XA9949621

APPLICATION OF THE DEFENSE-IN-DEPTH CONCEPT TO QUALIFY COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY

F. SEIDEL
Federal Office for Radiation Protection,
Salzgitter, Germany

Abstract

In parallel to the technological development, the authorities and expert organisations are preparing the application of computer-based I&C to NPPs from the regulatory point of view. Generally the associated world-wide procedure follows steps like identification of safety issues, completion of the regulatory framework particularly regarding the licensing requirements and furthermore, recommendation of an appropriate set of qualification methods to prove that the requirements are met. The papers' intention is to show from the regulatory point of view that the choice as well as the combination of the qualification methods are depending on system design features and development strategy. Similar as for the safety system design required, a defence-in-depth qualification concept is suggested to be helpful in order to prove that the computer-based system meets the licensing requirements.

The implementation of computer-based instrumentation and control (I&C) important to safety into nuclear power plants (NPPs) is proceeding, including both, safety-related application (e.g. reactor power control and limitation) as well as safety-critical functions (e.g. reactor shut down). On base of national and international standards vendors are developing their qualification strategy for computer-based I&C covering the whole I&C system life cycle including the safety categorisation of the distinct I&C functions and associated equipment.

In parallel to the technological development, the regulators and expert organisations are preparing the application of computer-based I&C to NPPs from the regulatory point of view. In Germany, the RSK-guidelines are complemented [1]. Generally the associated world-wide accepted procedure follows steps like identification of safety issues, completion of the regulatory framework and furthermore, recommendation of an appropriate set of qualification methods to prove the requirements. The papers' intention is to show both, the choice as well as the combination of the qualification methods, are dependent on system design features and development strategy; similar as it is required for the safety system design, a defence-in-depth qualification concept is suggested to be helpful in proving the systems appliance against the licensing requirements. As an example to show the regulator's perspective the qualification concept described in [2] is used.

The issues of qualification and licensing of computer-based safety I&C are identified in publications like [3,4], which involve the recent results of international specialists'

meetings. From our point of view, the main issues are listed in Table 1. On the way to establish licensing criteria, the international positions are growing more and more together. For example, deterministic criteria become dominant because of the difficulties in proving high reliability goals. Furthermore, there is a uniform understanding that the qualification methodology has to cover the whole system life cycle and that the I&C critical to safety shall govern the common mode failure.

To prove that the I&C system meets the licensing criteria there are several qualification methods that can be combined regarding different qualification concepts. Consequently, also the qualification concept in [2] varies from other experienced concepts regarding certain aspects as pointed out in Table 1.

From the regulatory point of view following aspects of the concept in [2] are of particular interest:

- According to the nuclear regulatory framework, the safety I&C shall not determine the unavailability of the safety system. Therefore the single failure and the common mode failure are to be governed also by the safety I&C.
- As high reliability goals are claimed for safety critical I&C functions, they can not be proved solely by analytical qualification measures; in addition, constructive as well as administrative qualification measures should be applied.
- A defense-in-depth concept is applied for qualification: During design and implementation phases, faults can be avoided by application of approved methods of quality assurance; after each phase of the life-cycle model. The most remaining faults will be detected and eliminated applying analytical qualification measures. In the last level of the defense-in-depth concept, constructive qualification measures are responsible for failure tolerance; for details see Table 2.

Within the defense-in-depth qualification concept, constructive and analytical qualification measures will be combined dependent on the distinct life-cycle phases, and the results of previous phases will be taken into account during later phases. For instance, it is suitable to execute the distinct functions of reactor protection by small software modules with strong restricted functionality (constructive measure). Such modules can be verified nearly completely, e.g. in the frame of type testing. Consequently these modules can be treated to be exact in the following qualification steps. Taking advantage of this, the analytical qualification effort in later phases can be reduced significantly. As a further analytical measure, the software modules are coupled for executable software routines using specification and coding tools on base of a graphical specification language. Due to these measures of fault avoidance, the integration tests can be restricted to essential test cases as well as robustness tests, by which the deterministic functional behaviour of the I&C system is demonstrated to be not susceptibly to random input signals. To our opinion this test strategy has the potential to lead to a sufficient test coverage. Particularly this strategy may be helpful in the case that the spectrum of all possible scenarios following failures and disturbances is too extensive for detailed testing.

Primarily, the German qualification concept takes into account deterministic requirements and the quantification of software reliability is not necessarily required. Anyway,

the process of hidden software faults are becoming active is not of probabilistic nature. In the case there is a hidden software fault, it is present permanently and not caused by a temporary mechanism like ageing. Because a hidden software fault mostly will become active only if a seldom parameter configuration occurs, the activation wrongly seems to follow a stochastic process. Instead of reliability in the quantitative meaning, dependability requirements are more useful for the software licensing process. Constructive requirements like redundancy or diversity are contributing to dependability.

Nevertheless, also in the German qualification concept an I&C system reliability analysis is involved, particularly in order to prove the balance of the I&C system design. Because of the accuracy of the reliability analysis results is mainly dependent on derived data from operational experience, in future such data will be gained using the safety I&C for safety related functions, e.g. from the modernised reactor power limitation and control systems. In order to ensure that future reliability assessments will be successful, the aspect of data collection should be stressed in more detail. Therefore, the data collection should be completely built up as well as appropriately structured in order to derive the necessary data for reliability analysis including the main data to characterise the plant status and spent time for corrective actions, etc. An other topic of reliability analysis consists of establishment of an appropriate reliability model in order to consider the common cause failure. Such models are in developing state.

The qualification concept in [2] supports the design goal, that the I&C system is applicable to different reactor systems. Due to the I&C modularisation, type testing of software and hardware modules as well as the application of a graphical design language, a flexible adaptation of the I&C system is possible with moderate effort in design and qualification. We think, this basic concept is even useful in order to qualify the I&C in the frame of modernisation of older plants with distinct design.

In order to optimise the qualification effort, in [2] it is assumed that a great portion of the qualification effort will be spent for type testing (static analysis and functional testing of modules), and furthermore, that the functionality of the I&C system can be demonstrated to be correct regarding the requirements specification of a representative part of the I&C system (like modules for the one complete signal processing line from sensors over signal processing, voting (e.g. 2v3) till safety system actuation). From the regulatory point of view such qualification steps can support the general understanding of the functional and non-functional properties of the I&C system. On the other hand, regarding a distinct I&C application, this step can not substitute the functioning testing for the complete system. System functioning testing mainly consists of simulation, test field testing and on-site testing. Coming back to the defence-in-depth concept of qualification, constructive qualification measures can be used to postulate the most probable system behaviour for operational and accidental modes, in order to select the main test cases and predetermine the test and simulation results.

Regarding software, the above described qualification concept is particularly suitable to application-specific software. Regarding codes of the shelf (COTS), mostly the main steps of development are finished before the COTS will be implemented in a plant simulator or even in the plant. Often the former qualification measures are not traceable. Methods for post-delivery qualification of COTS are in developing state.

In the frame of associated research projects of the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety *(Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit - BMU)* following aspects are considered particularly:

- Proposals for the further elicitation of harmonised international safety requirements on computer-based safety I&C
- Approaches towards a general qualification concept in order to prove computer-based safety I&C against these safety requirements
- Gain generic plant-non-specific conclusion from experience in I&C modernisation of existing plants
- Elicitation of qualification requirements for the safety-related use of application-specific I&C (ASIC) in NPP.

[1] RSK-Leitlinien für Druckwasserreaktoren, 3. Ausgabe vom 14.10.1981, Neufassung des Kapitels 7, Elektrische Einrichtungen des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung", Bundesanzeiger, 23. August 1996

[2] H.-W. Bock, Governing of Common Cause Failures, Proceed. of IAEA Specialists' Meeting on Computerised Reactor Protection and Safety Related Systems in Nuclear Power Plants, Budapest, Oct. 1997

[3] Results of Workshop and Special Issue Meeting on Technical Support for Licensing of Computer Based Systems Important to Safety - Final Draft; OECD/NEA; Issy-le-Moulineaux, May 1996

[4] European Nuclear Regulators' Current Requirements and Practices for the Licensing of Safety Critical Software for Nuclear reactors, European Commission, Nuclear Science and Technology, draft Report Version 8, EUR 18158 EN, Luxembourg 1998

Issue	Aspects of the German Qualification Concept	Aspects of Further Harmonisation of Qualification Requirements
Regulatory framework: guidelines, standards	Extended RSK-guidelines; KTA-Standards with detailed requirements, but without distinct requirements on computer-based systems	International standards (e.g. IEC) are not mandatorily involved into the German nuclear regulatory framework; Guidelines for European Pressurized Water Reaktor (EPR) being in discussion
Categorisation of I&C functions	Categorisation of functions and equipment according to RSK-guidelines [1]	Mostly categorisation of functions and equipment according to IEC 1226; or just categorisation of equipment; in certain cases categorisation involves uncertainties (e.g. manual emergency safety features actuation); different plant safety goal concepts
Common cause failure (CCF); diversity	CCF is supposed to one of several (2 or 3) systems processing diverse signals; functional diversity as the main precaution against CCF; deterministic cyclic-asynchroneous processing mode; defense-in-depth qualification concept	World-wide, there are different design concepts, including e.g. - functional diversity - analogue or digital backup - diverse safety-related functions performed by operational I&C as well as different qualification concepts
Quantitative reliability requirement	No distinct licensing criterion, however, a reliability analysis is recommended	In some countries quantitative licensing criteria are established; there are controversial discussions regarding the proof of this criteria approaches to reliability analysis being under dicussion

Table 1: Aspects of further harmonisation of qualification requirements on computer-based safety instrumentation and control

Issue	Aspects of the German Qualification Concept	Aspects of Further Harmonisation of Qualification Requirements
Qualification of application specific software	Structured according to life cycle; in general tool-supported; graphical specification language; type testing applied also to SW	World-wide: tool support; different methods for SW-qualification, e.g. with different ratio of static analysis to testing; different positions regarding the application of formal methods; independend assessment
Qualification of codes of the shelf (COTS)	Focal point: operating systems and data transmission	Concepts for qualification and proof of dependability are in developing state
Qualification of tools	Focal point: target software testing; combination of several development steps on the way to software implementation	Either the tool or the target software is subject to verification
System qualification	Early testing of system design specification (e.g. using a one-unit workstation); lab tests at a representative test bay; random testing; on-site commissioning and testing; comprehensive application of self-monitoring	World-wide structured according to life-cycle model; different combination of (in general) comperable qualification methods; there aren't any distinct criteria to terminate testing at sufficient coverage; random testing and/or detailed failure analysis
Operational experience regarding computer-based I&C	In application to safety-related (non-critical) functions like reactor power limitation	International exchange of experience is very useful, particularly regarding safety-critical applications; experience gained using non-safety applications are of limitted value; requirements on log, e.g. in order to support later reliability analysis;

Tabelle 1: Aspects of harmonisation of qualification requirements on computer-based safety instrumentation and control (continuation)

Defense-in-depth Concept	Constructive Measures	Analytical Measures	Administrative Measures
Fault avoidance	Categorisation of I&C functions; simple Hardware/Software (HW/SW) construction; deterministic functionality	Application of a (graphical) specification language; general tool support for SW development	Accepted/certified quality assurance methods for SW/HW-development; complete documentation of HW/SW-development and application (manuals); configuration management
Fault detection and removal	Constructive precautions to ensure the system testability	Comprehensive verification and validation according to life-cycle model; application of formal or semi-formal methods; type testing applied to HW and SW; simulation; representative off-site test bay; commissioning tests, maintanance	Independence of I&C development and qualification; complete test documentation (including findings); audition; configuration management
Failure tolerance	Redundant trains are spatial and energetical decoupled; (functional) diversity; state-independent computer operation (e.g. due to cyclic-asynchroneous operating mode)	Comprehensive I&C self-monitoring during operation, together with fail-safe failure reactions	

Table 2: Defense-in-depth qualification concept (selected qualification marks)