BgNS TRANSACTIONS volume **23** number 1 (2018) pp. 25–30

# Risk Monitoring in Kozloduy NPP

**E. Stefanov**[1], **L. Kandov**[1], **K. Filipov**[2]

[1] *Kozloduy NPP, Risk Management Section, Bulgaria*

[2] *Department of Thermal and Nuclear Power Engineering, Technical University of Sofia, Bulgaria*

**Abstract.** A Risk Monitoring is one of the specific applications of PSA and is a real-time analysis tool used to determine the point-in-time risk. Risk Monitor calculates the risk for the actual plant configuration defined in terms of the Plant Operational Mode (power operation or one of the shutdown modes), the out of service components, availability of trains of normally operating systems, standby and running mode of trains of operating systems and specifying environmental factors.

The risk measures assessed by Risk Monitors usually include quantitative risk measures such as Core Damage Frequency (CDF) and sometimes the frequency of boiling (for shutdown modes), and qualitative risk measures such as changes of safety functions, safety systems availability and plant transient status (defense-in-depth).

The numerical values associated with quantitative risk measures are quoted in a number of ways which include baseline risk, average risk, point-in-time risk, incremental risk and cumulative risk. These terms are illustrated in the report.

This report illustrates risk assessment in case of taking out the high pressure emergency injection pump in operation mode. The point-in-time risk, allowed outage time (AOT) as well as qualitative risk assessment by changes in Safety functions (defense-in-depth) are assessed and presented as results on the operators screen of risk monitor program. The cumulative risk diagram shows the difference in risk level when a high injection pump or an emergency injection pump is taken out of service in planning mode.

**Keywords:** risk monitoring, CDF, maintenance planning, risk measures, PSA.

| **Abbreviation (designation)** | **Description (explanation)** |
|---|---|
| AOT | Allowed Outage Time |
| CDF | Core Damage Frequency |
| $\Delta$CDF | Incremental CDF |
| CDP | Core Damage Probability |
| $\Delta$CDP | Incremental CDP |
| LERF | Large Early Release Frequency |
| $\Delta$LERF | Incremental Large Early Release Frequency |
| PSA | Probabilistic Safety Analysis/<br>Probabilistic Safety Assessment |
| POS | Plant Operational States |
| RIF | Risk Increasing Factor |
| RWF | Risk Worth Factor |
| TS | Technical Specification |

## 1 Introduction

Risk Monitor is being used to provide an input into maintenance planning to ensure that these activities are scheduled in such a way that high peaks in the risk are avoided wherever possible and the cumulative risk is low. It provides information on which components should be returned to service before particular maintenance activities are carried out and which of the remaining operational components are the most important to ensuring plant safety during specific maintenance outages. It can also provide added weight and assurances when presenting cases for changes in a plants licensing basis – for example, for performing more online maintenance without increasing the overall risk.

Risk Monitor is software based on full scope PSA model that includes the contributions to the risk from all internal initiating events, and internal and external hazards, provides a detailed model for both core damage and large early release and addresses operation at power and all the modes that arise during shutdown and refueling.

In Kozloduy NPP is used RiskWatcher risk monitoring tool based on a RiskSpectrum (both software developed by Lloyd‘s Register) PSA model and provides features of setting plant operational mode, equipment outages, system configurations, periodic tests, environmental factors in operation and planning modes. It includes probabilistic safety measures and defence in-depth capabilities. One of the key features is that all data is edited in the model in RiskSpectrum PSA and no changes need to be introduced “afterwards” in a separate Risk Monitor model.

## 2 Risk Monitor Use

Risk Monitors are used by a wide range of plant personnel in a number of roles. They are used on-line by control room staff that regularly input information to update the current plant configuration, and monitor the plant using the quantitative and qualitative risk measures, allowed configuration time AOT and cumulative risk. They are used off-line for the planning of future maintenance outages, long term risk profiling, analysis of cumulative risk, evaluation of unplanned events such as equipment failures, and feedback of lessons learnt. They are also used as a PSA tool for applications such as PSA-based event evaluation, and as a training aid to enhance safety culture at the plant and increase risk awareness by plant operating staff.

Decision making using a Risk Monitor usually requires the definition of three types of quantitative criteria – risk bands, Operational Safety Criteria and Allowed Configuration Time.

Risk Monitors usually present the quantitative (and qualitative) risk information in the form of colored displays that give the user a clear visual indication of the level of risk.

This is normally done using a four colored band scheme as shown in Table 1.

Table 1. Quantitative (and qualitative) coloured risk information of the level of risk

| | |
|---|---|
| **Low risk** | Band, where maintenance can be carried out with no restrictions; |
| **Moderate risk** | Band, where maintenance needs to be completed quickly; |
| **High risk** | Band, where severe time restrictions need to be imposed and compensatory measures may be required; |
| **Unacceptable risk** | Band, which is not entered voluntarily and immediate action needs to be taken to reduce the risk. |

## 3 Risk Parameters

The risk measures addressed by Risk Monitors usually include **quantitative risk measures** such as Core Damage Frequency (CDF), Large Early Release Frequency (LERF), and **qualitative risk measures** such as safety function, safety system and plant transient status.

**Quantitative risk measures:**

- Core Damage Frequency (CDF);
- Large Early Release Frequency (LERF);
- Equipment importance (RIF, RFW).

**Qualitative risk measures:**

- Defence-in-Depth;
- Safety functions;
- Safety systems and the protection for plant transients;
- Integrated decision making;
- Additional justification to support decision making.

The numerical values associated with quantitative risk measures are quoted in a number of ways which include baseline risk, average risk, point-in-time risk, incremental risk and cumulative risk. These terms are illustrated in Figures 1, 2 and 3, and defined below.

### Baseline risk

The baseline risk is the numerical value of the risk (CDF, LERF, etc.) calculated by the PSA with all components available to carry out their safety function – that is, no components have been removed from service for maintenance or repair. This is shown in Figure 1.

The baseline risk is normally quoted for full power operation and depends on the scope of the PSA that has been carried out – that is, the range of internal initiating events (transients, loss of coolant accidents, etc.), internal hazards (internal fire, flood, etc.) and external hazards (seismic events, external fires, etc.) that have been included. It is also possible to calculate a baseline risk for shutdown conditions. This would require establishing a shutdown sequence which would give the timing for the activities carried out during the outage including the expected Plant Operational States (POS) during shutdown, the decay heat levels, the operational systems and the status of the reactor coolant system (reactor coolant level, pressure, venting, etc.). However, the more usual approach is to use an average shutdown risk for most calculations. The way that the baseline risk is calculated is equivalent to making the assumption that the Plant Operational State for which it is quoted would continue for a year so that there is no weighting that relates to the duration of the Plant Operational State. The baseline risk is usually expressed in units of per reactor year.

### Average risk

The average risk is what is normally calculated by the Living PSA for full power operation. This is the level of risk that is calculated when average maintenance unavailabilities are introduced into the model and hence it is always greater than the baseline risk. This is shown in Figure 1. The average risk can also be calculated by averaging the risk over all the Plant Operational States (full power, low power and shutdown modes) and all the maintenance outages that could occur during these states. In this latter case, the risk from each of the Plant Operational States is weighed according to its relative duration. It is also common to calculate total average risk using an average risk for power and an average risk for shutdown, weighting each with its relative duration. The average risk is usually expressed in units of per reactor year.

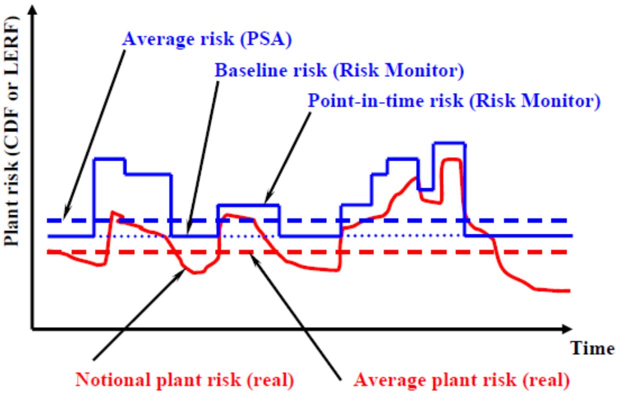


Figure 1. Risk measures used in PSA – average/ baseline/ point-in-time risk.

### Point-in-time risk

The point-in-time risk is the level of risk that arises from a specific plant configuration and this is what is calculated by a Risk Monitor. This is shown in Figure 1.

The point-in-time risk will change as the plant configuration and environmental factors change. This is usually expressed in units of per reactor year. The way that the point-in-time risk is calculated is equivalent to making the assumption that the plant configuration for which it is quoted would continue for a year so that there is no weighting that relates to the duration of the plant configuration.

### Incremental CDF (LERF)

The incremental CDF ($\Delta$CDF) is the increase in the Core Damage Frequency from a specific plant configuration. This is equal to the CDF for the configuration minus the baseline CDF. The incremental LERF ($\Delta$LERF) is defined in the same way.

$$\Delta \mathrm{CDF}_{\text{configuration}} = \mathrm{CDF}_{\text{point-in-time}} - \mathrm{CDF}_{\text{baseline}}$$
$$\mathrm{LREF}_{\text{configuration}} = \mathrm{LREF}_{\text{point-in-time}} - \mathrm{LREF}_{\text{baseline}}$$

### Incremental Core Damage Probability (CDP) or Large Early Release Probability (LERP)

The incremental CDP ($\Delta$CDP) is the increase in the Core Damage Probability from a specific plant configuration $\{1\}$. This is equal to the incremental CDF for the configuration multiplied by the time spent in the configuration. The incremental LERP ($\Delta$LERP) is defined in the same way. This is shown in Figure 2.

$$\Delta \mathrm{CDP}_{\text{config}} = \Delta \mathrm{CDF}_{\text{config}} \times \mathrm{T}_{\text{config}}$$
$$\Delta \mathrm{LERP}_{\text{config}} = \Delta \mathrm{LERF}_{\text{config}} \times \mathrm{T}_{\text{config}}$$

This can be used in the calculation of the Allowed Configuration Time.

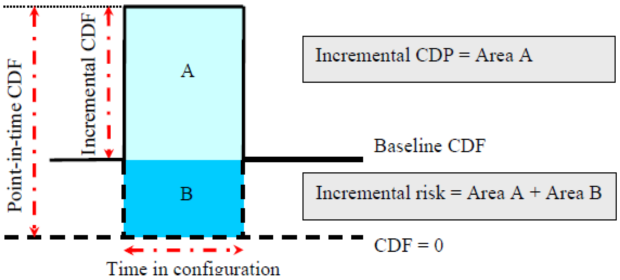


Figure 2. Risk measures used in the Risk Monitor.

### Cumulative risk

The cumulative risk (Figure 3) is the sum of the incremental risk values for all the actual plant configurations that have occurred during a period of time. The annual cumulative risk is the one that is normally quoted but the cumulative risk for other periods or for the duration of a particular outage may also be calculated. This is used by plant operators as a performance measure which indicates how effective they have been in managing the risk from the plant which arises during maintenance outages.

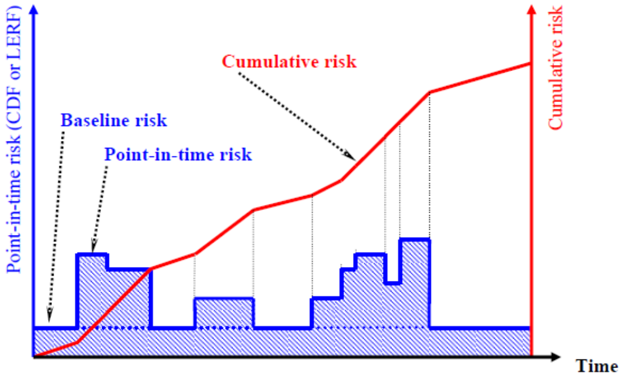


Figure 3. Risk measures used in PSA – cumulative risk.

The baseline/ point-in-time risk and the cumulative risk have been plotted on different scales so that this figure is for illustrative purposes only.

### Allowed Outage Time AOT

The AOTs for components/canal are the times given in the plant Technical Specifications for typical/ bounding plant configurations and are mandatory requirements that need to be met by the plant operators. These requirements have been based on deterministic criteria but now are often based in part on risk information obtained from the Living PSA.

It relates to the maximum time for which a component/ train unavailability or a plant configuration is allowed to persist before some action has to be taken to move the plant to a safer state – for example, by returning items of equipment to service or by shutting the plant down.

### Risk importance factors

Risk increasing factor (RIF) – Factor with which the risk would increase if the equipment was taken out of service.

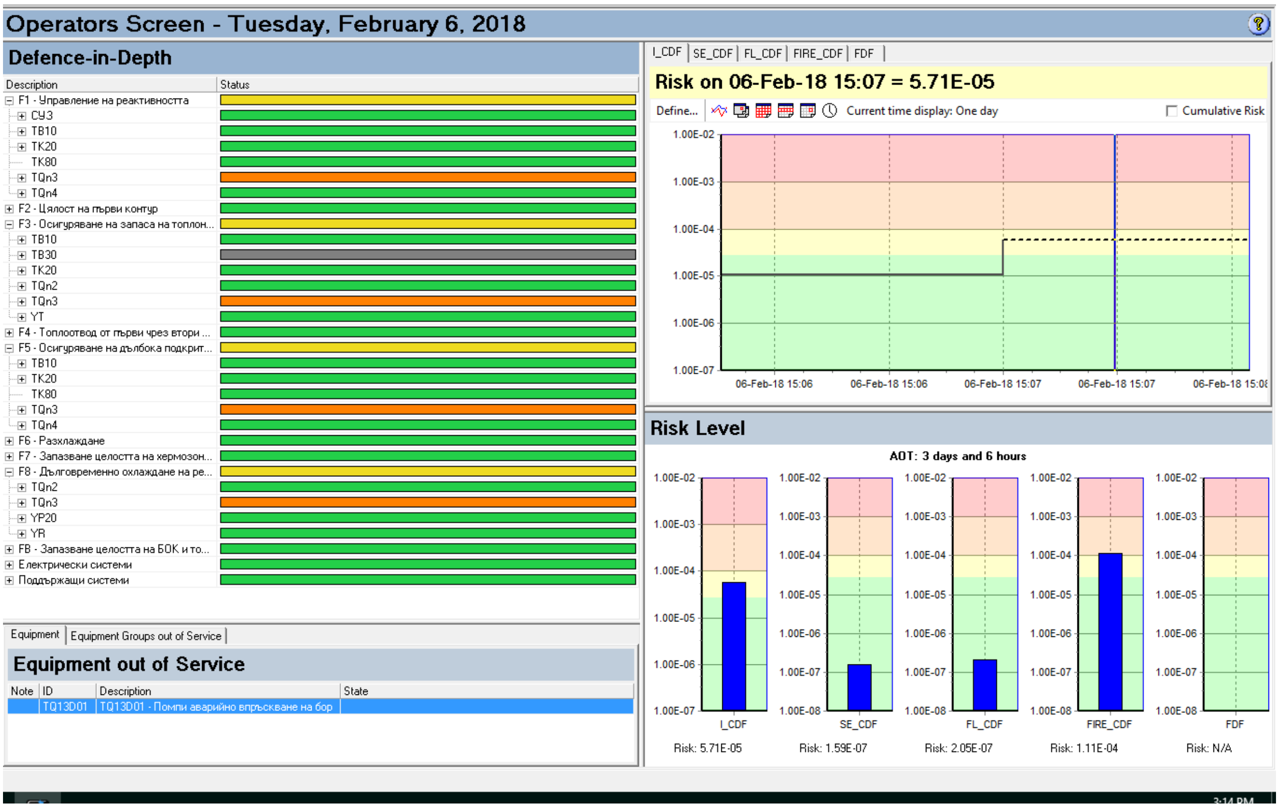
Risk worth factor (RWF) – Factor with which the risk would decrease if the equipment (taken out of service) was restored to service.

### 3.1 Defence-in-depht

Defence-in-depth relates to the provision of redundant and diverse trains of the safety systems that carry out the above safety functions. This is a more restrictive use of the term than normal usage which relates to the approach to safety at nuclear power plants that is aimed at preventing initiating events from occurring and, if this fails, mitigating their potential consequence and preventing progression to a more severe condition.

### Integrated decision making

This is the process that is used by plant operators and regulators in which information from a number of sources is combined in reaching a decision on a plant safety issue. The aim of the integrated decision making approach (sometimes referred to as a risk-informed approach or a blended approach) is to ensure that the relevant mandatory requirements are complied with, the deterministic requirements such as defence-in-depth, safety margins, etc.



Operators Screen - Tuesday, February 6, 2018

Defence-in-Depth

| Description | Status |
|---|---|
| ⊟ F1 - Управление на реактивността | 🟨 |
| ⊞ СУЗ | 🟩 |
| ⊞ TB10 | 🟩 |
| ⊞ TK20 | 🟩 |
| TK80 | 🟩 |
| ⊞ TQn3 | 🟧 |
| ⊞ TQn4 | 🟩 |
| ⊞ F2 - Цялост на първи контур | 🟩 |
| ⊟ F3 - Осигуряване на запаса на топлон... | 🟨 |
| ⊞ TB10 | 🟩 |
| ⊞ TB30 | ▨ |
| ⊞ TK20 | 🟩 |
| ⊞ TQn2 | 🟩 |
| ⊞ TQn3 | 🟧 |
| ⊞ YT | 🟩 |
| ⊞ F4 - Топлоотвод от първи чрез втори ... | 🟩 |
| ⊟ F5 - Осигуряване на дълбока подкрит... | 🟨 |
| ⊞ TB10 | 🟩 |
| ⊞ TK20 | 🟩 |
| TK80 | 🟩 |
| ⊞ TQn3 | 🟧 |
| ⊞ TQn4 | 🟩 |
| ⊞ F6 - Разхлаждане | 🟩 |
| ⊞ F7 - Запазване целостта на херметизон... | 🟩 |
| ⊟ F8 - Дълговременно охлаждане на ре... | 🟨 |
| ⊞ TQn2 | 🟩 |
| ⊞ TQn3 | 🟧 |
| ⊞ YP20 | 🟩 |
| ⊞ YR | 🟩 |
| ⊞ FB - Запазване целостта на БОК и то... | 🟩 |
| ⊞ Електрически системи | 🟩 |
| ⊞ Поддържащи системи | 🟩 |

Equipment | Equipment Groups out of Service

Equipment out of Service

| Note | ID | Description | State |
|---|---|---|---|
| | TQ13D01 | TQ13D01 - Помпи аварийно впръскване на бор | |

I_CDF | SE_CDF | FL_CDF | FIRE_CDF | FDF

Risk on 06-Feb-18 15:07 = 5.71E-05

Define... Current time display: One day ☐ Cumulative Risk

Risk Level

AOT: 3 days and 6 hours

Risk: 5.71E-05 Risk: 1.59E-07 Risk: 2.05E-07 Risk: 1.11E-04 Risk: N/A

Figure 4. RiskWatcher operators screen. A high pressure injection pump (5TQ13D01) is out of service.

are met, the risk from the plant is understood and managed, and the performance of the plant is monitored. This is illustrated in Figure 4.

## 4 Risk Assessment in Kozloduy NPP (Examples)

### 4.1 RiskWatcher Operation (online) mode

The Operators screen in RiskWatcher for current unit configuration shows:

- Defence-in-depth safety functions F1-F8 (TS requirement is met – green; TS requirement is met, but system(s) are using AOT – yellow/orange and TS requirement is not met – red);
- Risk profile;
- Equipment out of service;
- AOT.

In Figure 4 is shown the operators screen when a high pressure injection pump (5TQ13D01) is out of service during full power operation. The risk level increases upto 5.71E-5 which is in yellow area and actions may be required to decrease the risk. The estimated AOT is 78 hours. For comparison, TS requirement for full power operation with an unavailable safety channel is set AOT to 72 hours (deterministic criteria).

### 4.2 RiskWatcher Planning (offline) mode

An emergency cooling pump TQ12D01 or a high injections pump TQ13D01 are planned for maintenance for 24 hours during full power operation. A decision will be made with the help of RiskWatcher program in planning mode.

In Figure 5 is shown the risk profile when an emergency cooling pump (5TQ12D01) is taken out for 24 hours. CDF increases to 5.99E-05 which is in yellow area, i.e. increased risk, actions may be required to lower risk.

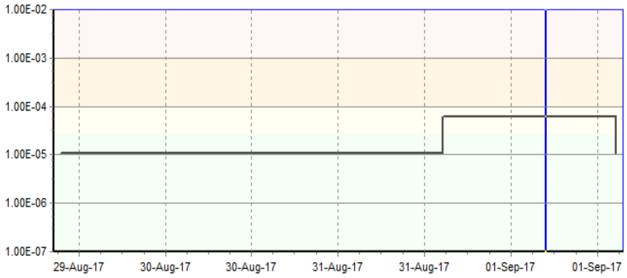


Figure 5. RiskWatcher risk profile when a emergency cooling pump (5TQ12D01) is taken out for maintenance for 24 hours.

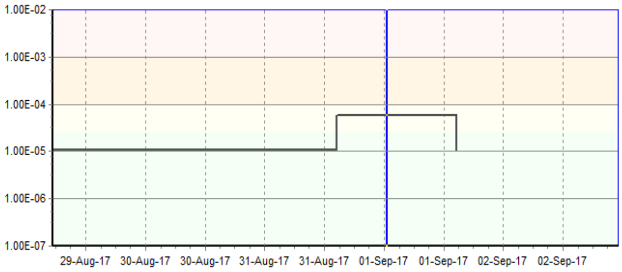


Figure 6. Risk profile when a high injections pump TQ13D01 is taken out for maintenance for 24 hours.

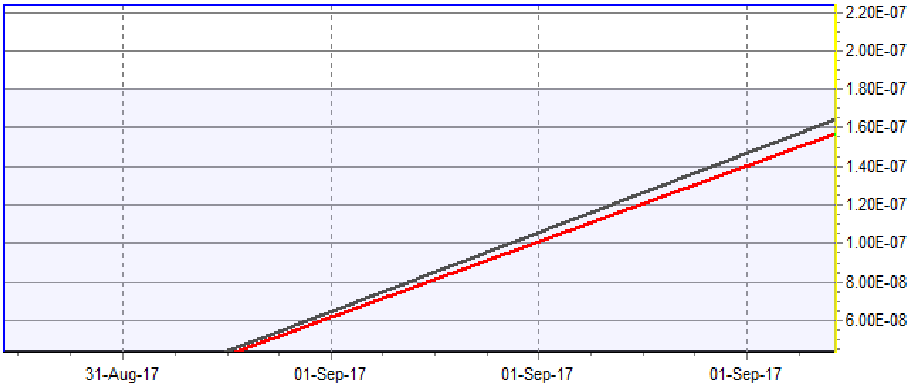


Figure 7. A comparison of the cumulative risk when TQ13D01 (red color) and TQ12D01 (black line) are taken out for maintenance for 24 hours.

In Figure 6 is shown the risk profile when a high injections pump TQ13D01 is taken out for 24 hours. CDF increases to 5.74E-05 which is in yellow area, i.e. increased risk, actions may be required to lower risk.

To compare these two profiles it is used RiskWatcher feature for cumulative risk calculation. This is used by maintenance staff as a performance measure which indicates how effective they have been in managing the risk from the plant which arises during maintenance outages.

## 5 Conclusion

Based on results for cumulative risk (Figure 7) it can be recommend a maintenance of a high injections pump TQ13D01 (lower cumulative risk for 24 hours).

The decision making process (see Figure 8) is used by Kozloduy NPP operators and maintenance staff to ensure that the deterministic requirements such as defence-in-depth, safety margins, etc. are met and the plan risk issues are monitored, understood and managed.

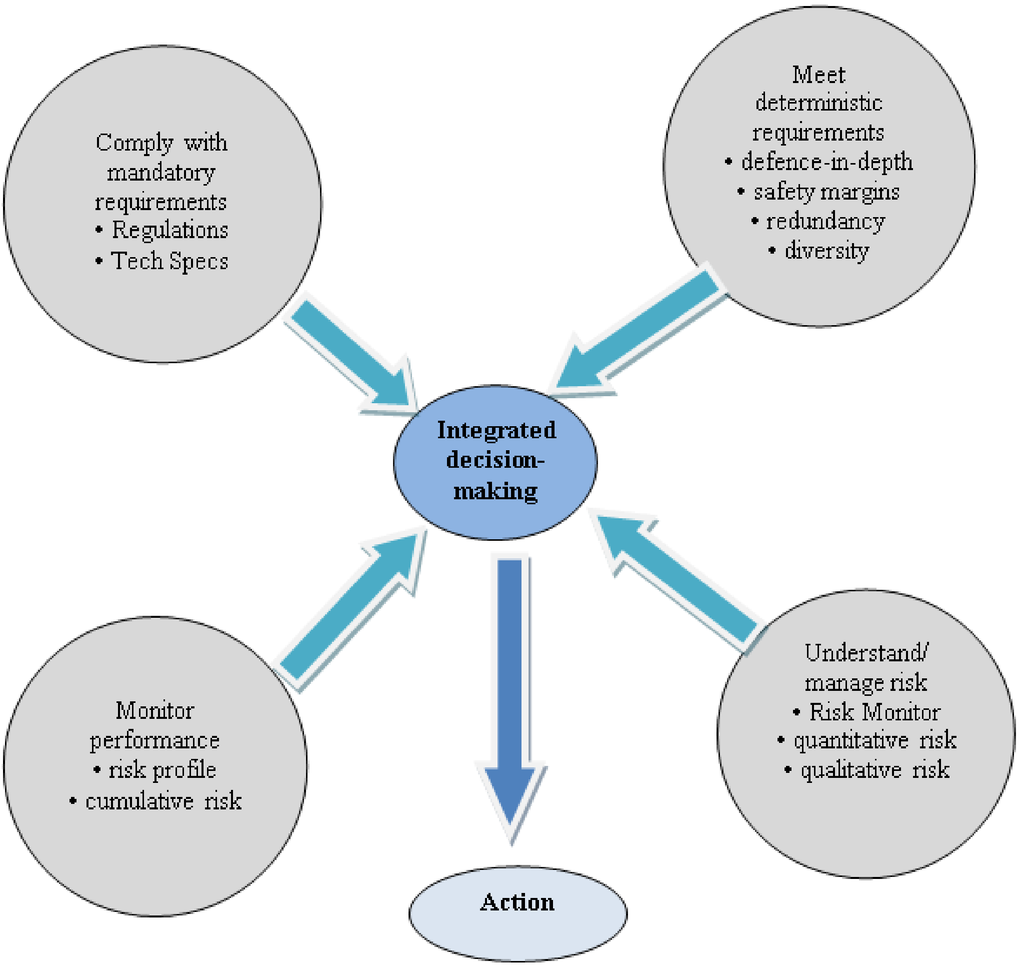


Figure 8. Integrated decision making process.

## References

[1] BNRA (2016) Regulation for the Safety of Nuclear Power Plants.

[2] BNRA (2010) Safety Guidelines for the Application of Regulatory Requirements: Use of PSA to Support NPP Safety Management. BNRA, PP-6/2010.

[3] NEA/CSNI/R92004)20, Risk Monitors the State of the Art in Their Development and Use at Nuclear Power Plants.