International Journal of Economics, Commerce and Management
United Kingdom Vol. VI, Issue 11, November 2018
http://ijecm.co.uk/ ISSN 2348 0386

RISK ANALYSIS FOR BUSINESS CONTINUITY MANAGEMENT OF NPP

Kiril Stoichev
"HI-TECH IMS" LTD., Sofia, Bulgaria
kstoichev@ims.bas.bg

Abstract
Risk Analysis is an activity that is fundamental to providing critical infrastructure security. The analysis is widely used in nuclear energy. The purpose of this article is to demonstrate the empathy of Risk Analysis to the Business Continuity Management System. A risk analysis of a specific nuclear power plant in Bulgaria has been carried out. For the purpose of the analysis is examined the effect on NPP of the Maximum Water Levels of the water sources and their potential effect on the adjoining area. Risk Analysis is performed on a real object of critical infrastructure and is combined with the techniques of Business Continued Management. As main goal of that manuscript is the performance of the results of these two techniques used for assessment of the risks connected with the continuity of NPP activities.

Keywords: Risk Analysis, Business Continuity Management, Risk Levels, Risk Level Reduction

INTRODUCTION

Nuclear security is not a new matter for those working in the field of nuclear energy, but compared to nuclear safety is a very young science, structuring and development of which is on the rise in recent years. In the field of training of specialists in this area leading are the publications of International Atomic Energy Agency - IAEA Nuclear Security Series. In it there are considered in exceptional detail almost all aspects of nuclear security and its organizational and technical aspects.

In the recent years, in life and business practices enters Business Continuity Management (BCM), including the activities of the management of nuclear safety in nuclear power plants (in Bulgaria we introduced this practice in 2011, leading European Project

Licensed under Creative Common

HOME/2010/CIPS/AG/019). Specific issues BCM considered one way or another, in one form or another form and content are known for the specialists and many of them are enshrined in the IAEA Nuclear Security Series. The main difference between them and the professionals applying BCM is the emphasis on the latter detail and targeted efforts to systematize the synergies of achieving the intended results.

BCM worldwide is an area of business practice with a long tradition of formal elements and requirements in international standards and a number of national regulatory documents with internationally recognized institutions and a network of means of disseminating best practices, many of which are an integral part of these requirements in the process of updating the standards and normative requirements against which individual companies organize and carry out their activities and achieve planned business objectives.

BCM is a subsystem of Business Management System (BMS) and interacts with all other subsystems of BMS. The latter entirely applies to the management systems of nuclear power plants (NPP). The improvement of any subsystem of BMS improves the overall management of the organization. In this case, the improvement relates to security of NPP and from there to the continuity of the activities as a whole.

Considering the above, in this article we will bring to the attention of the readers practical methodology applied to build Business Continuity Management System (BCMS), which I developed in the course of implementation of the aforementioned European project. Model system was developed for the System for removing the heat and its transforming into kinetic power of the steam turbine rotation of NPP with steam generator of reactors WWER - PWR type. The aim was to develop such system model for one of the elements of the control system of the NPP, which is approximated to the entire control system of the nuclear power plant and to improve its security. This plant uses steam generator of reactors WWER - PWR type, which are installed in European Union countries such as Bulgaria, the Czech Republic, Slovakia, Hungary and Finland. The considered methodology can be used not only for this type of nuclear power plants, but for all who use nuclear power to generate electricity.

BCMS has a lot of elements the main of which are Risk Analysis, Policy and Strategy for BCM. In that article we will highlight the first and founding element -Risk Analysis of BCMS for Bulgarian NPP.

ANALYSIS OF THE PROBABILITY OF THE POTENTIAL TERRORIST ATTACK EFFECT ON SYSTEM CONTINUOUS FUNCTION (RISK ANALYSIS)

The analysis of terrorist attack risk should consider their goals as well as the methods and manners of their achievement. In compliance with the Frame Resolution of Council of Europe

Licensed under Creative Common

concerning counteraction against terrorism (2002/475/JHA), the goals of the terrorist attacks include spreading fear among the population, forcing the governments to act or suspend acting in certain way or to seriously destabilize or destroy fundamental political, constitutional, economic or social structures of individual states or international organizations.

Causing great damages on important production powers resulting in serious economic losses is one of the methods to achieve such goals. Because of this reason it is advisable for NPP (particularly concerning the System for removing the heat and its transforming into kinetic power of the steam turbine rotation of NPP – named in the followed rows as "System") to make analysis and assessment of the risk about the probability of potential terrorist act effect on the continuous operation of the System/plant and the results to be recorded in the adequate set of documents for its (and analogical to it) activity/ies.

The System considered is of key importance for the NPP operation. The eventual, sufficiently long interruption of its functioning would cause interruption of reactors (5 and 6) operation for a long period of time. In individual cases, as a result most of all of operator's mistakes in sophisticated situation created as a result of effective terrorist impacts on the System it is possible to provoke accidents of dramatic transboundary consequences. Therefore, the System may be considered as a preferred objective of terrorist violation because of which it is an object of the present risk assessment.

METHODOLOGY

The main purpose of the present risk assessment is to ensure System continuous function (as part of the total plant operation process), in order to guarantee continuity of the business processes in NPP. In this direction, at international level, there are developed and applied several standards, in the same time the matter being considered comparatively new. From the view point of the gap in the field of Business Continuity Management the Great Britain standard BS 25999 appears as basis. On its basis, by reference and enrichment of the content for the purposes of the organizations and regional needs, many international and national standardization documents are developed such as:

- NFPA 1600 – document of the USA National Fire Control Association, considering the conditions/medium of perspective access rejection;
- ISO 17799 – standard for information security management systems which manage and minimize the threats for the information;
- ISO 22399 – instructions for actions in case of accidents and continuity operative management;

Licensed under Creative Common

- AS/NZS 4360:2004 – standard issued by Australia and New Zealand providing instructions about risk management;
- SPRING TR 19 – Singapore technical reference to BCM that in its base considers the engineering aspects of the systems;
- The King II report of Corporate Governance –instructions in South Africa for risk management considering BCM from the view point of management prospect.

The International Standardization Organization (ISO), develops the subject of activity of BS 25999, as a result of that on May 16, 2012, ISO 22301:2012, “Societal security - Business continuity management systems - Requirements” has been published and enforced.ISO 22301 emphasized the importance of:

- The understanding of the organization needs and the necessity to create policy for business continuity and goals management;
- Implementation and application of control mechanism and measures for guidance of the organization general ability to manage accidents interrupting its business;
- Permanent control and review of the BCM fulfillment and efficiency;
- Permanent improvement on the basis of objective measurements.

On the grounds of the above said it is necessary NPP to demonstrate correct application of the BCM process by developing and putting in operation BCM System of the System for heat removal and its transforming into kinetic energy of the steam generator (not only). In the most general lines this consists of :

- Business impact analysis (BIA): Identification of the critical processes related to key products and services, the interdependences between the processes and resources required for the organization functioning;
- Risk assessment: ISO 22301 suggests reference to standards ISO 31000/ISO 31010, for applying this process. The aim is a formally documented risk assessment process to be established, applied and maintained which systematically to identify, analyze and assess the risk of destructive accidents impact on the organization;
- Strategy of operation continuation: After implementation of the requirements, by BIA and risk assessment, the strategies could be developed in order to identify the measures that will allow the organization to protect and restore its critical functions, which is based on the organization stability towards the risk in the frames of the defined time for restoring the objects;

Licensed under Creative Common

- Procedures of operation continuity: Documenting of procedures (including required agreements), in order to guarantee business continuity and management in case of destructive accident impact;
- Training and control: In order to ensure compliance of the procedures with the goals of the organization they should be periodically inspected. The training and control are the processes of confirming the plans and procedures of operation continuity.

In the interest of methodology, for carrying out the Analysis of impact probability of potential terrorist attacks on the system continuous operation, the ISO 31010 standard is used. In accordance with its recommendatory requirements the risk assessment should include (Fig. 1):

- dentification of the risks as a result of terrorist acts;
- Analysis of these risks both from the view point of their potential to cause prolonged interruption of the production process and from the view point of the probability of their realization and determination of their level;
- Comparative assessment of risk level.

SYSTEM RISKS IDENTIFICATION

In the most general and complex case the business processes continuity of NPP and the System considered in particular could be subjected to the effect of the following threats - Fig. 2 (ECP-601).

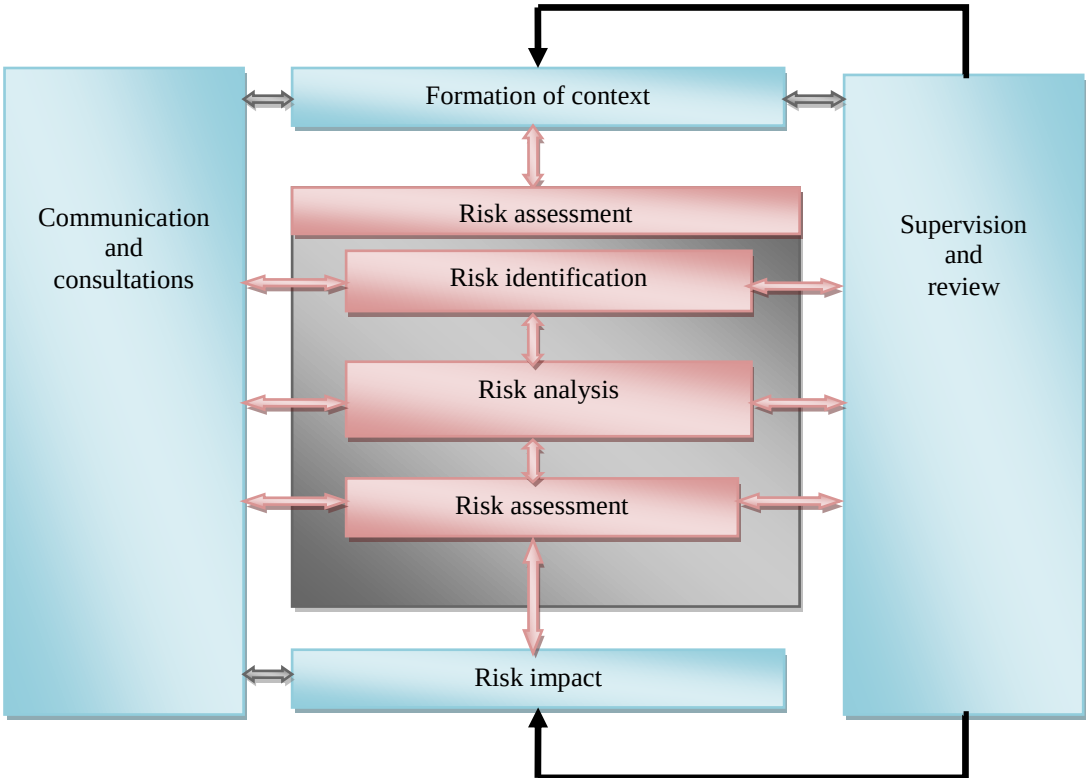

Figure 1 Place of risk assessment process in the risk management

Licensed under Creative Common

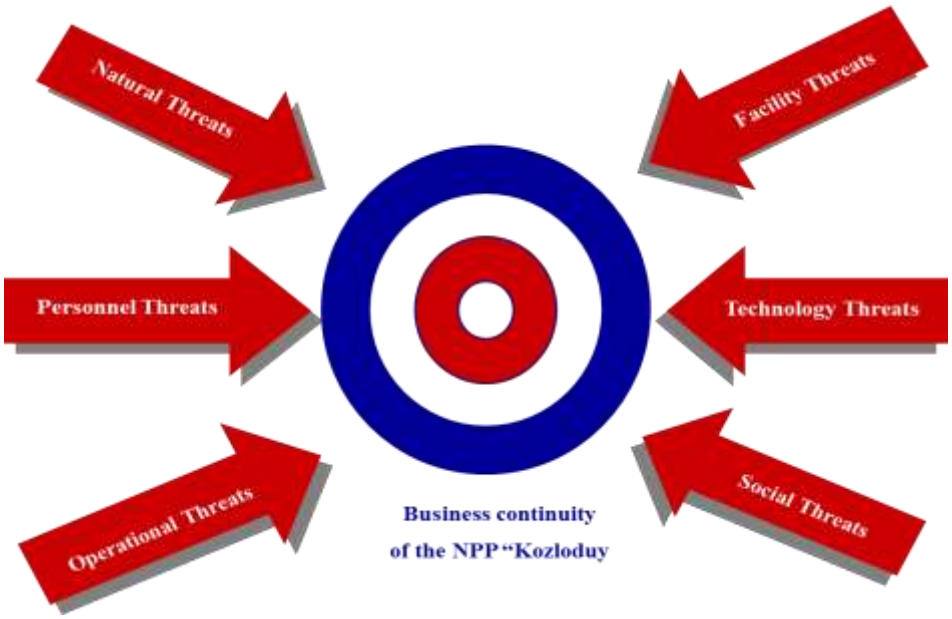

Figure 2 Threat against business continuity

The types of threats contain in them a group of events (Table 1) that may cause transition of the business processes in emergency mode or interruption (ECP-601).

Table 1 Type of threats and their content

Types of threats/content	**Types of threats/content**	**Types of threats/content**
Natural threats	Threats against machines, installations and buildings	Threats against the staff
• Floodings; • Tornado; • Hurricanes; • Earth quakes; • Snow storms; • Ice storms; • Devastating fires.	• Fire; • Explosion ; • Loss of power supply; • Loss of water supply installation; • Loss of access; • Failure of machines and installations.	• Strikes; • Epidemic; • Risk materials; • Transportation problems; • Loss of key personnel.
Threats against technologies	Threats against operations	Social threats
• Viruses; • External penetration in computer networks; • Data loss; • Hardware failure; • Software failure ; • Network failure; • Telephone system failure.	• Financial crises; • Loss of key suppliers; • Failure of equipment; • Normative issues; • Bad public image; • Lack of due diligence assessment.	• Revolts/turbulences; • Protests; • Sabotages; • Vandalism; • Bomb threats; • Defilement of work place; • Terrorism.

Licensed under Creative Common

In this connection it is necessary to make an assessment of operations interruption potential from the view pint of:

- Loss of machines, installations or buildings;
- Loss of computer systems;
- Data loss;
- Loss of communications;
- Loss of key personnel, and etc.

Loss of machines, installations or buildings

It is possible machines, installations and buildings of the System considered to be damaged/destroyed as a result of caused floods and fires by probable terrorist action. Because of this reason the potential of loss is considered as probable threat.

Loss of computer systems

The structure built of computer information systems and engineering facilities maintenance forms Control equipment and Automatics and ensures reliable operation of the information system in NPP. This system is of extreme importance for the continuous operation of the plant/reactors. It is not analyzed and assessed because:

- The electric power supply is four times backed-up – main, auxiliary, emergency and by alternative sources, (redundant diesel generators and mobile diesel generator). From this point of view it is in practice uninterruptible provided operability of the Control equipment and Automatics is ensured;
- The thickness of the reinforced concrete reactor vessel guarantees 100 % protection against electromagnetic weapon attack;
- The level of the reactors physical protection, by consecutively embedded circles-levels of physical access, guarantees 100 % protection against physical penetration in the protected zone with the purpose to infiltrate computer virus;
- The system has no access to external information systems, which guarantees impossibility for computer virus infiltration in it from outside source;
- The system is backed up, by „duplicate control hall“, on the base of the principles of physical separation and independence.

Licensed under Creative Common

Data loss

Data formation and storage is a process which is backed up and does not give rise to threat of interrupting NPP function on the base of the conclusions concerning loss of computer systems.
In the same time, NPP operation is controlled by Main Control Room (MCR – on altitude mark 6.60) by means of Computer information-control system OVATION developed by WESTINGHOUSE, US, which controls the safety systems, reactor control system, electronic control system, generator control system, turbine hall, etc. The system base is “SUN” servers, operational system SOLARIS 2.6, data base ORACLE and CISCO network equipment. It scans 80 000 signals per second; the controlled data and information are stored in two “history” servers located on altitude mark “0” in units 5 and 6 where every day in 00.00 hour backup records are made on optical disks for long time storage. Every month complete duplicate copying of the system is made and the information is stored for long term in specialized premises of restricted access.

Main OVATION constructive components are the controllers, comparatively independent (they could function fully autonomously in case of computer system breakdown), basic and duplicate, with double back up power supply, which process the current information from the sensors and systems.

Global time system is introduced for improvement of the accuracy and reliability of the computer systems by satellite system with timeserver (main and duplicate).

Independent system for critical parameters control which processes the signals from 200 independent sensors in the leak tight zone is also located in MCR. The information is sent in real time to the Accident Management Center and Nuclear Regulatory Agency where it is kept within 8 hours.

The safety parameters indication system analyzes up to 3000 signals per second from the main data flow and sends the results in real time to the Accident Management Center and Nuclear Regulatory Agency.

Loss of communications

The main communication facilities available in NPP are as follows – this information belongs to the NPP. The built and deployed announcement facilities and communication facilities – for information, telephone and radio interchange and loud-speaker installations, guarantee notification of the personnel, management bodies and population. The information flows are backed up because of the impact on them and therefore they do not present potential danger for plant operation interruption.

Licensed under Creative Common

Loss of key personnel

The system of key personnel training is repeatedly backed up by training of deputies. It should be noted that the training will be presented in further document as part of the BCM planning process.

For the purposes of working out the details of Probability analysis of potential terrorist acts impact on the system continuous operation, the probability of terrorist threat is considered as possible event that could provoke floods and fires in the System components and to lead to disturbance of the NPP business processes continuity.

IDENTIFICATION OF THE RISKS FOR THE SYSTEM AS A RESULT OF TERRORIST ACTS

The terrorist acts could be performed either through overt actions or through secret penetration and causing direct damages to machines and equipment or leaving devices which can be activated later remotely. As for prevention of secret penetration in NPP there are applied sufficiently large-scale measures of physical protection, the probability of using this method of terrorist actions is minimum and it will not be subject of the present study.

Overt terrorist actions would have limited chance to succeed and would cause minimum effect if they are directed to damaging separate installation, machine or equipment. It is more probable the terrorists to aim at large scale effect, the counteraction to which is difficult and would result in decommission of considerable part of the installations, machines and equipment. Such effect would cause both prolonged interruption of the System function and spending considerable finances and materials to restore the function – both of the System and of the rest of affected components in the plant. It is even possible to reach a situation in which recovery of NPP operation will be found inexpedient.

In case of planned penetration with the purpose to affect the system, a technically well-informed enemy will aim at destroying critical/vitally important and important/very necessary functions of it, by disabling equipment of easy access and that would cause long-term reactors shut-down and sizable material and financial losses.

Most probably the terrorist acts would be committed by penetration of one or more groups of terrorists, well-armed, prepared and equipped with suitable munitions and auxiliary means, acquainted in advance with the NPP structure and the type, number and approximate location of the System critical/vitally important and important/very necessary equipment.

The methods of penetration in the NPP area could be:

- Penetration to the object on foot;
- Penetration to the object by vehicle;
- By parachute;

Licensed under Creative Common

- Custom-made flying machines power glider/hang glider;
- Contamination of the cold channel water or affecting by the waters of Danube River or water sources near NPP.

The results of such large-scale impacts on the System would cause fire or flooding, therefore these risks are defined as subject of the present study.

FLOODING AND FIRE RISK ANALYSIS

Flooding risk analysis

Floods that may affect the NPP function could be divided into internal and external.

Internal flooding risk analysis

Taking into account the contribution of the internal flooding risk proves to be an important stage of SPA from the view point of its completeness and comprehensiveness (European „stress-tests“ of nuclear plants. National report of Bulgaria–December, 2011), as it is found that not a small part of the emergency event cases are due to internal flooding.

As flooding it is defined every event connected with steaming, spilling, overflowing, splashing or pouring out of fluid (water, steam, oil and various reagents used to maintain water - chemical regime of the first and second loop) from broken pipeline (steam pipeline) or other equipment (European „stress-tests“ of nuclear plants. National report of Bulgaria–December, 2011). The effect of broken vessels of non-condensable gases (hydrogen, nitrogen, etc.) is not examined as this does not cause failure of technological equipment in the context of the term “flooding”.

Splashing affects the equipment directly. Spilling affects the equipment by water accumulation. Pouring out is overflow of water through wells, staircase cells, lifts or other technological holes (holes for pipelines routing, non-hermetical penetrations, no gasket spots of unsealed doors, etc.). The moisture effects due to released hot water and steam are considered in the conventional manner in the frames of the flooding analysis.

The internal flooding risk analysis considers the effect on the System equipment located in the turbine hall (TH) because in compliance with expert assessment it is assumed that the impact on the remaining System components is negligible. The identified flooding scenarios are grouped by certain initial events (European “stress-tests” of nuclear plants. National report of Bulgaria–December, 2011, Table 5-35, p. 242÷244 – Annex 1)–turbine stop; stop of one main feed water pump; loss of both turbine feed pumps; loss of main centrifugal pump cooling; loss of circulating water system leading to vacuum breakdown; non-operability of four fast-acting

Licensed under Creative Common

reducing valves and not at last place TH failure. For the most part these events could cause damages or emergency decommissioning of the electrical equipment.

In determination of the frequencies of flooding occurrence the following factors are taken into account:

- Outflow from pipelines or breaking of them;
- Leakages from parts (cracks in the housing, shaft gaskets, rods, collapse, etc.).

During the examination of the possible impacts on the System equipment it was found that the terrorists could not provoke internal flooding resulting in simultaneous failure of all possible channels for cooler feeding and removal or damages of the electrical equipment leading to reactors emergency shut-down. After elimination of the terrorists, the operative staff will be able to prevent further progress of the emergency process and limit the consequences of it.

Taking into account the results obtained from SPA and on the basis of the above expert assessment the risk for the System ensuing from internal flooding caused by terrorists is defined as low.

External flooding risk analysis

The sources of eventual external flooding are the maximum possible natural water levels of Danube river, collapse of the walls of hydro system “Zhelezni vrata”’, accident of reservoir “Shishmanov val”, slope waters from the area “Marishkin dol”, waters from feeder valley “Marichin valog” and continued pouring rains on the plant site. For the purpose of the analysis is examined the effect on NPP of the Maximum Water Levels (MWL) of the above said sources and their potential effect on the adjoining area as follows:

- Determination of MWL as a result of Danube river level rise.

In actualized technical substantiation of safety MWL are confirmed in natural conditions according to Table 2.

Table 2 Probability of reaching MWL.

Probability of reaching	1%	0,1%	0,01%
Water level	30,58 m	31,47 m	32,23 m

Also, MWL at NPP, when catastrophic wave occurs, initiated by collapse of hydro systems “Zhelezni vrata”, is 32,53 m., and this is established 28 hours and 20 minutes after the supposed collapse of hydro system “Zhelezni vrata 1” and will continue about 2 hours.

Licensed under Creative Common

In all postulated cases connected with extreme rise of Danube river level, the MWL altitude mark in case of inundation is below altitude mark 0,00 on the site, this confirms the determination of the plant site as „NON INUNDATABLE".

- Determination of MWL as a result of broken wall of reservoir “Shishmanov val”, waters from feeder valley “Marichin valog”, slope waters from the area “Marishkin dol” and continued pouring rains on the plant site.

The studies carried out as well as the performed activities for securing the site during recent years show that MWL from these sources could not cause interruption of NPP operation. Only, as result of collapse of the wall of reservoir “Shishmanov val”, it is possible for a short time the Well pump stations (WPS) to be out of service.

- Determination of potential impacts of MWL on the adjoining facilities in the lowland.

The lowland is separated by hydro technical channels of NPP in three zones. The most west zone is delimited in east by warm channel-2, in south by NPP “Kozloduy” and in west reaches and enters Kozloduy town. The Middle one is delimited by warm channel-2, NPP and the double channel. The east zone is delimited by the double channel and the bed of Ogosta River.

The following text considers the potential effects of flooding the three different zones (separately) with the purpose to show all indirect effects on the plant operation:

= Potential effects of flooding the lowland as a result of broken embankment in the zone between warm channel-2 and CoPS;

In case of collapse of the state embankment first there will be inundated and impeded WPS (as sources of additional water for the spray cooling ponds of units 5 and 6), located in immediate neighborhood of the state embankment heel. The access to CoPS by land most probably will be cut. That will happen in the first hours after the collapse of the state embankment because the draining channels and roads to CoPS are at low altitude mark and will be quickly inundated. During lowland inundation and its filling up to altitude mark 32.00 it can be also expected destruction of part of the poles of the electric transmission network got in the way of the tide wave.

The emergency pipelines from the emergency pump station of CoPS to the emergency volume are made of steel and laid in ditch but when crossing the draining channels they are open and pass over them. These open sections are vulnerable and could be damaged by the tide wave.

In the lowland formed by warm channel-2, cold channel-1 and Danube embankment all sewer waters pour, coming from the site of units 1 through 4 and from reactor compartment, diesel generator stations and Turbine hall on the site of units 5 and 6. The remaining part of the sewerage on the site of units 5 and 6 will be also blocked. That may create conditions for the water to return through the sewer collectors for fecal and rainwater sewerage passing along

Licensed under Creative Common

spray cooling ponds and fill up to the altitude mark of lowland inundation. It is possible the sewer wells on the site to be full of water to attitude mark 32, 93 m. The available purification plant for fecal waters on the site of units 5 and 6 does not hinder water penetration through the residential-fecal sewerage system as it is possible the water to pass through the well which is used as overflow drain when the capacity of the purification plant is exceeded.

= Potential effects in case of inundation of the lowland if the embankment breaks in the area between Kozloduy town and warm channel -2;

In case of inundation of the lowland of this area the final result will be that only a part of the poles will take on the initial shock of the tide wave because the rest of them are protected by warm channel -2.

= Potential effects in case of inundation of the lowland if the embankment breaks in the area between CoPS and Ogosta River.

In case of inundation of the lowland of this area, most of all electric transmission networks Harletz, Neutron and Danube will be affected. There are no other facilities in the area that have relation to NPP “Kozloduy” operation except for the open storehouses. Under certain conditions of the initial tide wave formation the embankment of warm channel-1 could erode and collapse. In pouring of water to the zone of the lowland between the double channel and warm channel-2 could occur only through the draining reinforced concrete pipelines passing under the double channel.

On the basis of the above said, the more important weak places for inundation of NPP by MWL = 32, 93 m could be defined as follows:

- suspension of electric power production and switching over to source of power supply by the diesel generators –as a result of possible dropping out of part of the mains connecting NPP;
- suspension of water feeding to cold channel due to loss of CoPS and no access to it by land;
- loss of emergency refill of spray cooling ponds of units 5 and 6 due to dropping out of WPS;
- flooding a part of the underground communications below altitude mark 32,93 m–drainage in the rain sewerage and incompactness of the channels in which they are placed;
- loss of the backup system (alternative) for spent nuclear fuel cooling through the steam generators when the fuel is placed in the reactor –dropping out of the pumps for steam generators emergency feeding auxiliary system.

In the examination of the sources of eventual external floodings and their potential effect on the System, it was found that the terrorists could not be able to cause simultaneous discontinuance of critical/vitally important and important/very necessary functions of it, which will lead to emergency reactors shut down (but it is possible that they are shut down because of damages in mains poles which is not the subject of the present risk assessment as the poles are not

Licensed under Creative Common

components of the System). After elimination of the terrorists the operative personnel will be able to prevent further progress of the accident process and limit the consequences of it.
Taking into account the results obtained in the Report of Bulgaria from the carried out stress tests of NPP and on the basis of the above expert assessment the risk for the System as a result of external floodings caused by terrorists is determined as low.

Fire risk analysis

Approach of risk analysis

According to experimental assessment, it is determined that causing external fires has no potential to damage considerably the System and to affect materially its operation because of which this risk is assumed negligible and is not considered. The internal fire risk for the System is determined depending on:

- The terrorists possibilities to penetrate in fire cells of critical/vitally important and important/very necessary System components that are potentially highly inflammable;
- The terrorists possibilities to cause fires of high intensity that could not be put under control and extinguished in the frames of technologically safe for the System period of time;
- The possible effects on the System operation in case of fires covering critical/vitally important and important/very necessary System components.

In the studies it is assumed that for each fire cell the fire caused in it leads to loss of power supply to the respective components of the automated fire extinguishing system.

Potential objects of terrorist act with the purpose to cause fire

In selecting objects of action with the purpose to cause fire the terrorists most probably will direct to:

- Highly inflammable System components/equipment such as pumps, electric engines, transformers, cable networks, panels, cabinets, as well as cooling oil tanks whose decommissioning or destruction would lead to loss of critical/vitally important and important/very necessary functions;
- Other System components/equipment that are located in immediate neighborhood to the components/equipment under the above item or along the route to reaching these components/equipment as a result of which to achieve also additional effect connected with fire escalation;

Licensed under Creative Common

- Highly inflammable materials with the purpose to achieve additional effect as a result of fire escalation.

Assessment of the terrorists' possibilities to cause fire in fire cells of critical/vitally important and important/very necessary System components.

It could be affirmed at high degree of probability that in order to achieve their goals the terrorists will direct to penetration in CoPS, CPS 3 and 4, TH of unit 5 and TH of unit 6 and fire cells of components/equipment, potential object of act.

If with the purpose to avoid underestimation of internal fire risk, in the risk analysis we adopt conservative approach and assume the terrorists would succeed to penetrate in CoPS, CPS 3 and 4, TH of unit 5 and TH of unit 6 and would reach to fire cells of critical/vitally important and important/very necessary equipment (European 'stress-tests' of nuclear plants. National report of Bulgaria–December, 2011, Table 5-14, p. 157÷158 – Annex 2), then they would be able to cause fires of high intensity in them (i.e., self-sustained fires which could lead to ignition of components or materials out of the fire source boundaries and which could not be controlled and extinguished in the frames of technologically safe for the System period of time), affecting and bringing out of order the selected components/equipment for potential impact.

Determination of fire risk level

In the general case, the fire as risk is function of the probability such terrorist threat to occur (in this case), exposure to the danger and vulnerability (SEC (2010) 1626 final), i.e.

R = f (ExVxP),

Where, R (Risk) is risk,

E (Exposure) exposure to the danger and

V (Vulnerability) is vulnerability.

At the assumptions made (the possible penetration methods) and in case that the terrorists succeed to penetrate to the selected object of action, the exposure to danger (expressed by the possibilities of the terrorists to access highly inflammable critical/vitally important and important/very necessary System components) and vulnerability (the possibility of the terrorists to cause high intensity fire in the fire cells of critical/vitally important and important/very necessary System components) would be high.

Therefore, in the application of conservative approach for the risk analysis the risk for the System, as a result of terrorist acts causing internal fire would be high and the consequences of such actions most probably would lead to suspension of the System operation for a time period longer than the technologically admissible one for the reactors safe function.

Licensed under Creative Common

Objectively seen, such fires have the potential to cause emergency shutdown of the nuclear reactors for considerable period of time (in some cases even exceeding 6 months), which will give rise to considerable financial and material losses for NPP related to interruption of the electric power production and repair or replacement of System components/equipment as well as to recovery of damaged buildings and other facilities.

COMPARATIVE ASSESSMENT OF RISK LEVEL

Comparative assessment of flooding risk level

The external flooding risk analysis made shows that terrorists could temporarily bring out of order separate System components/equipment whose functions will be assumed by auxiliary/alternative components/equipment. This means that by causing flooding they could not achieve interruption of the System functions resulting in emergency reactors shut down.

However, in the same time the risk of internal flooding as a consequence of realized terrorist treat and from there deterioration of the System operation that would lead to disturbance of its continuous operation and the continuous operation of the plant as a whole may be considered a risk of average level. On the one hand, any ill-intentioned act on the System may disturb its continuous functioning but, on the other hand, it is more probable if a terrorist act on NPP is planned, the aim to be destruction of the reactors and from there causing maximum damages on the personnel, economy and environment, rather than temporary disturbance of its functions through internal or external flooding. Therefore, the risk does not exceed the accessible and permissible level and it is not necessary to carry out additional actions for decreasing the risk of flooding as a result of terrorist acts.

Comparative assessment of fire risk level

As in compliance with the above made risk analysis it is possible its level to be high then it could strongly exceed the accessible and permissible risk level because of which it might be necessary to develop and apply a complex of measures directed to decrease of exposure to danger, as well as to decrease of the vulnerability of the System components to fire caused by terrorists.

CONCLUSION

Risk level reduction

As on the one hand the Strategy of European Union Security (Security strategy of European Union, Fri, 12/12/2003) defines terrorism as “key threat” and on the other hand NPP is a strategic object of importance for the national security of Republic of Bulgaria (Decree of

Licensed under Creative Common

Council of Ministers No. 181 of 20.07.2009) and the electric power produced by it has considerable significance both for the country economy and for the countries in the region it is necessary to provide plant continuous operation which in its turn requires application of adequate measures to decrease the risk.

Objectively seen, the potential of decreasing the vulnerability of the critical/vitally important and important/very necessary System components is limited because on the one hand the respective components (in connection with their functions) have specific construction which involves corresponding vulnerabilities and on the other hand the decrease of vulnerability of each component individually not always would be rational from engineering and economical point of view. The decrease of vulnerability by improvement of the capacity of the fire-alarm and extinguishing system also may not be accepted as the most effective solution. Therefore, the potentially necessary decrease of the risk could be achieved first of all by decreasing the exposure to danger, i.e., by eliminating the possibility for the terrorists to penetrate in close proximity to the vulnerable critical/vitally important and important/very necessary System components.

RECOMMENDATIONS FOR RISK REDUCTION

The risk may be reduced by:

- Development of policy, strategy and plan for System continuous operation;
- Periodical analysis of the activity and actualization of the policy, strategy and plan for System continuous operation.

The policy of securing System continuous operation should be directed to, but without being limited by, formulation of the basic principles and the frame necessary to ensure fast reaction in crisis situations, restoring of the System to normal exploitation and recovery of the caused damages and sustained losses.

The strategy for System business continuity is necessary to comprise the following tools of risk decreasing but without being limited to them:

- Improvement of the level of NPP security and protection;
- Building of modern systems of fire centers detection and their extinguishing;
- Providing uninterruptible power supply (UPS systems);
- Permanent back up copying of the electronic data;
- Reliable safe-keeping of critical documents on hard copy;
- Management of records;
- Regular maintenance (service) of the emergency equipment and materials;

Licensed under Creative Common

- Examination of the personnel in advance, before joining the organization/going to work;
- Commissioning, personnel taking holidays and assigning deputies of absentees (management of business trips);
- Ensuring multitude of suppliers of critical products (materials) and services;
- Training the personnel for actions in various situations;
- Ensuring continuity of management.

The plan of System business continuity is necessary to secure maintenance of its normal operation or recovery of interrupted System critical processes in the frames of the required for that time. It should comprise but without being limited to:

- Conditions of plan activation;
- Procedures of plan activation;
- Procedures for action in crisis situations;
- Schedule for inspection of the plan operation and of the process of its maintenance;
- Mastering the plan by the personnel and training for its application;
- Critical assets and resources necessary for fulfillment of the procedures in crisis situations.

REFERENCES

Decree of Council of Ministers No. 181 of 20.07.2009 for determination of strategic objects and activities important for the national security, issued State Newspaper, No. 59 of 28.07.2009

ECP-601: Effective Business Continuity Management, the Institute for Business Continuity Training, US.

European „stress-tests“ of nuclear plants. National report of Bulgaria–December, 2011.

Frame resolution of Council of Europe concerning counteraction against terrorism (2002/475/JHA).

Guiding principles of EU for assessment and chart-making of crises management risk Methods of EU for risk assessment and risk chart-making. (SEC (2010) 1626 final).

Security strategy of European Union - A Secure Europe in a Better World, Fri, 12/12/2003.

Licensed under Creative Common