Development of The Efficient Emergency Preparedness System for The Nuclear Critical Infrastructure

Venceslav Kostadinov1, Jure Marn2, Stojan Petelin3

1) SLOVENIAN NUCLEAR SAFETY ADMINISTRATION
   Železna cesta 16, SI-1000 Ljubljana, SLOVENIA
   Venceslav.Kostadinov@gov.si

2) UNIVERSITY OF MARIBOR
   Faculty of Mechanical Engineering
   Smetanova 17
   SI-2000 Maribor, SLOVENIA
   Jure.Marn@Uni-MB.SI

3) UNIVERSITY OF LJUBLJANA
   Faculty of Maritime Studies and Transportation
   Pot pomorscakov 4
   SI-6320 Portoroz, SLOVENIA
   Stojan.Petelin@fpp.edu

ABSTRACT

The evaluation of the critical nuclear infrastructure vulnerability to threats like human occurrences, terrorist attacks and natural disasters and the preparation of emergency response plans with the estimation of optimized costs are of the vital importance for the assurance of a safe nuclear facilities operation and the national security. In the past national emergency systems did not include vulnerability assessments of the critical nuclear infrastructure as the important part of the comprehensive preparedness framework. The fundamental aims of the efficient emergency preparedness and response system are to provide a sustained emergency readiness and to prevent an emergency situation and accidents. But when an event happens the mission is to mitigate consequences and to protect the people and environment against the nuclear and radiological damage. The efficient emergency response system, which would be activated in the case of the nuclear and/or radiological emergency and release of the radioactivity to the environment, is an important element of a comprehensive system of the nuclear and radiation safety.

In the article the new methodology for the critical nuclear infrastructure vulnerability assessment as a missing part of an efficient emergency preparedness system is presented. It can help the overall national energy sectors to identify and better understand the terrorist threats and vulnerabilities of their critical infrastructure. The presented methodology could also facilitate national agencies to develop and implement a vulnerability awareness and education programs for their critical assets to enhance the security, reliability and safe
operation of the whole energy infrastructure. The vulnerability assessment methodology will also assist nuclear power plants to develop, validate, and disseminate the assessment and survey of new efficient countermeasures.

The significant benefits of the new vulnerability assessment research are to increase nuclear power plants security, reliability and availability. The basic objectives of performing a nuclear power plant vulnerability assessment are to better understand threats and vulnerabilities, determine acceptable levels of a risk, and incorporate countermeasures to reduce identified vulnerabilities. The prevention of a nuclear power plant shutdown because of the terrorist attack or sabotage will avoid loss of overall national economic activities. Initial estimates of only economic losses due to the nuclear power plant shutdown because of the terrorist attack and/or sabotage could run into millions of dollars, depending on the size and types of areas affected.

First attempts of developing the new methodology for the nuclear critical infrastructure vulnerability assessment as a part of an efficient emergency preparedness system are presented.

1 INTRODUCTION

1.1 Risk Assessment after 01/09/2001

For long time the security and the safety have been key priorities at nuclear power plants and the nuclear critical infrastructure like facilities that manufacture, store, use, or handle the hazardous nuclear material. After the terrorist attacks on 11.09.2001, a new and immediate risk model has been existing [1]. The decision-makers become aware that the nuclear critical infrastructure could also be an attractive target to terrorism, with the purpose of using the physical and radioactive properties of the nuclear material to cause mass casualties and property damage with detrimental economic or environmental impacts.

The capability to evaluate a nuclear plants vulnerability to different kinds of threats, like human occurrences, terrorist attacks and natural disasters, and the preparation of the national emergency response planning framework, including estimation of needed costs, are of the vital importance for an assurance of a safe operation of the critical nuclear infrastructure and the national security. All kind of nuclear facilities could be potential targets for an attack of terrorist organisations world-wide.

Some analyses and assessments of similar topics have been stated in some older articles like as in recent ones [2-11]. Moreover, the assessment of the possible military attack on a NPP as early as in 1991 was also presented [5]. In those articles some bases and new insights into models and the new methodology for vulnerability assessments of different types of facilities have been presented. Some ideas were useful for our framework and some topics were the base for developing the new vulnerability assessment methodology for the critical nuclear infrastructure.

By adapting simplified but sophisticated risk analytical processes and assessments [6-10], we would be able to evaluate [11-15] where are potential vulnerabilities on a wide range of threats to some critical nuclear infrastructure assets: the nuclear facilities, the utility staff, the essential knowledge, the information technology, the plant control room and technical support center, the electrical dispatch center and the electrical power transmission.

Armed with such vital insights, nuclear operators and nuclear regulatory bodies could plan and optimise changes in oversight procedures, organisations, equipment, hardware and software to reduce risks consistent with security and safety of a nuclear power plants operation, budget, manpower, and other limitations.

We have started our original work in 2004 by first adopting the vulnerability methodology and by developing procedures for a nuclear regulatory vulnerability assessment
of nuclear power plants [10, 12]. In the article initial qualitative and new quantitative vulnerability estimations for nuclear applications are shortly presented.

1.2 The Basic Definition and Different Types of Risk

In the changed world of the turbulence we need the new or at least an improved definition of risk and types of risk. In view of the possible terrorist sabotage and attack on nuclear power plants, it is an urgent need for reassessing effectiveness of the existing protective measures. The nuclear regulators need new risk based decisions for monitoring a security and a safe operation of the critical nuclear asset, especially nuclear power plants (NPPs), regarding possibility of a sabotage and terrorist attacks. Therefore it is a need for developing the new strategy and methodology for terrorism risk assessments of nuclear power plants [11-15]. The new approach is somewhat different in comparison with the methodology for a classical risk assessment.

The classical definition of a risk usually assumes to be a product of a probability of an event and its consequences. Sometimes a risk could also be defined as a frequency of events times its severity. The design of old NPPs had possibly assigned a little more weight on a likelihood of occurrences of severe NPP accidents than on a severity of their consequences. Thus, the nuclear management and regulators have performed the categorisation of design basis accident consequences. The design and safety analyses of NPPs had considered an identification of the postulated trigger events and assumed their frequencies [9]. Then developing scenarios and consequences for trigger events have been evaluated. The nuclear industry in this way has based control of a safe operation and design limits of NPP safety systems.

This strategy has also greatly influenced nuclear plants’ operational procedures. Because of assumed a very low probability of very severe accidents (beyond design bases) and especially postulated a very low probability of terrorist attacks, these trigger events had not been considered in design and safety analyses of nuclear power plants. Consequently the overall potential magnitude of a risk has been underestimated. In short, the typical classification of trigger events was mainly based on their initiating frequency. Therefore, at design stage trigger events were mostly analysed depending on their postulated likelihood of occurrence.

That very important fact has reappeared at newer advanced nuclear plants (facilities) design before 09/11/2001, therefore complete NPPs vulnerability and terrorist risk assessments had unfortunately not been taken into account. But after it overall “risk picture” has dramatically changed and now engineers, management, decision makers and politicians are aware of a very real possibility of terrorist attacks (internal and external) on the critical nuclear infrastructure, especially on nuclear power plants and research reactors [13]. Actually a very important presumption could be that the nuclear critical infrastructure emergency arrangements (preparedness and anticipated response) could be essentially improved. To improve their national nuclear regulatory emergency arrangements, world-wide all nuclear administrations need to develop the new vulnerability assessment methodology and solution methods.

The new strategy needs the comprehensive definition of a terrorism risk assessment. The comprehensive integrated risk assessment definition could include the safety concerns, asset performance and cost [11-15]. As a first step in developing the new methodology, we need deeper understanding of the new terminology and definition of the threat analysis at a NPP risk assessment. Especially, we need to include the new important component in the risk assessment model, namely the vulnerability assessment (VA) of the critical nuclear infrastructure assets (objects).
2 OBJECTIVES AND BENEFITS OF NEW NPP VULNERABILITY ASSESSMENT METHODS

The basic objectives of performing nuclear power plant vulnerability assessments are to improve understanding of threats to NPPs and their vulnerabilities, to determine the acceptable levels of risk, and to incorporate new countermeasures to reduce identified vulnerabilities. The direct benefits of a performing nuclear power plant vulnerability assessment include:

- Defining key critical nuclear infrastructure assets (especially NPPs and research reactors as key critical assets).
- Identifying vital NPPs vulnerabilities (weak points) and timely developing preventive plans and effective emergency responses.
- Developing methodology and methods for integrated risk management process.
- Developing and sustaining internal new skills and expertise.
- Initiating new industry and regulatory actions and standards for NPPs responses.
- Establishing cost-effective and efficient countermeasures and training programs, and
- Establishing and disseminating consciousness of necessity to develop and implement new standards and regulatory principles.

The significant benefits of the vulnerability assessment research are related to an increased NPPs security, reliability and availability. Actually the effective, secure and safe operation of the critical energy (nuclear) infrastructure (especially NPPs) is crucial for the integrity of the national security, human health and safety and the economic vigour of nations. Consequently the safe operation, security and reliability of the critical nuclear infrastructure assets is becoming a vital national concern. The possibility of terrorist attacks on the critical nuclear infrastructure assets is especially problematic in the post 11/9 world [14-17].

The vulnerability assessment methodology and new solution methods can help the overall national energy sector to identify and understand the terrorist threats to critical infrastructure and its vulnerabilities. Moreover, the VA methodology could help national regulators (administrative bodies) and agencies to develop and implement a vulnerability awareness and education programs for their critical assets to enhance the security and safe operation of the whole energy infrastructure. The new VA solutions can also help nuclear energy utility companies (NPPs) to develop, validate, and disseminate the assessment and survey of new efficient countermeasures.

The regulatory bodies have to facilitate the development of new methodologies and strategies with associated tools to assist in the implementation, to provide the training and technical assistance and to stimulate regulatory actions to mitigate significant problems.

3 THE NEW TERRORISM RISK AND VULNERABILITY ASSESSMENT NPP MODELS

3.1 The introduction to the new terrorism risk and vulnerability assessment NPP models

To effectively cope with new threats it is necessary to develop strategy for a risk management as an integrated process for assessing possible terrorist risk scenarios. Because of possible targets dispersion world-wide and potentially very high national losses, we need proper prioritization and allocation of limited resources. It could be achieved by the new comparative risk assessment model and by prioritizing countermeasures and preventive actions and by timely and an efficient response in the case of attacks.
In the article we in short present the first stage of developing new methods and adapted methodology. This unique methodology contains all needed (counter)measures required to reduce risk and mitigate the severity of consequences.

3.2 The new vulnerability assessment conception

Probability of terrorist attacks can be defined as the probability of occurrence of severe and harmful consequences in a defined time frame. In the process of the procedure development we have presumed new understanding of probability of terrorist attacks on critical nuclear objects. We have supposed that probability is not constant but rather it will change with time, depending on circumstances and on our preparedness and countermeasures. Thus, we assumed the risk (vulnerability) assessment model as a dynamic process where threats, trigger events and information are changing with time, as our countermeasures also do.

3.3 Developing threat analysis scenarios

The selection of the trigger event (TE) is important an initial step for determining the proper threats analysis scenario. The establishment of accurate threat analysis scenario is the most important step in the successful vulnerability (risk) assessment. Actually TE can be defined as an initial event in the scenario that has high potential to produce harmful (adverse) consequences. Some examples of a trigger event could be: the aircraft crash in the NPP containment, the missile attack on NPP spent fuel pool, the internal bombing in the NPP control room, etc.

The most important term in understanding the terrorist threats is a comprehensive overview of credible terrorist scenarios. For developing this special type of analyses we have defined the scenario as a set of unexpected but credible and connected adverse time events.

3.4 Interactive trigger events

On the base of the qualitative estimation we supposed that the most dangerous scenario for the threat analysis on critical nuclear objects (asset) will result from interactive trigger events (ITE). It means that two or more synchronic trigger terrorist events interact and result in unexpected disastrous consequences.

In the VA model we have imagined the time frame of the threat analysis scenario as the course of connected events on the time (x-axis) scale in form of the cause-outcome chain: trigger (threshold) event → planning → preparation → action (destroying effect) → resulting damage → feedback (lessons learned from “operating” experience) leading to harmful consequences on the y-axis.

In this process not only our critical asset but the terrorist’s organizations are fortunately also vulnerable. As a result of the qualitative model estimation the weakest points in terrorists scenarios could be preparatory and before the attack phases. We will check the result on the base of the computer model scenario based threat analysis.

3.5 The difference between definition of the risk and the hazard

Another a new important point at developing the VA model is that we must differ between definition of the risk and the hazard in the case of the threat analysis on the nuclear critical asset. Sometimes in classical analyses of a risk there is equalization of those terms. By our opinion in the case of terrorist threats (attacks) on NPPs there must be a reasonable difference [10].
We can define the hazard of the terrorist attack on a NPP as the potential of occurrence of harmful consequences. In the process of developing the new VA model and method we have proposed a new definition of a risk at threat analysis on the critical nuclear asset as the combination of a probability of the terrorist attack and a vulnerability of the nuclear asset (object) [10,14,15].

3.6 The new vulnerability assessment model for nuclear power plants

In general, the vulnerability of the critical nuclear asset can be defined as a probability of the (predicted) terrorist attack times a probability of a failure of a critical asset protection or an effectiveness of protection systems. The more specific, the vulnerability of the critical nuclear system or component can be defined as a probability of the (predicted) terrorist attack times a probability of a critical component (C) failure if an attack occurred and a protection fails. At nuclear power plant it could be a probability of a failure of the containment as the last and most robust defence system.

3.7 The new nuclear power plant mathematical model for the threat analysis and the risk evaluation

This quite new mathematical definition for the risk evaluation at threat analysis to the critical nuclear asset can enable the better understanding of whole process.

We have defined the quite new mathematical equation for the risk (R) calculation as a probability estimation of terrorist attacks on a nuclear power plant:

\[ R = PUC \times VA \]  

(1)

The term PUC is defined as a probability of occurrence of harmful (undesired) consequences of the terrorist attack on a nuclear power plant.

The new term, the nuclear power plant vulnerability assessment (VA) is defined as:

\[ VA = A(P)AF \times PCF \]  

(2)

In the new mathematical model we supposed the term A(P)AF as the assumed (predicted) trigger event frequency. It can be estimated from the statistical analyses of NPPs operating experiences data or could be assumed on the basis of the personal expertise of analyst.

So, in the new risk model we have assumed the risk of the terrorist attack on a NPP as:

\[ R = A(P)AF \times PCF \times PUC \]  

(3)

Because consequences of the terrorist attack on operating facilities could be more adverse than on the decommissioned or temporarily shutdown, we could further assess the risk of the terrorist attack on the nuclear power plant during operation:

\[ R = A(P)AF \times PCF \times PUC \times OF \]  

(4)
For a NPP vulnerability assessment of the terrorist attack we supposed a probability of the containment failure (PCF). In this way the vulnerability is presented as the joint probability distribution for each asset-threat combination.

The OF can be assumed as the overall world-wide nuclear facilities operation factor. Only for NPPs the OF conservative value could be assumed as 0,95, that means that from all world’s nuclear plants at time of assumed attack (threat) operate 95% or about 400 power plants. Clearly, there are not included decommissioned and closed NPPs and large number of research reactors and nuclear waste facilities. All of them, together with aviation and petroleum sectors, are possibly highest priority terrorist targets.

3.8 The new perceived and estimated risk definition

For the sake of new model development we defined another useful risk definition [10]. It is a very important for the timely and accurate risk estimation of the terrorist attack on critical infrastructure objects, to distinguish between the perceived and estimated risk. The perceived risk of the terrorist attack on a NPP at the time of an assessment considering available information or the perceived probability of the terrorist attack on a NPP based on circumstances (political, etc.) and on intelligence information could be the degree of belief of the decision-makers that the terrorist attack will occur. This subjective (politicians, analysts) risk assessment could change (improve) with time as information gathering through new data and the experience feedback. In this manner the perceived risk converge to the estimated risk that is known (its probability distribution) and it does not change with time.

This recognition has two important implications for the risk assessment of the terrorist attack on NPPs:

1. Even with very little or incomplete information the good analysts and risk management organizations can produce subjective but valid and valuable probability estimates for regulatory and political decision makers to timely decide on this terrorist risk (threat), and

2. Because of clear difference between subjective and objective risk assessments of the terrorist attack on critical infrastructure objects, there is always a chance of the hindsight.

The key step in the timely and good defence strategy and the safe and secure a NPP operation is the credible vulnerability assessment to minimize this hindsight.

4 THE ASSESSING CREDIBLE TERRORIST THREATS ON NPPs AND THEIR ADVERSE CONSEQUENCES

In the model we have imagined the threat analysis as an integrated system of methods for ranking possibility of the terrorist attack on the specific critical infrastructure objects (targets), especially on NPPs.

For our vulnerability assessment model we could assume some credible and important terrorist threats on NPPs as:

- The suicidal attack with fully fuelled civilian or even military aircraft on a NPP (plant containment, plant spent fuel pool or plant control room).
- The intentional fully fuelled and loaded with explosives small airplanes crash on a NPP (plant containment, plant spent fuel pool or plant control room).
- The intentional attack with remote-controlled fully fuelled and loaded with explosives small airplanes on a NPP (plant containment, plant spent fuel pool or plant control room).
- The intentional attack with rocket missiles.
- The internal attack with hostage taking of key operational personnel.
4.1 The definition of the possible consequences of terrorist attack on a NPP

The very important step at integrated risk assessment is accurate understanding of consequences. In general we can define consequences as undesired and harmful effects of the terrorist attack, sabotage or natural catastrophe on a NPP. Because in the model we have supposed the time dependence of risk (vulnerability) assessment, we have also to consider all credible short and long term consequences effects.

Possible undesired consequences of the terrorist attack or sabotage (internal/external) on a NPP may be:

- The large plant and equipment damage.
- The large personnel harm.
- The large environmental impact, people injury and psychological effects.
- The large material and economic damage (loss of operation, etc.).
- The large national and international security and progress influence, and a very important long term consequence of
- The large turmoil and alteration of accepted psychological life’s matrices.

The degree of adverse consequences depends on amount of an uncontrolled radioactive release into an environment.

In our risk assessment model we have supposed that a probability of an uncontrolled radioactive release into an environment depends on:

- The mode of terrorist attack.
- The design and construction of the attacked plant.
- The operation mode of the plant at time of attack.
- The environmental conditions at time of attack.

5 THE CREDIBLE KEY COUNTERMEASURES

The important averting factor of the terrorist attack on nuclear power plants could be in advance prepared and tested an intelligible structure of protective measures.

By gathering new knowledge and better comprehension of a new VA methodology, we could propose some effective countermeasures:

- The timely intelligence analyses and assessments of available information.
- The good worldwide cooperation and exchange of information about threats and risk assessments with other world’s or national organizations.
- The adequate decision-makers coordinate patience.
- The persistence in prevention efforts and practiced response on all kind of threats.
- The robust and inventive asset protection.
- The international treaty requiring the governments specific protection against the terrorist attack on NPPs.
- The strengthening specific national regulatory requirements for the nuclear facilities secure and safe operation, and especially important
- The persistent consultations between politicians, nuclear regulators, scientists, military, intelligence and police experts.

6 CONCLUSIONS

On the basis of the deeper understanding of the new VA strategy and developed methods for the assessment of the threat analysis on NPPs, we could recommend some key protective measures influencing the magnitude of harmfulness:
1. The intelligent and timely prepared and tested preventive actions to reduce the probability of occurrence of the terrorist attack on a nuclear power plant.
2. The planned, prepared and verified strong response actions to mitigate adverse consequences of the terrorist attack on a nuclear power plant.

On the base of the qualitative estimation and our expert experience the one unusual but very efficient inherent protective measure preserves NPPs from the large-scale devastative terrorist attack and it is the fact that the terrorist attack on the one NPP will badly affect the safe, secure and economic operation of all NPPs world-wide.

Some of our presented work will be the part of several new procedures and it could be implemented in our emergency preparedness plan [12].

On the base of the new knowledge gathered by developing the new model, methodology, methods and scenarios analysis, we can expect that:

- The credible terrorist attack on the nuclear power plant should be and can be prevented, but
- The unexpected (incredible) terrorist attack scenario that will result in the large and irreversible plant damage and disaster should be expected. Therefore all efforts should be done to forecast and conceive all kinds of “unexpected” attacks in advance.

REFERENCES


