Úrad jadrového dozoru Slovenskej republiky
Nuclear Regulatory Authority of the Slovak Republic

Outline of the Requirements of Application of Computer Based Instrumentation and Control Systems in the Systems Important to Safety on Bohunice NPPs

Jozef Bačurík
Nuclear Regulatory Authority
of the Slovak Republic

Abstract

In the paper the most important regulatory requirements and issues are described related to review, evaluation and assessment of computer based I&C systems important to safety with emphases to safety I&C. These aspects include Safety classification and categorization of I&C, Ranking of applicable codes and standards, Design evaluation on the system level and Software assessment.

Introduction

Upgrading and replacement of the existing Instrumentation and Control (I&C) in the Safety and Safety Related Systems of NPPs by new computer based I&C is one of key issues withing the activites of reconstruction of Bohunice V-1 (VVER 440/2320) and V-2 (VVER 440/213) NPPS, which are aimed at safety and availability improvement of the operating reactor units.

From the regulatory point of view the utilization of computerized, software controlled I&C in safety and safety related applications requires elaboration and establishment of the regulatory approach and policy for review, evaluation and safety assessment of these new digital computer based systems and particularly the software.

In the paper same aspects of evaluation and assessment process, the requirements and criteria are outlined and described which the NRA SR already has applied and mainly intends to apply within I&C upgrading and replacement projects, namely:

- the planned reconstruction of the Reactor Protection System at VVER 440/230, Bohunice V-1 NPP, Unit 1 and Unit 2 using a programmable system TELEPERM XS
- the staged replacement of the ESFAS at VVER 440/213, Bohunice V-2 NPP, Unit 3 by the CEGELEC/ACEC AC 132-16 compurized system (PLC technology)

A. Safety Classification of I&C

Classification of I&C systems according to their importance for nuclear safety is of great importance because requirements and criteria for design, development, manufacturing and operation of I&C are derived in accordance to this safety classification and categorisation. Safety classification of the I&C functions, systems and equipment (FSE) contained in IEC 1226 standard defines three safety category A, B, C according to importance to safety. This standard also defines and specifies the general and specific requirements for the individual categories for assurance of functionality, reliability, performance, environment resistance and QC/QA. This is of great significance for both the supplier and the utility. It is the requirement of the NRA SR that I&C should be classified according to IEC 1226 standard. This regulatory requirement is already applied for improvement, upgrading or replacement of existing I&C within reconstruction activities.

B. Ranking of Applicable Codes and Standards

The regulatory (NRA SR/ÚJD SR) requirements and acceptance criteria for review, evaluation and assessment of I&C important to safety within the licensing process are those defined and specified in applicable codes and standards. There is lack of domestic national standards, codes and regulations and a great amount of the international ones of different sources. It is the reason for ranking of the available codes and standards. This ranking according to the priority of application of codes and standards may be useful in creation and establishment of the regulatory framework and in selection of primary licensing standards.

1. National standards and regulations if available. Regulations of the former Czechoslovak Commission for Atomic Energy (CSAEC) are still applied. The regulations of NRA SR are in the process of development and preparation.

2. IAEA NUSS Codes, Safety Guides and Guidelines.

3. IEC Standards. Standards prepared by Technical Committee No. 45, the Technical Committee for Nuclear Instrumentation of the International Electrotechnical Commission.

4. Standards and regulations of the supplied technology country.

As the supporting standards can be taken:

- IEEE Standards. Standards of the Institute of Electrical and Electronics Engineers.

- Codes and regulations of the other national regulatory bodies as US NRC Regulatory Guides and NUREGs.

C. Design Evaluation

Design evaluation of the safety systems (RPS, ESFAS...) should be done in the early stages of design process. The design concept of the safety system should be evaluated according to qualitative criteria (deterministic approach) and also quantitative criteria (probabalistic reliability analysis). Up to the present the deterministic methods of evaluation and assessment prevail and are considered as decisive, but in the latest time the quantitative methods of the safety and reliability gain on significance. Futher only deterministic methods are mentioned.

Design evaluation of the safety system should include:

1. *Application of Defence-in-depth principle.*

There are some aspects of applying of this principle.

* It is recommended that any applicant for a digital RPS replacement performs a "Defence-in-Depth and Diversity assessment" of the proposed I&C system to demonstrate that vulnerabilities to common mode failures (CMF) have been addressed. Software design errors are considered to be a credible CMF potential which must by specifically included in evaluation.

* If a postulated CMF is capable of disabling a safety function then diverse means, that is unlikely to be subject to the same CMF, shall be required to perform either the same function or a different safety function.

* Diverse and independent digital or non-digital systems are acceptable means. The specific set of equipment required will be evaluated on case-by-case basis.

* Manual actions from the control room is acceptable if an analysis shows that information, not dependent on the computer system and adequate for diagnostic and plant shutdown is available to the operator.

2. *Compliance of the design with applicable standards*

Design of the safety system should be in compliance with the principles, criteria and requirements of applicable standards;
IAEA-50-SG-D3 Protection System and Related Features in Nuclear Power Plants
IEEE 603-1991 Criteria for Safety Systems for Nuclear Power Plant Generating Stations.

Design principles, criteria and requirements contained and specified in the above mentioned standards are applicable on the system level both for conventional analog systems as well as for computer based safety systems. For computerized, software controlled safety systems futher standards should be applied, for the hardware the IEC 987 - Programmed digital computers important to safety for nuclear power station and for software the IEC 880 - Software for computers in the safety systems of nuclear power stations and supplements 1&2 to this standard.

Within evaluation of I&C design concept at least the following criteria and requirements should be examined:

- Single Failure Criteria (SFC)
- Resistance against Common Cause Failures (CCF)
- Completion of protection action
- Equipment qualification
- System integrity
- Channel redundancy
- Independence of trains and channels
- Separation of safety protection system from non safety I&C system
- Testability during operation
- Fail-safe design
- Reliability
- Maintenance and repair

D. Software Assessment

The aim of software assessment of computer based I&C systems important to safety and especially of the safety systems is to demonstrate an acceptable safety and reliability. Up to the present there are no generally accepted means of quantifying the software reliability. Consequently, the safety and reliability required in particular for safety critical software should be based on other methods and techniques that comprise:

* demonstration of the quality of software production within design and development process, including comprehensive checking and testing by the manufacture (verification and validation after completion of every phase of the software design and development proces, validation of the integrated system, different type of testing, factory acceptance test).

* full independent assessment that covers examination and analysis by specialist teams independent of the manufacture to evaluate the quality of the software produced.

* commissioning testing of the installed system in the real on-site conditions and environment.

The independent software assessment should encompass:
- comprehensive manual checking of code and data
- application of the static analysis to the source code
- checking of the correctness of the object code using a specially developed software tools
- use of specially developed dynamic testing facility which applies a large number of randomly generated input combinations to the integrated hardware and software system (random testing).

Static Analysis.

The process of evaluation of a computer program without executing the program. Various techniques can be employed as "desk checking", code audit, inspection, walk through and the use of a static analyser. (ANSI IEEE 729/1983).
The analysis applied to the resulting product of software design and development process, i. e., the executive code, should show that the product meets the requirements (software requirements specification) and in addition to demonstrate that the code does not carry out unintended (unspecified) functions or unsafe actions. The analysis should include both analysis of the functionality of the software and analysis of the safety of the software. Functional analysis should demonstrate that the software performs all required functions and does not perform any unspecified function. The analysis of software safety should demonstrate that the software does not initiate any unsafe actions under operating and also under accident conditions. Software should be designed to incorporate fail-safe and fault-tolerant features.

Software Testing.

Software should be tested to find and remove as many faults as reasonably possible and should also be tested to gain confidence in the safety and reliability of the final product. There are two basic type of software testing, the functional and random testing. Functional testing examines the software with inputs selected to cover the functionality and logic of the software. Random testing examines the system with inputs randomly selected form a realistic operating profile. Test plans (programmes) should be written before test are run and records should be kept of all test runs and results.

Functional Testing.

Should include integration testing and system testing. Functional tests should examine every function of the software. This is of the greatest importance for safety critical software. This type of testing should include also boundary-value cases and cases representing all system hazards. Functional testing should also include checking of the timing, time responses and performance requirements of the software running on the target computer.

Random Testing.

Statistically valid random testing establishes confidence that a product will function without failure under specific operating conditions. Statistical validity should be demonstrated by showing that a large number of independent, randomly selected test cases have been run without failure. The selection of input data for the random tests should represent accurately real operating conditions. The number of tests should be related to the reliability requirement and conditions (targets).
Both functional testing and random testing should be performed, if it is possible, within the real in-plant environment and conditions. During testing, the status of all outputs should be monitored to insure that unintentional actions do not occur. Any errors should be documented and their correction tracked. Errors should be analysed for cause.

Maintainability.

The repair and modification of both software and hardware should only be performed off-line. Mean Time To Repair (MTTR) has an effect on total system reliability and availability, therefore, there should be sufficient spare parts and test equipment and adequately trained staff to enable the proposed figure to be met. Any modifications both in hardware or software should be subjected to a full V&V process. In case of arising a need to change specific system parameters such as trip settings or calibration constants from operational reasons an agreed modification procedure should be provided. The available range should be limited to values specified in safety analysis report. A display of current values or states of such parameters should be provided.

The scope and amount of testing and the different types of testing that are to be included in the individual phases of software life cycle and performed within V&V process, factory acceptance tests (FAT), site acceptance tests (SAT) and during commissioning testing depend on the software reliability and safety requirements (software requirements specification). The tests plans for the individual type of testing and the results of the testing should be submitted to the regulator for review and evaluation. Licensing documentation related to the software analysis and software testing should be elaborated to such an extent and be precise enough to permit systematic review and evaluation by the regulator.

Conclusion

NRA SR approach to licensing of computer based I&C systems important to safety is under development. Up to the present this approach can be characterized as application of domestic regulations together with requirements and criteria of international accepted standards.