel fabrication plants, reprocessing plants and spent fuel storage facilities. However, the emphasis is on nuclear power plants because they involve the most complex analysis.

Events considered to be within this scope include those that:

(a) Involve forced intrusion into the protected area of the site (i.e. the area under the administrative control of plant management), such as by a 'malicious vehicle' (e.g. a truck loaded with explosives and carrying armed intruders);

(b) Are initiated by persons outside the site area. Such an event may involve missiles, the release of a toxic gas within the site area or an aircraft steered to hit the installation;

(c) Are initiated by insiders;

(d) Include multiple modes of attack, for example, combinations of the above events;

Two types of threat are distinguished:

(a) Threat type 1 (TT-1) refers to those threats posed to the nuclear power plant by insiders or by adversaries intending to intrude into the facility (with or without insider assistance).

(b) Threat type 2 (TT-2), in contrast, refers to threats that are initiated outside the plant boundary and do not require the presence of the adversaries on-site. Examples of this type of threat include standoff attacks such as shoulder launched missiles and malicious aircraft impacts.

Obviously, specific criteria are needed to perform risk assessments. Generally, these criteria are provided by the national nuclear regulator. The following is a sample set of criteria:

(a) Is the nuclear power plant sufficiently robust to prevent immediate, uncontrolled release of significant amounts of fission products (i.e. catastrophic failure) in the event of an attack?

(b) Do the essential safety systems continue to perform their functions (e.g. to cool the nuclear fuel and contain the release of radioactive material), or can they be started and operated as needed?

(c) Following an attack, can the essential safety systems be operated until repairs can be carried out, even given related effects such as fire, smoke and structural damage?

(d) Are the design and operation of the nuclear power plant and the response procedures and capabilities such that any exposure of the public and facility personnel is minimized in the event of a large external attack?

The evaluation methodology outlined provides a means to determine whether one or more safe shutdown paths exist to perform the required safety functions when subjected to a given threat scenario. The term 'success path' refers to a minimal set of components for a subset of plant systems whose operability and survivability are sufficient to ensure that the plant performance criteria are met, as required and defined by the regulator or other governing body. A success path may include plant functions beyond safe shutdown if the metric of interest is radioactive release to the environment below an acceptable limit.

The term 'safe shutdown path' is defined here as a minimal set of components required achieving and maintaining a safe shutdown condition without consideration of containment or exposure of the public due to radioactive releases. While the terms 'safe shutdown path' and 'success path' are not necessarily identical, they are used interchangeably in this report. Furthermore, the term 'performance criteria' is used to denote criteria related to the type of function (performance) required from the SSCs.

The term 'acceptance criteria', in contrast, refers to the allowable behaviour limits for the SSCs in relation to the given function. Both are determined by the regulatory body.

3. Evaluation methodology

3.1 Threat evaluation

Every operator has to define the consequences with regard to which the nuclear threat is to be evaluated. In the case of sabotage, the criteria are related to the safety of plant personnel and the public, and the risk acceptance criteria are described in terms of radiological consequences [6].

The DBT describes the "attributes and characteristics of potential insider and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated" [6].

Threats that may need to be considered by the plant but that are not included in the DBT are referred to as being 'beyond the DBT'. The distinction is made because acceptance criteria used for events beyond the DBT may differ from those used for DBT events **[7].** All threats may also be described in terms of TT-1 and TT-2.

3.2 Development of specific threat scenarios

This step in the evaluation process aims at better defining the threat scenarios with regard to the specific facility being evaluated [8]. This process may lead to the exclusion of some scenarios on the basis of the following considerations:

Site and installation characteristics

The surrounding topography and vegetation may be sufficient to exclude certain scenarios of threats initiated outside the plant boundary. For certain types of threat, the location and layout of the plant site may limit the likelihood that particular on-site areas will be affected.

For example, a plant's location in hills, mountains or a valley may limit the feasible approach angles and speed of large aircraft in an attack on the site. Other factors, such as the location of transmission lines, may limit approach paths for attacks by large aircraft. For blast loading conditions, the shielding of structures provided by topographic effects and adjoining structures may limit the area of influence and thus should be taken into account.

Similarly, potential site conditions that may benefit adversaries also need to be taken into careful consideration, for example, the proximity of nuclear facilities to public transport infrastructure (roads, railways, and airports) or to industry and populated areas. Research reactors tend to be located within research centres or on university campuses, which may make the identification of potential intruders or attackers difficult.

Type and number of facilities at the site:

A nuclear power plant may have several reactor units on-site, with the possibility of interdependent safety or support systems. Multi-unit sites often assume the availability of companion unit systems when addressing non-common-cause events. In addition, other critical facilities may be present within the plant boundary, such as those for spent fuel storage in fuel pools or dry cask storage.

Research reactor sites may have associated laboratories, isotope production facilities and hot cells. All facilities at the site may require simultaneous physical protection when subjected to TT-2 attacks.

The evaluation should take into consideration all on-site facilities and any interdependence of their safety systems. Such consideration includes consequence assessment of environmental discharges that are cumulative for all facilities on a site.

Design

Nuclear power plants are designed for a wide range of extreme environmental loading conditions. The measures to defend against design basis internal and external events - such as fire, pipe whip, earthquakes, extreme winds, explosions or aircraft impacts - provide an 'envelope' of protection for a nuclear power plant.

It is important that this protection be taken into account when evaluating threat scenarios. In fact, some scenarios may be excluded from further consideration because they are effectively bounded by design basis conditions. Bounding can be demonstrated on the basis of the event (for the whole facility), the extreme load (for each item) or the sizing requirement derived from the loads.

Facility independent off-site security measures

Administrative and other measures in force outside the plant boundary are called facility independent off-site security measures. These measures can range from increased security in the aviation industry to surveillance performed by off-site entities in the vicinity of the site. If they are in place and effective, the measures may serve to exclude certain threat scenarios from consideration or to better define the parameterization of threat scenarios.

In the screening process for external events of a natural or an accidental human induced origin, two methods are generally used:

screening by distance and magnitude, and screening by probability of occurrence. In the first method, the minimum distance and the maximum magnitude (i.e. the most conservative conditions) of the event are postulated with regard to the nuclear power plant site, and the potential damaging effects on plant safety are assessed.

If the effects are found to be insignificant, the event is screened out with regard to the assessed parameter. For example, an attack scenario involving a vehicle containing explosives may be screened out on the basis of the effective barrier's distance from the safety related systems of interest.

3.3 Extreme environment load evaluation

The sabotage threat scenarios to be evaluated may be of two types, TT-1 or TT-2. The scenarios are described in sufficient detail such that the extreme environment associated with each can be specified.

The focus here is on the engineering safety aspects of the threat scenarios and the associated extreme environment. The list of potential threats encompasses internally and externally initiated events, and combinations of the two. In addition, multimode threats, as described herein, are identified and evaluated. It is expected that some of the threat scenarios will involve intruder attacks, either alone or as part of a multimode attack.

The objective of the extreme environment load evaluation is to provide the plant engineering organization with a matrix of environmental conditions produced by the threat scenarios, which can be applied to portions of or the entire facility. The result is an environment load table that specifies the environmental loads and load combinations to be considered by the plant engineering staff in evaluating of structures, systems and components (SSCs) necessary for successful plant performance. Given this information, the plant engineering organization can determine the facility's capability of resisting the threat. The environment load evaluation serves as the interface between the threat scenarios and the evaluation process; it includes only the engineering aspects, and not the details of the threat scenarios.

In the evaluation process, the inherent strengths of facilities due to the design and construction conditions should be recognized. In this process, the focus is on the SSCs required to safely shut down the facility and maintain it in a safe shutdown condition throughout the period required for recovery actions and for additional entities outside the plant to assist, if necessary. Structures, systems and components are designed and evaluated for a large number of environmental conditions:

- Structures generally provide one or more of the functions of pressure retention, shielding and confinement, and support to systems and components. Structures and structural elements are designed for the operating and accident conditions expected throughout the life of the facility. Operating loads include dead load, live load, atmospheric temperature, thermal loads, vibration, radiation effects, pressure retention and ageing effects (radiation, corrosion and other effects of material degradation). Structures are designed for accidental loads such as missile impact (internally or externally generated), extreme winds, flooding, earthquakes, explosions/blasts (internally or externally generated), extreme heat loads, extreme radiation effects, impulse loads due to pipe whip and other phenomena, and heavy load drops. Some of these loading conditions are considered in the design to act simultaneously.

- Systems are, in general, designed for a companion set of operating and accident conditions for structures. System design also includes considerations of redundancy of function and separation, segregation and diversity of trains and elements to provide high reliability for successful system performance under both normal operating and accident conditions.

- Components are generally designed for a companion set of operating and accident conditions for structures and systems. However, the environments for which components are designed, qualified and maintained are typically more extensive than those for structures and systems. Normal operating conditions comprise a wide range of specified conditions (e.g. temperature, humidity, radiation, cooling, vibration) under which components must function (e.g. pumps delivering fluid at a specified flow rate).

4. Overview of design and evaluation of physical protection systems

The PPS in a nuclear power plant is designed to protect the facility against the DBT. During a DBT event, the engineering safety aspects support the PPS and constitute an additional layer of defence in depth. A very brief description of a PPS is included here for completeness. The effective assessment and implementation of this procedure requires the integrated efforts of the PPS experts and those personnel responsible for engineering and operational safety.

4.1. Physical protection systems

Physical protection against sabotage requires a combination of hardware (security devices), procedures (including the organization of guards and the performance of their duties) and facility design (including layout). The physical protection measures are designed taking the nuclear facility's characteristics, the nuclear material, the DBT and the potential radiological consequences into account.

An effective PPS performs the primary functions of [9]:

(a) Deterrence;

(b) Detection and assessment;

(c) Delay;

(d) Response.

4.2. Vital area identification

A vital area is an "area inside a protected area containing equipment, systems or devices, or nuclear material, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences" [6].

By evaluating the consequences of malicious acts, safety experts, in close cooperation with security experts, identify potential sabotage targets within nuclear facilities that require protection to prevent unacceptable radiological consequences in the case of an attack [6]. The minimum complement of equipment, systems and devices may include all designated safety systems if required by the overall safety philosophy.

Alternatively, the minimum set may be a subset of all equipment, systems and devices, again dependent on the criteria established by the regulatory body or its designee. The VAI process is complex, and many different methodologies may be used. The number and extent of the vital areas are facility specific.

As mentioned above, the VAI process involves target identification, which is the basis of PPS design. Target identification focuses on what to protect, while a PPS design addresses how to protect identified targets.

Target identification does not consider whether the physical protection measures can be overcome or the difficulty of providing physical protection. In other words, target identification identifies areas, components or functions to be protected; the threat to these items and the ease or difficulty of protecting them against a threat is considered after the items have been identified.

4.3. Sabotage margin assessment (SMA) procedure

Generally, the SMA approach to evaluating the capacity of engineering safety features comprises the following steps.

(a) Introduce into the evaluation process the extreme environment definition matrices, which contain the definition of loading environments and load combinations for engineering evaluations. These extreme environments may include impact, explosion/blast,

heat/ fire, vibration, hazardous material release, flooding and other site specific conditions.

(b) Define the overall performance criteria for the nuclear power plant subjected to the extreme loading environments. For example, the overall performance criteria may be defined as hot or cold shutdown for 24 h after the threat scenario is initiated. A further assumption is that additional aid from outside the plant boundary can be effectively mobilized within 24 h.

(c) Define the assumptions that will be used in the engineering evaluation. Examples of assumptions for a nuclear power plant are:

(d) Define SSC capacity criteria.

(e) Define one or more safe shutdown or success paths.

(f) Verify that each candidate vital area set identified in the VAI process contains the equipment for at least one success path. An alternative approach would be to determine the candidate vital area sets and then perform the capacity evaluation on some or all of them.

(g) Identify the SSCs that make up the safe shutdown path(s) and are required to function during and after the threat scenario event, given the aforementioned assumptions. Define the specific functions that these SSCs must perform during and after the event. Note that some threat scenarios may have such large affected areas or footprints that a simple screening of the overall plant site for likelihood of significant damage within the footprints may limit the number of SSCs to be evaluated.

(h) Evaluate SSC capacity when subjected to the extreme environmental loading conditions specified.

(i) Define a measure of plant capacity, such as the high confidence of low probability of failure (HCLPF) when subjected to the identified threat scenarios.

4.3. Composition of the sabotage margin assessment team

The SMA team comprises:

(a) Plant experts knowledgeable about plant systems, security, operations and engineering, who are responsible for converting the threat scenarios into specific extreme loading conditions in different areas of the plant. This activity should be treated as strictly confidential, with the extreme loading conditions produced being passed on to relevant experts for evaluation.

(b) Experts in security (PPSs) supplemented with experts in plant operations and on-site emergency management.

(c) Experts in engineering safety assessment, system design, engineering (civil, structural, fire, electrical, mechanical, instrumentation and control) and plant operations. This aspect of the assessment team is the focus and the related activities ultimately screen out certain SSCs with regard to the relevant extreme loading conditions and identify those for which more detailed analysis is required.

Other experts in areas such as missiles, aircraft or demolition are helpful in the evaluations.

Procedures need to be in place to minimize the disclosure of confidential information, especially to the experts responsible for evaluating SSC capacity when subjected to specific environmental loading conditions. One goal is to keep threat information separate from plant condition information, particularly when informing the relevant experts - who do not need to know threat specifics. This is accommodated by the SMA approach.

5. Conclusions

The facts presented in this report are based on the premise that the design, layout and safety infrastructure built into existing nuclear facilities may be of considerable benefit in mitigating the effects of malicious acts. However, this benefit may not apply uniformly to all threats and all required safety functions.

The evaluation process described here, together with the proposed model for the interaction of specialists in the operation of nuclear facilities, nuclear safety engineering and physical protection, provides plant management and other stakeholders with the robustness and vulnerability information needed to make decisions concerning upgrades or implementing other means to reduce the risk to the public.

Decisions to allocate the resources required for upgrades and changes are based on estimated improvements in the capacity to either prevent the act of sabotage or eliminate its ability to initiate a release of radioactive substances.

Specifically, decisions are based on:

(a) Estimated 'performance' improvements (e.g. margin improvements);
(b) Ease of implementation;
(c) Time for completion of upgrade (e.g. outage);
(d) Time at risk.

6. Acknowledgement

The issues discussed in this report are aimed at the implementation of Work Package 2 "Intelligent Security Systems" of the project BG05M2OP001-1.002-0006 "Construction and development of a Center of Competence" Quantum communication, intelligent security systems and risk management (Quasar)", which has received funding from the European Regional Development Fund through the Operational Program "Science and Education for Smart Growth" 2014-2020.

Bibliography

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/ Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, International civil aviation organization, International criminal police organization-interpol, United nations interregional crime and justice research institute, united nations office on drugs and crime, world customs organization, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering safety aspects of the protection of nuclear power plants against sabotage, technical guidance, IAEA, Vienna, (2007).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/ 225/Rev. 4 (corr.), IAEA, Vienna (1999).

[7] Valeri Panevski. Possible approach for standard operating procedures development for intelligent security systems functioning. International Scientific Journal “Security&Future”, 5, 3, STUME, 2021, ISSN:2535-082X (online), 2535-0668 (print), 81-84;

[8] P Valeri Panevski. Possible integrity framework between the Intelligent Security Systems parameters and the Business Continuity Management processes. International Scientific Journal “Security & Future”, 5-ти, 2-ри, Scientific Technical Union of Mechanical Engineering “Industry-4.0”, 2021, ISSN:2535-0668 (print), 2535-082X (online)), 42-45;

[9] Valeri Panevski. Some standardized peculiarity in defining the processes / stages providing input data for Intelligent Security Systems development – peripheral security systems. International Scientific Journal “Security & Future”, 5-ти, 1-ви, Scientific Technical Union of Mechanical Engineering "Industry 4.0", 2021, ISSN:2535-0668 (print), 2535-082X (online)), 3-6;