

# Review of the Preventive Maintenance Requirements for the Safety Systems of the Mochovce NPP

Zoltan Kovacs<sup>a\*</sup>, Robert Spenlinger<sup>a</sup>

<sup>a</sup>RELKO Ltd., Bratislava, Slovak Republic

---

**Abstract:** A requirement to optimize the Preventative Maintenance (PM) tasks assigned to specified safety systems has been identified at Mochovce Nuclear Power Plant (NPP). RELKO Ltd has been tasked with optimising the PM tasks via application of the Reliability-Centered Maintenance (RCM) and PSA methodology. This paper details the results of the RCM analysis performed on the Core Cooling Systems. It is concluded that the PM tasks assigned to the Core Cooling Systems were, in the main, based upon the original equipment manufacturers' (OEM) recommendations. Following the accumulation of about ten years of operating and maintenance experience it was concluded that many of the current task types and task frequencies required major revision in order to maintain the optimum levels of both reliability and availability of the Core Cooling Systems. It is also concluded that in several cases, specific components within the Core Cooling Systems will benefit from a shift in maintenance strategy from fixed interval invasive routines to a predictive maintenance (PdM) based strategy. Such a strategy will ensure close monitoring of system and component performance without compromising nuclear safety or availability. It is recommended that the Mochovce NPP replaces the current maintenance catalogue assigned to the Core Cooling Systems with new PM tasks detailed in the paper. In addition, the paper presents the impact of changes on CDF and LERF after implementation of the new PM tasks.

**Keywords:** Preventive maintenance, reliability-centered maintenance, PSA, core damage frequency

---

## 1. INTRODUCTION

The construction, operation and maintenance of the nuclear power plants has been a well-subsidised business for a long time. However, the financial sources are considered as a very important aspect in this matter during the last decades. The budgets are limited and taken into account very carefully. They are needs to make reliable and cost effective choices with respect to the improvements that have to be made in case of modernization or maintenance projects.

Probabilistic Safety Assessment (PSA) is a tool which is used to evaluate the effects of improvements that are being implemented in the plant. Importance measures are defined which can show us the importance of the components from the safety point of view. These importance measures are applied mainly in the following areas: 1) optimization of the test and maintenance activities, 2) optimization of the plant design by adding, removing and modification of systems or components and 3) configuration control with the effect of taking a component out of service.

The paper is focused on optimization of maintenance activities in the Mochovce plant using the RCM methodology. The level 1 full power, low power and shutdown PSA model of the plant is used to identify the most important systems and components and to provide their importance ranking.

A requirement to optimize the PM tasks assigned to specified safety systems has been identified at Mochovce NPP. RELKO Ltd has been tasked with optimising the PM tasks via application of the RCM and PSA methodology. This paper details the results of the RCM analysis performed on the Core Cooling Systems. The focus of the study is entirely upon major electro-mechanical and mechanical components, i.e. pumps, valves, tanks, etc. It should be noted that the pipework is subject

---

\* kovacs@relko.sk

to a discrete programme of specialist inspections, e.g. pipe wall thickness checks, etc., the pipework associated with the Core Cooling Systems is excluded from this review.

After introduction the usage of PSA importance measures is described in section 2 to identify the dominant list of components. Then, the overview of RCM methodology is provided in section 3. Section 4 describes the functional breakdown of the Core Cooling System. Section 5 provides the discussion of the RCM results. The results of risk assessment for the state of the plant after implementation of the proposed changes in the maintenance activities are presented in section 6. The conclusions are described in section 7.

## 2. USAGE OF IMPORTANCE MEASURES

The nuclear power plants are designed using the defence-in depth principle. Therefore, a single failure of a component or other basic event will probably not result in a large accident. Such accidents will be the result of combinations of multiply basic events. The PSA determines all important minimal cutsets that could lead to a large accident. The final results of a PSA study are then represented in the form of core damage frequency, early release frequency, etc. The risk importance measures give an indication of the contribution of a certain component (item) to the total risk.

The following importance measures are defined and more frequently used [2]:

- |                             |   |
|-----------------------------|---|
| 1. Risk reduction worth     | $RRW = R(\text{base}) / R(x_i = 0)$                   |
| 2. Risk achievement worth   | $RAW = R(x_i = 1) / R(\text{base})$                   |
| 3. Fussel-Vesely importance | $FV = [R(\text{base}) - R(x_i = 0)] / R(\text{base})$ |

The following definitions are used in the formulas:

- $R(x_i = 1)$  - the increased risk level with basic event  $x_i$  assumed failed
- $R(x_i = 0)$  - the decreased risk level with basic event  $x_i$  assumed to be perfectly reliable
- $R(\text{base})$  - the present risk level with baseline unavailability of component  $i$ .

The RRW represents the maximum decrease in risk for an improvement to the component associated with basic event. The RAW presents a measure of the worth of the basic event in achieving the present level of risk. In addition, it also indicates the importance of maintaining the current level of reliability for the basic event. FV importance is a normalised risk reduction importance and is comparable to RRW.

Nowadays the most important area where importance measures are applied is in test and maintenance programmes of the plants. The influence of test and maintenance is completely connected to the change of unavailability and not to a change in the defence in depth against a failure of the component. The components are considered important from the risk point of view during maintenance and testing if:  $RRW > 1.005$  or  $RAW > 2$  or  $FV > 0.9$  [3].

## 3. METHODOLOGY OF RCM

After identification of the safety important components using the importance measures the application of RCM methodology is performed. In this part the overview of the methodology is presented [1].

### 3.1 The RCM Overview

RCM logic is primarily concerned with the preservation of the ability of a plant item to perform its prescribed function. Note that the term 'item' may apply to a system, sub-system or a single component.

The process begins with a functional breakdown of the 'item' to ensure that all functions performed by the item undergo analysis. Once this is achieved, the second stage of the process, significant item selection, is completed. A 'significant item' is defined as any item the functional failure of which would result in an adverse effect on safety, an adverse effect on operational capability or high repair or recovery costs.

Following the compilation of the list of significant items, a comprehensive Failure Modes and Effects Analysis (FMEA) is performed for each item. The result of the FMEA for each function of each item is then subjected to the main RCM algorithm with a view to defining the optimum PM task (if one exists) to protect the function. If no suitable task exists, the RCM logic may, under some circumstances, direct that redesign is necessary, i.e. modification for in-service plant.

Assuming a suitable task is defined, the next stage is to derive the task frequency. The method of calculating task frequencies will vary dependent upon the type of PM task, however, for in-service plant, all rely heavily on historical data and operator experience.

The final stage of the analysis is to package the PM tasks into the maintenance plan for the item analysed. In the case of each pilot study it is expected that the list of tasks will form the basis for the revision of the existing maintenance schedule.

### **3.2 Functional Breakdown**

In order to ensure that all functions of the system under scrutiny are taken into account during the RCM analysis, it is of paramount importance that the analysis is performed at the correct level of complexity. This level is known as the 'indenture level'. The normally preferred indenture level is that of 'system', however, due to the complexity of some systems it may be necessary to break down the system into sub-systems, assemblies or components.

### **3.3 RCM Logic**

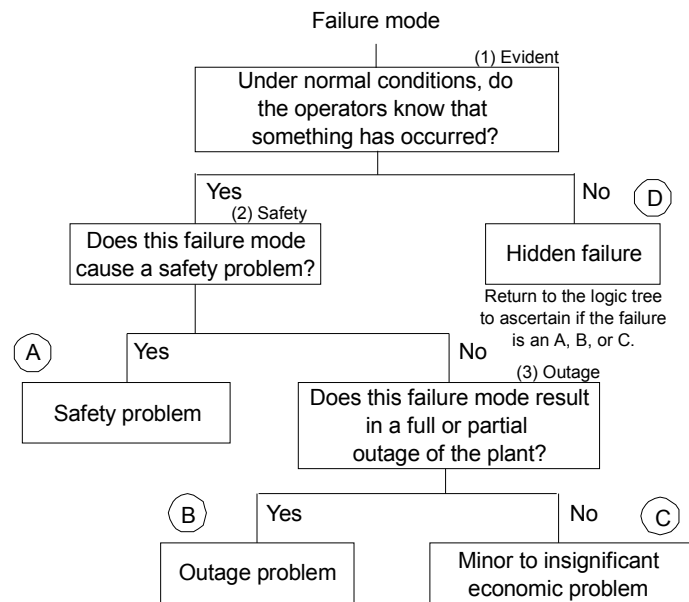
The RCM logic is embedded in RCM analysis. It provides answers to specific basic questions presented by the RCM logic. The first series of questions define the failure consequences:

- Evident Safety (evident failure with safety consequences)
- Economic/Operational (evident failure without safety consequences)
- Hidden Safety (hidden failure with safety consequences)
- Hidden Non-safety (hidden failure with economic/operational consequences only)

The failure modes of components are classified using the logic tree. The priorities are determined in this step. All failure modes are evaluated using the following issues: A) safety related failure mode, B) failure mode leading to plant shutdown or C) failure modes with minor economical problems. There are also hidden failures (D) or failures evident for the operator. After termination of analysis each failure mode is classified as A, B, C, D/A, D/B or D/C. There are the following priorities of evident and hidden failure modes:

1. A or D/A
2. B or D/B
3. C or D/C

The logic tree to identify priorities is presented on Figure 1.



**Figure 1: RCM Logic Tree**

### 3.4 Types of Preventive Maintenance Tasks and Task Frequency Calculation

PM tasks are grouped into four basic types:

1. On-Condition Task - calls for corrective maintenance on the condition that an item does not meet a specified performance standard.
2. Hard-Time Task - an item is discarded or restored before a specified life limit
3. Combination Task - a combination of Task 1 and 2
4. Failure-Finding Task - to find the failure of hidden functions.

On-condition task frequencies are derived from factoring the calculated interval between the Potential Failure condition and the Functional Failure condition, i.e. the total time between the item no longer performing to its specified performance parameters and complete functional failure. This interval, known as the P-F interval, is then factored depending upon the failure consequences. If the functional failure of the item has safety consequences, the P-F interval is divided by a factor of 3 to produce the task interval. Should the failure consequences be economic or operational, a factor of 2 is sufficient. Therefore, should the P-F interval of an item be calculated using historical data as 2016 hours, and the failure would have safety consequences, the task frequency would be calculated as:

$$\frac{2016 \div 24 \div 7}{3} = 4 \text{ weeks}$$

‘Operator Monitoring’ is a recognized On-Condition Task which involves no specific maintenance effort. It may be assigned to an item where a reasonably high degree of routine monitoring already exists. It must not be assigned to place an additional task on the operator.

Hard-Time Task frequencies are derived from calculating the ‘Safe Life’ of an item and then factoring the life by 2 or 3 depending upon the failure consequences. Often the Safe Life of an item, e.g. a structural or pipework support, is supplied by the manufacturer. Therefore, an item with a calculated Safe Life of 8 years, the failure of which would have only economic consequences, should be replaced or overhauled every 4 years.

A combination task is an amalgamation of an On-Condition Task and a Hard-Time Task, hence two task frequency calculations are required. This type of task is usually assigned to an item which required scheduled replacement or overhaul, but, possibly due to a harsh operating environment, it is judged prudent to also apply a series of inspection based tasks to ensure that degradation is not so rapid as to shorten the perceived life of the item.

Failure-Finding Task frequencies for safety-related hidden functions are derived primarily by calculating the acceptable degree of unavailability of the redundant or protective plant item. This is calculated by dividing the acceptable cumulative probability of failure, i.e. a Safety Case claim, by the failure rate of the primary or protected plant item. However, in order to perform this calculation precise historical data is required. Where no such data is available it is acceptable to derive the task frequency as a percentage of the Mean Time Between Failures (MTBF) dependent upon the required confidence level. For items the failure of which may carry nuclear safety consequences, a ninety-five percent confidence level is appropriate, for those without a safety consequence or plant/operator safety only, a ninety per cent confidence level is sufficient. It should be noted that for plant items that have not suffered any failures, the MTBF is taken to be the total usage to date. Some task frequencies within an RCM study may be the result of a necessary default due to constraints imposed by the Safety Case, i.e. should a revised task frequency cause a disruption to a probabilistic claim in the Safety Case, the RCM derived frequency should be ignored in favour of that stated in the Safety Case. It should also be noted that changes in the system operating regime may impact upon some task frequencies.

Should the analyst be unsure of the answer to any question posed by the main decision algorithm, he may elect to resort to the 'default logic'. For example, if it were unclear whether or not a functional failure would have an adverse effect on operating safety, the default logic would instruct the analyst to default to 'yes'. Likewise, should the analyst be aware that a functional failure would be evident to the operator whilst performing normal duties, but the failure consequences would be rapid and severe, he may default to 'hidden' thereby allowing the possibility of generating a Failure-Finding Task not available for evident functional failures.

#### **4. FUNCTIONAL BREAKDOWN OF THE CORE COOLING SYSTEMS**

The Core Cooling Systems are broken down into four major sub-systems:

- High Pressure Safety Injection System
- Low Pressure Safety Injection System
- Core Flooding System
- Containment Spray System

##### **4.1 High Pressure Safety Injection System**

The High Pressure Safety Injection System is further broken down into the following components:

- Boric acid tank
- Injection pump
- Motor operated valves
- Check valves
- Manual valves

##### **4.2 Low Pressure Safety Injection System**

The Low Pressure Safety Injection System is further broken down into the following components:

- Boric acid tank
- Injection pump

- Motor operated valves
- Check valves
- Manual valves

### **4.3 Core Flooding System**

The Core Flooding System is further broken down into the following components:

- Hydro-accumulators, including pressure relief valves
- Check valves
- Motor operated valves

### **4.4 Containment spray system**

The Containment Spray System is further broken down into the following components:

- Boric acid tank
- Heat Exchanger
- Injection pump
- Motor operated valves
- Check valves
- Manual valves

## **5. DISCUSSION OF THE RCM RESULTS**

In this part the main results of the RCM analysis are discussed for the different systems and components.

### **5.1 High Pressure Safety Injection System**

The HPSI tanks are subject to daily operator monitoring during which any signs of external corrosion or fatigue cracking would become evident and prompt timely repair action. The tank contents are also dipped monthly to test the boric acid concentration. Any internal corrosion mechanism would be revealed during water analysis as the presence of foreign material would be evident. Accordingly, no discrete PM tasks are assigned to the tanks.

The ongoing performance and reliability of the HPSI injection pump is a cause for concern. The pump is currently of poor reliability due to design issues, especially with the hydro disc. It is noted that many other WWER440 NPPs have overcome similar historical problems via successful modification action. Following a beneficial liaison visit of these plants, Mochovce NPP engineers have emulated part of their modification programme. However, some pump problems continue to occur. Accordingly, it is recommended that the Mochovce NPP HPSI pumps undergo a programme of modification in the same manner as that undertaken at other WWER440 NPPs. In the meantime, it is recognised that the current HPSI pump overhaul strategy is unnecessary and may even be counter-productive to successful pump operations by introducing maintenance-induced failure. As with the majority of pumps associated with Core Cooling Systems, the HPSI pumps are currently subject to both invasive overhaul and a condition-based PM strategy. Modern techniques associated with rotating plant tend towards PdM-based strategies (on the proviso that the plant in question runs frequently enough to render the PdM data as effective in predicting impending failure). In the case of the HPSI pumps this is clearly the case and as a result, the existing invasive overhaul routines are recommended for deletion in favour of existing PdM routines, i.e. vibration diagnostics, NDT, etc.

It is readily apparent that the majority of MOVs associated with the HPSI System (and the Core Cooling Systems as a whole) are routinely overhauled in accordance with OEM recommendations.

However, such recommendations are often based upon a pessimistic assessment of the number of annual valve operations, i.e. it is assumed that many operations will occur. However, when installed into standby or emergency systems, this is clearly not the case. The fundamental function of any given valve is simply to open or close on demand, i.e. to physically move to the desired position. Preservation of this functionality is supported by routine valve movement rather than fixed interval invasive overhaul. To this end, all HPSI MOV overhauls are recommended for deletion in favour of frequent freedom of movement checks, supported by valve functional tests, most of which are performed by default during 3-monthly, annual and 4-yearly system/full injection tests.

The primary failure mode associated with check valves is that of leaking, i.e. failure of the valve to maintain tightness in order to prevent reverse flow whilst allowing full forward flow (this often also applies to MOVs, etc). To this end, a task of functional test is recommended for HPSI-related check valves. It should be noted, however, that as the relevant check valves are tested as a matter of routine during 4-yearly injection tests, assigning these functional tests does not constitute an increased maintenance burden. Assigning these tasks to the relevant check valves simply formalises the process and ensures that the valves will be routinely stroked from fully open to fully closed during the 4-yearly injection test with the results formally recorded.

As with MOVs and check valves, freedom of movement is the primary consideration regarding manual valves. Assigning infrequent valve overhaul, e.g. every 8 years during alternate outages simply cannot guarantee that the valve will not seize between overhauls. Manual valve seizure can cause significant delays when, for example, attempting to isolate a pump for repair or maintenance. Accordingly, 8-yearly overhauls are recommended for deletion in favour of more frequent (1 monthly) freedom of movement checks.

## **5.2 Low Pressure Safety Injection System**

The conclusions for LPSI tanks, MOVs, check valves and manual valves are the same as in case of the HPSI system.

The LPSI System pump is currently subject to both invasive routine overhaul and a PdM-based strategy. Furthermore, the 3-monthly test includes vibration diagnostics on all 3 pumps and pump motor bearing temperatures are constantly provided. Accordingly, the current scheduled overhaul recommended for deletion in favour of existing PdM.

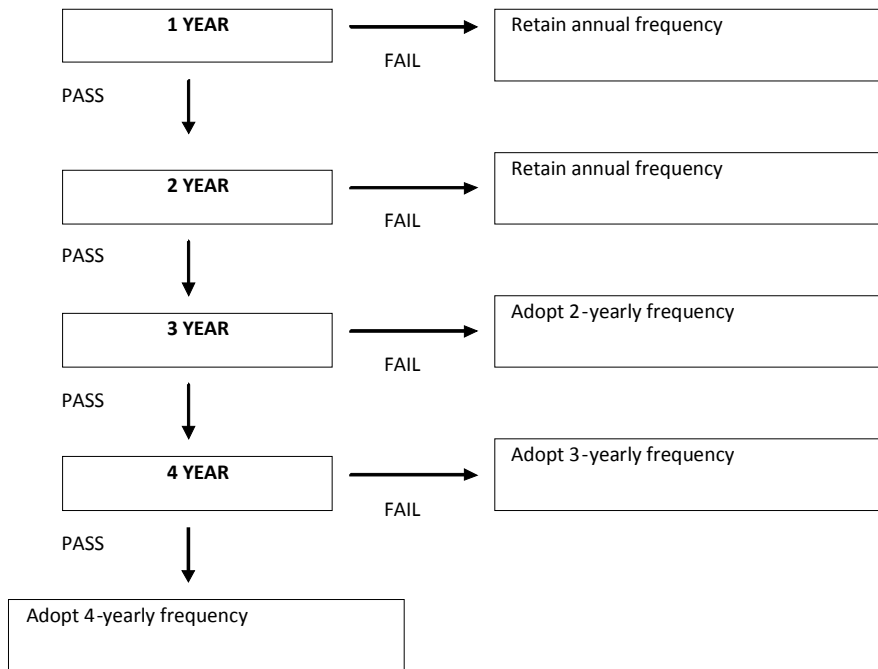
## **5.3 Core Flooding System**

The current strategy of 4-yearly specialist inspections and NDT (as a component of the overall primary circuit inspection programme) are recommended for retention. However, 4-yearly pressure test is recommended for deletion on the grounds that intentional over-pressurisation of a nuclear-safety related vessel is not good engineering practice. Consultation with the relevant engineers from the Sizewell Power Station (where the hydro-accumulators are similar in size and construction to those in use at Mochovce NPP) has revealed that although similar detailed inspections and NDT are performed, pressure testing is not carried out.

The Pressure Relief Valves (PRVs) associated with the hydro-accumulators require a specific strategy. The 8 Core Flooding System PRVs provide protection against possible hydro-accumulator breach should the nitrogen pillow cause an over-pressurisation. If such a breach were to occur owing to failure of the PRV to lift the minimum consequences would be a reactor trip, system drain down with the loss of up to 14 days of generation, and the requirement to replace an extensive quantity of boric acid.

Notwithstanding the commercial importance of these PRVs, the current annual overhaul (assigned to 8 valves) is a high maintenance burden. Furthermore, consultation with the relevant systems engineer has revealed that during approximately 40 overhauls to date, no problems with the PRVs have been

encountered. In close co-operation with the Mochovce engineers, the following strategy has been identified. For a trial period of 4 years, each year 2 PRVs (1 each from a different hydro-accumulator) will be tested. Should any defects or degradation in valve performance be noted after 2 years, the current annual frequency will remain in force. Should there be no problems after 2 years, but observed failures after 3 years, the frequency will be set at 2 years. Should there be no problems after 3 years, but observed failures after 4 years, the frequency will be set at 3 years. Should there be no problems after 4 years, the frequency will be set at 4 years. The whole process is presented on Figure 2.



**Figure 2: The frequency determination strategy for PRVs**

RCM Logic recommends that check valves are subject to a similar trial to that detailed above for the PRVs. However, the trial will be simplified by overhauling 1 valve per train after 4 years. Should no problems be encountered during the second batch overhaul at 8 years, the frequency of overhaul for all 8 valves will remain at 8 years. However, should there be any problems encountered at 8 years, the current 4-yearly frequency will remain in force. During this trial, annual valve tightness checks have been introduced as an extra measure of protection against unforeseen valve failure.

For MOVs a similar trial to that detailed above for check valves is recommended. However, the current 8-yearly pump motor overhaul is recommended for a similar trial with a light maintenance routine replacing full overhaul. As with check valves, an annual valve tightness check is recommended as additional high frequency protection whilst the trial is undertaken.

#### **5.4 Containment spray system**

The conclusions for the tanks and pumps are the same as in case of the LPSI system.

The heat exchanger within the Containment Spray System is of primary importance as it not only cools the water re-circulated from the containment sump during HPSI and LPSI System operations, but also provides the means of emergency core cooling following a seismic event. RCM Logic has recommended that the current PM strategy assigned to the heat exchanger should be retained, i.e. continuous leak testing (via integral pumps), permanent measurement of chemical solutions in case of tube leaks and 4-yearly detailed inspections, performed by specialists team and including vessel wall thickness check.



For the majority of MOVs installed within the Confinement Spray System, it was determined that the consequences of failure were of little or no significance. Accordingly, a run-to-failure policy is recommended.

The check valves remain subject routine testing during scheduled system testing. Where necessary, valve testing via air pressure injection should be performed.

As with other manual valves within the Core Cooling Systems, the manual valves associated with the confinement spray system should be subject to monthly freedom of movement checks.

## **6. THE RESULTS OF RISK ASSESSMENT**

The pumps, the motor operated valves and check valves of the HPSI and LPSI system were identified as the most dominant components from the risk point of view. There are the components of the safety systems which are in stand-by operating modes and periodically tested. The unavailability of the components is influenced by:

- failure rate
- testing interval
- repair time
- testing and maintenance duration and
- human errors

The impact of maintenance changes on the failure rates cannot be evaluated before their implementation and receiving experience from operation. Then, after a time period, some trends can be identified in the failure rates. However, the RCM approach has the objectives not increase but to decrease the failure rates by implementation of the new PM tasks.

The analysis recommended changes in the intervals of overhauls or these interactions were deleted. These changes decrease mainly the maintenance duration and impacts of human errors. In some cases the interval of overhauls is changed from 4 to 8 years. It decreases the risk during the refueling outage. The core damage frequency for shutdown operating modes is decreased by about 5%. There are no significant changes in the large early release frequency. However, on the other side, significant financial sources are saved by the proposed changes.

## **7. CONCLUSIONS**

The following conclusions associated with the Mochovce NPP Core Cooling Systems are made:

- Operating experience indicates that the system components are currently over-maintained as the current PM tasks and frequencies are primarily OEM based.
- Mochovce NPP performs sufficient non-invasive PdM monitoring of important components to render invasive overhaul unnecessary.
- The current PM tasks assigned to the Core Cooling Systems have to be replaced with new one detailed in the analysis.
- The modern ultrasound techniques should be employed for the purposes of performing valve tightness checks.
- Several plant items analyzed are recommended for 'run-to-failure' as their failure present no safety, commercial or economic consequences.
- The proposed changes minimize the maintenance activities and reduce the shutdown risk.

## References

- [1] Smith, A. M., Hinchcliffe, G. R.: RCM Gateway to World Class Maintenance, Elsevier, USA, ISBN 0-7506-7461-X, 2004
- [2] M. van der Borst, Schoonakker, H.: An Overview of PSA Importance Measures, Reliability Engineering and System Safety, (2001)
- [3] Optimization of the Preventive Maintenance Tasks Using RCM, RELKO report 3R0404, Bratislava 2006 (in Slovak)