Safety Analysis Uncertainty Related to Design and Manufacturing Quality Assurance

E. N. SOKOLOV, Siberian Directorate of Gosatomnadzor of Russia*, Novosibirsk, Russia

INTRODUCTION

A substantial change in the regulatory requirements has accompanied the development in the nuclear energetics since the Chernobyl accident. Present paper describes aspects of regulatory guides and inspection reports which are closely related to influence of WWER fuel and equipment design and manufacture quality assurance (QA) on safety analysis reliability and vice versa.

The need for detailed guidance in the performance and review of accident analysis for WWER nuclear power plants has been identified as a priority within the IAEA Extrabudgetary Programme on Safety of WWER and RBMK NPPs. The guidelines [1] have been elaborated to be used primarily by regulatory bodies for the review of accident analysis provided by the operating organisations. The objective of another basic report [2] of the Programme is to present a consolidated list of safety deficiencies, called safety issues, ranked according to their safety significance and the corrective measures to improve overall safety.

The WWER-1000 nuclear power plants are more similar than other reactors of Soviet design to PWRs of western design when considering design philosophy, design features and construction. The design of the model 320 is, in general, consistent with standard international practice for safety systems and safety related systems. The basic safety concept of defence in depth is realised by general design criteria including the use of redundancy, diversity, independence and fail-safe design.

However, operational experience has revealed some deficiencies regarding implementation of engineering design solutions, quality of manufacture and reliability of equipment used, and the consequential need for safety improvements. Other shortcomings reflect deviations from current safety standards which evolved over the last two decades since the original design of WWER-1000 plants.

DEFICIENCIES REGARDING IMPLEMENTATION OF ENGINEERING DESIGN SOLUTIONS, QUALITY OF MANUFACTURE AND RELIABILITY OF FUEL AND EQUIPMENT [REF. 1, 2].

Nuclear and Technical Safety (NTS) work is an interaction between authority and company. The authority has the responsibility for regulation, surveillance and analysis, whereas the company has the operational responsibility ensuring that NTS standards are adhered to.

---

* Federal Nuclear and Radiation Safety Authority of Russia

The nuclear and technical safety standards in company are determined on the basis of authority regulations which represent the minimum level, together with additional requirements laid down by the responsible manager of a company.

Since 1986 companies of nuclear fuel cycle had been prepared and in 1992 they were passed under surveillance of Gosatomnadzor of Russia. Because of this, codes and standards for nuclear fuel safety licensing and regulatory activities are developed only at the moment.

Now such a standard "Special requirements on construction, materials, production, quality and quality assurance of nuclear fuel assemblies for WWER-1000" substitutes for typical the National Standard "Rules of Construction and Safety Operation of Equipment and Pipelines of Nuclear Power Plants"[3] used for other types of NPP equipment of safety class 1 and 2 systems. The first one links the operational safety criteria with parameters (characteristics) of product and manufacturing. This link is deterministic.

One of the task of licensing and regulatory process is to evaluate these deterministic criteria using known fuel defect mechanisms for normal operation, anticipated transients and postulated accidents. But the safety analysis reports (TOB) for WWER NPP's include the reliability analysis of safety class 1 and 2 systems based on generalised data.

OPB-88 [4] requires the analyses of severe accidents for WWER-1000 NPP's. These analyses are not available at many of the WWER-1000 NPP's. The COUNTRY/PLANT SPECIFIC STATUS information is required for transient and accident conditions and scenarios evaluation. The need for accident analyses for safety relates modifications has been recognised, and the related calculations have been performed.

But this information is incomplete and sometimes very general, lacking technical details. It should be farther completed, updated and included in the IAEA database for use by Member States. Therefore, a sub-task is to develop an approach for a revision of the adopted transient and accident analysis which allows to check these analyses at a later date on the basis of data obtained from operating experience and appropriate surveillance results concerning designing and manufacturing.

As a basis for such a surveillance, the following parts of "Special requirements ..." are being considered:

1. The list of safety related calculations and experiments, incorporated initial data and assumptions (safety criteria).
2. Parameters of fuel's specifications corresponding to the above data and assumptions.
3. Methods of reliability (authenticity) analysis of controlled specification parameters (see "Analysis of QA Programs in Licensing Process").
4. Acceptable defect level of these parameters according to initial data and assumptions (see p. 1, 2).

The whys and wherefores of "Special requirements..." is the list of construction parameters (properties, characteristics) of items defined this items in terms of the physical safety barriers.

There are following groups of these parameters:

a) defined by calculation as such,
b) limited by specification, to say, implicitly included in assumptions for safety analysis codes,
c) or implied by manufacture technology, usually that is, left out of account as such.

Regulatory body is interested in analysis of these parameters for scenarios within the design basis (DB) envelope, diminution of group b) parameters, elimination causes concerned parameters belonging to *group c)* or/and their determination (conversion to group b)). There are some typical examples of the parameters of the fuel rod manufacturing.

The internal pressure is parameter belonging to *group a)*. According the national research, as well as JAERI research, the initial fuel rod internal pressure showed the most evident effect for reactivity initiated accidents (RIAs) conditions [5]. During an regulatory inspection a fuel manufacturer was prescribed to put into practice the total measurement of the initial fuel rod internal pressure. Respective technology and equipment are developed. Another typical parameter belonging to *group a*) is permissible depth of pointed pin-hole defects of cladding surface arisen during fabrication. This one is defined from crack generation conditions for high burn-up.

Non-uniform design and test requirements upper and lower welds may be belonged to *group b)*. According normal operation conditions requirements for the upper weld are not so strict. But for transient and (serve) accident conditions such requirements have to be equal. Now this question is under discussion.

Thinnings caused by hand buffing to eliminate pointed pin-hole surface defects of cladding, is *group c)* parameter. It is an example of parameter *conversion from group a) to group c)*. Hand buffing operation was cancelled by regulatory body prescription.

Parameters belonging to group b) and group c) and caused by deficiencies regarding implementation of engineering design solutions, quality of manufacture and reliability of equipment, render single failure criterion (used for the availability of the protection and safety functions in accident analysis) less conservative and may provoke new (serve) scenarios and initial events.

There are two examples concerning main safety functions define as "*protection of the first physical barrier*" and "*cooling the fuel*". Deficiencies in engineering design solutions provoked pump motor failures just after their engaging. The design solution allows for a voluntary rotor location in the standby mode. The failures were caused by touch of the rotor frontal part to the stator. These pumps are used everywhere in safety systems and safety support systems. A failure like that may change accident scenario arbitrarily.

Another example concerns the potential initial events. For a long time there had not been qualification requirements for liquid penetrant examination from cracks of main coolant pump motor flywheel. Regulatory inspection revealed very low probability of the crack exposure. Disbalnce and following fracture of the pump-motor bearing assemblies may have very hard consequences on other pumps and pipelines because of the considerable mass and velocity of the parts. Probability of such an event is not very low for there was a case of bearing fracture of thevertical-shaft induction motor of turbine pipeline pump.

The safety concerns with respect to the treatment of components of WWER-1000/320 NPPs are first, the non-uniform treatment of elements provided to fulfil a given safety function, and secondly, the deviations in the requirements regarding design, manufacture and pre-and in-service inspection from those currently used.

The non-uniform treatment of elements provided to fulfil a given safety function and deviations from current requirements for manufacturing and testing affect the safety provisions at level I of protection. Consequently, all safety functions may be impaired for scenarios within design basis (DB) envelope.

ANALYSIS OF QUALITY ASSURANCE PROGRAMS IN LICENSING PROCESS

It has been found very useful for the regulatory body, as a part of its inspection efforts, to perform periodic evaluations or appraisals of the effectiveness of the licensee's quality assurance program. The main purpose of these periodic evaluations is to determine in an integrated and systematic fashion whether or not the licensee is satisfactorily complying with the quality assurance program requirements imposed by the regulatory body and whether or not the licensee's quality assurance program is effective in providing adequate confidence in the observance of safety criteria.

Product quality audit plan (PQAP), as a part of the Quality Assurance Program, is best suited to the analysis of the program. From the viewpoint of the reliability theory PQAP can be treated as a system and then PQAP operations should be evaluated as this system's elements. Among important measures of reliability is an availability factor - the probability of a unit to operate satisfactorily at present instants of time.

The aim of the surveillance is to analyse the Quality Assurance Programme and PQAP as a part of this program. For such an analysis an availability block diagram is plotted. Such *a block diagram of mechanical strength and leak testing for WWER-1000 fuel rod fabrication* is depicted in the accompanying drawing. The block diagram includes only operations of acceptance inspections.

From theoretical principles of monotonic system reliability [6], availability factor of the system is

$$p_s=[1-(1-p_1)(1-p_2)(1-p_3)(1-p_4)]\cdot[1-(1-p_1)(1-p_2)(1-p_5)]\cdot[1-(1-p_1)(1-p_2)(1-p_6)]\cdot[1-(1-p_1)(1-p_2)(1-p_7)]$$

Thus, using this correlation, it is possible to make rough estimates of availability factor. It comprises 0.69 for one of the real system. Evidently, it is not sufficient because allowable value of the factor has to be not smaller than that achieved by realisation of the "Rules of Construction of Safety Operation of Equipment and Pipelines of Nuclear Power Plants"[3] for systems belonging to safety class 1 and 2 (approximately 0.8).

Availability factors of elements (control operations) may be defined by statistical data base processing. Such a data base for WWER fuel manufacturing are now in the making.

The challenge is to achieve the system of probabilistic estimates, linking controlled characteristics of the product and it's manufacturing process with probability of NPP's operational safety criteria, initial conditions and assumptions of safety analysis .

Along with providing of reliability block diagrams, there is also a possibility of a pictorial rendition of functional behaviour of monotonous systems - that is constructing of so-called fault trees. They also calls for determination of minimal cut and path sets of the systems and are used for PSA.

CONCLUDING REMARKS

It is proposed to continue a study of the influence of WWER fuel and equipment design and manufacture quality assurance on reliability of the safety analysis and vice versa. Continued efforts in the development of statistic and probabilistic methods of quality assurance analysis of design and manufacture activities are needed to maintain an acceptable level of efficiency and credibility. Some methods which are analogous to NPP's PSA approaches may be used.

REFERENCES

[1] Guidelines for accident analysis of WWER Nuclear Power Plants, IAEA-EBR-WWER-01, 1995

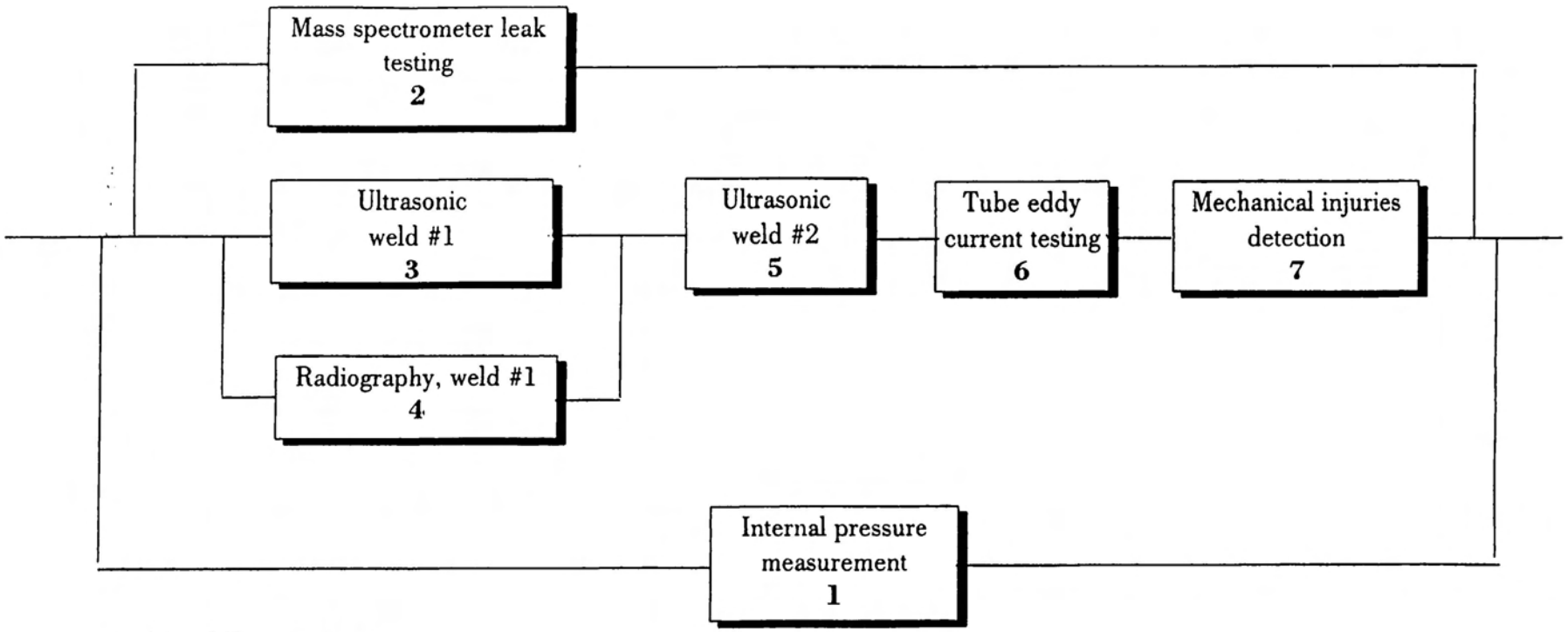
[2] Safety Issues and Their Ranking for WWER-1000 Model 320 Nuclear Power Plants, IAEA-EBR-WWER-05, 1996

[3] PNAE-G-7-008-89, Rules of Construction of Safety Operation of Equipment and Pipelines of Nuclear Power Plants, Moscow (1990)

[4] OPB-88, General Provisions for Enhancing the Safety of NPPs, PNAE-G-I-011-89, Moscow (1989)

[5] Kiyomi Ishijima. Fuel Behaviour in the NSSR Experiments Simulating Reactivity Initiated Accident and Its Application, JAERI, 1996

[6] Frank Beichelt, Peter Franken. Zuverläsigkeit und instandhaltung. Matematische methoden, Berlin, 1983.



7 - Visual Examination

Availability factor of the system $p_s = [1-(1-p_1)(1-p_2)(1-p_3)(1-p_4)] \cdot [1-(1-p_1)(1-p_2)(1-p_5)] \cdot [1-(1-p_1)(1-p_2)(1-p_6)] \cdot [1-(1-p_1)(1-p_2)(1-p_7)]$

Block diagram of the Quality Assurance Program analysis. Mechanical strength and leak testing of fuel rod.