UDC 004.41

HORST MIEDL, JOSEF MÄRTZ, GÜNTER SCHNÜRER

Institute for Safety Technology (ISTec) GmbH, Munich, Germany

QUALIFICATION OF INTEGRATED TOOL ENVIRONMENTS FOR NUCLEAR APPLICATIONS

Due to technical reasons Instrumentation and Control (I&C) systems have to be replaced to an increasing degree by computer-based I&C systems. For the development and implementation of safety-related computer-based I&C systems Integrated Tool Environments (ITE) are employed. Most of these ITE were not conceived originally for the implementation of nuclear specific applications. The quality of the ITE may be proven and certified for industrial applications but the qualification for the nuclear application has to be demonstrated. This paper proposes an assessment method and activities for the efficient and transparent qualification of ITE for the use in safety-related applications according to nuclear standards and state of the art. The assessment aims at a pre-qualification of ITE detached as far as possible from the safety functions implemented by them. The results of this pre-qualification shall assist and facilitate the safety analysis of the application software.

Instrumentation and Control systems, software, safety-related applications

Introduction

Due to technical reasons Instrumentation and Control (I&C) systems of nuclear power plants (NPP) have to be replaced to an increasing degree by computer-based I&C systems. For the development and implementation of safety-related computer-based I&C systems Integrated Tool Environments (ITE) are employed. Most of these ITE were not conceived originally for the implementation of nuclear specific applications. The quality of the ITE may be proven and certified for industrial applications but the qualification for the nuclear application has to be demonstrated.

This paper proposes an assessment method and activities for the efficient and transparent qualification of ITE. It is based on the analysis and classification of services which represent the functionalities of the integrated tool environments in form of software packages (e.g. software packages for specification, code generation, etc.).

The assessment of the ITE is carried out in a staggered approach. In a first step compliance with general requirements for the design of ITE are analyzed. These requirements have been derived from the experiences of assessments of ITE, conceived explicitly for the use in safety systems of nuclear facilities. These requirements are essential to establish the fundamental features of ITE. Aim of that analysis is the earliest possible determination of its basic suitability.

After an affirmative result a detailed investigation of the services of the ITE is performed in the subsequent steps in order to locate potential deficiencies and to evaluate compensating measures. In the second step requirements on the selection and use of ITE are taken as assessment basis. Dependent on the safety category of the target system implemented by the ITE international standards, e.g. IEC 62138, supply these requirements.

In the final step, after successful termination of the second step, a systematic approach is defined to weight the safety relevance of the ITE's services. Services with direct or indirect impact on the target system may address different requirements. It can be assumed that services that have a direct impact on the target system can be classified as pre-developed software. The analysis is based on the requirements and the procedure for pre-developed software as described in the international standard IEC 62138.

Qualification possibilities

The following chapter discusses the qualification possibilities with respect to ITE. The analysis and clas-

sification results of ITE of different I&C platforms are presented and methods to qualify the ITEs' services are addressed.

Analysis and classification of ITE. ITE of different I&C platforms have been analyzed and classified in services that represent their functionalities in software packages. The classification is carried out in services for:

- Project control: e.g. versioning of program elements, release management, control of project progress.
- Project documentation: e.g. automatic generation of project documents, consistent development recording, and tracing of assessment activities.
- Requirements capturing and tracing: e.g. documentation and management of functional and non functional requirements.
- Hardware development environment: e.g. hierarchical design of hardware arrangement and network diagrams.
- Software development environment: e.g. graphical or model-based specification method for the implementation of the safety functions.
- Code generation: e.g. automatic generation of the program code of the safety functions from the specification.
- System software: e.g. function blocks, operating system, self tests, input and output drivers.
- Qualification tools: e.g. tools for verification and validation, debugger, simulator.
- Maintenance: e.g. assistance in the execution of periodic tests, in the implementation of adjustments at the target system and in the error diagnosis.
- Safety features: e.g. error and failure control by redundant and/or diverse design.
- Security features: e.g. access management, prevention of unauthorized intervention.
- Help system: e.g. syntax-driven editor, online help system.
- Communication: e.g. communication protocols.

The table 1 shows the data of four tool sets, ITE-1 to ITE-4, of I&C platforms that have been investigated. The first column contains the services listed above.

Qualification methods. Nationally as well as internationally, several approaches are recommended for qualifying software. Qualification possibilities refer to the developer, the development process, the product, the V&V (verification and validation) and the product's operating experience.

In the case of ITE the qualification focuses on the product. The qualification of the developer is often no more possible due to the project history of the ITE. The same applies for the qualification of the development process. The qualification of the ITE on the basis of operating experience proves to be difficult because of changing application profiles.

Though the specification-compliant behavior of software can be demonstrated by tests, this is costly in practice and not feasible for ITE. For the qualification of predeveloped program parts testing is not sufficient. Besides testing of correctness and robustness, a set of supplementary and additional program analyses should be provided for providing evidence of the required quality.

Basically, the qualification of software products distinguishes between constructive and analytical methods. The qualification of ITE focuses upon analytical methods because they are pre-developed software products and not to be newly developed. At the same time, the type and the intensity of the qualification methods depend on the safety requirements of the product to be implemented with it.

Qualification of ITE

This chapter explains the assessment method and activities for the qualification of ITE. This comprises the definition of general requirements for the design of ITE, the classification of I&C functions according to IEC 61226, the weighting of services according to their influence on the safety function and the procedure for the qualification of the ITE.

General requirements for the design of ITE. Based on the experiences of assessments of ITE, conceived explicitly for the use in safety systems of nuclear facilities (e.g. ITE-4), general requirements for the design of ITE have been derived for the assessment framework. These requirements are essential to establish the fundamental features of ITE.

Table 1

Classification matrix

	ITE-1	ITE-2	ITE-3	ITE-4
Project control	Documentation support of project history and program version changes	Support of project management along the phases: realization, commissioning and operation.	Set of generic documents	Software plans and V&V procedures according to software lifecycle
Project documentation	Data sorting and documentation of project elements	Documentation with lists and directories	Engineering Station with documentation facilities	No information available
Requirements capturing and tracing	Requirements capturing available	Requirements capturing implicitly with project control	No information available	Tools for requirements capturing and tracing available, not part of ITE
Hardware development environment	Configuration editor	Planning of system hardware	Database elements	No information available
Software development environment	Specification by means of function block diagram (FBD), structured text (ST) and/or ladder diagram (LD)	Specification by graphical interface using function blocks	Specification by graphical language (function blocks), elements for process control and structural elements	Specification by means of function block diagram (FBD), sequential function chart (SFC) and/or ladder diagram (LD)
Code generation	Yes, staggered approach	Yes	Yes	Yes
System software	Libraries of basic functions	Function blocks	Function blocks	Kernel of operating system is based on COTS software
Qualification tools	Control panel for emulation, testing and debugging	Diagnosis system for surveillance and error handling	Engineering Station as service unit for testing and simulation	Data monitor for surveillance of variables and addresses
Maintenance	Support of fault diagnosis and performing maintenance operations	Services for downloading application programs into the target system	Engineering Station as service unit for online modifications	Download of target software
Safety features	Redundancy; Display of system status and monitoring of program execution	Redundancy; Operation and surveillance of the plant with the process control and information system	Redundancy; Asynchronous execution units, Engineering Station as service unit for surveillance	Redundancy; Surveillance and test of the target system
Security features	Definition of users and their privileges	Access protection with user name and password; licensing of certain functions	Password protection, program checksum, restricted network programming	No information available
Help system	Online help system	Online help available	No information available	Online help system foreseen
Communication	Communication between controllers via proprietary network; distributed control system with different interfaces (e. g. Ethernet)	Bus system for communication between the subsystems of the process control system	Three types of communication; network communication with fieldbus, serial communication with high-speed link and external communication with Ethernet	Ethernet to processing units; Profibus between processing units

The features should be available and should implement services of sufficient quality. An important aspect is the coherence of the services with respect to the software lifecycle. The following table 2 lists the general requirements for the design of ITE and gives a short explanation.

Classification of I&C functions. In nuclear regulation I&C functions are categorized according to their importance to safety. The international standard IEC 61226 [2] establishes criteria to assign functions of safety I&C to categories that designate the different importance to safety of the function. Thus, the categorization represents the safety relevance of I&C functions.

There are defined three categories A, B and C. Functions of category A have the highest safety relevance. Functions not belonging to one of the categories have no safety relevance and are called “not categorized”. The assignment of the functions is mainly determined by their contribution to avoid or control postulated initiating events and to mitigate their effects.

The category assigned to a function determines general and specific technical requirements. These require-

ments influence the use and the qualification of the ITE employed to implement safety functions. The IEC 61226 establishes requirements to ensure functionality, reliability and environmental durability as well as quality assurance and control. It states explicitly to use equipment with a documented, proven history of reliable operation in nuclear or other industrial applications, wherever possible.

Table 2

Requirements for the design of ITE

Requirement	**Explanation**
Software development according to life cycle	The development of the application programs should follow a software life cycle divided into clear defined phases. Each phase should be provided with quality assuring measures. Means for the verification of the phase transitions should be at disposal.
Configuration management	Services should be available for the capturing and control of components necessary for implementing the target system.
Software maintenance	Periodic tests and changes to the target system should be supported.
Formalized design methods	The design methods should be formalized and intelligible for all project parties.
Automatic code generation	Application code implementation requires services for the automated code generation.
Limitations to "manual" software (e.g. compliance with programming rules, etc.)	Manually implemented application code should be avoided. If necessary, the code should be designed as clearly arranged and completely testable modules. The modules should operate sequentially as far as possible.
Automated verification tools	Services for automated verification of all software components should be at disposal.
Constraints in operating system (e. g. static, etc.)	Operating system components of the target system should be comprehensible and approved. Dynamic resource management should be rejected.
Deterministic program behavior	The processes of the target system should operate cyclically. Interrupts should be avoided to attain deterministic program behavior. Sufficient reserves should be planned for self tests and batch processing.
Extensive system tests	Extensive system tests should be performed in order to obtain the highest possible test coverage.
Possibility of diverse measures	Program parts in redundant processing units should be implemented with different tasking sequence and memory allocation.
Independence of redundancy	Synchronization of redundant processing units should be renounced.
Adequate error handling	Dependent on the recognized error (e.g. runtime error) the target system should initiate error-tolerating measures or enter a fail-safe status.

Weighting of services. The services of the ITE are mainly based on pre-developed software and commercial off-the-shelf (COTS) products. For the assessment of the quality a systematic approach is defined for weighting of the safety importance of the services of the ITE.

First, the services are distinguished according to their usage in:

- services directly affecting the target system;
- services indirectly affecting the target system.

It is of essential importance for the qualification whether the services:

- are executed online in the safety-relevant target system;
- generate online software;
- provide offline assistance.

Services that influence the target system directly (e.g. pre-developed function blocks) are categorized just as the safety function they contribute to.

Services generating online software for the target system that cannot be verified thoroughly have to be qualified comparable with the requirements of the safety category of the generated software.

A lower category may be selected if outputs of the services are comprehensible and verifiable. For example outputs of a code generator can be verified with static or dynamic analysis in addition to tests. An independent tool for the verification of the generated code is highly recommended. Although, tests are indispensable and always done in practice they are estimated to be not sufficient for the qualification of computer code. This has to be taken into account especially in the situation of automatic generated code. Services that provide offline assistance are often considered as not classified. Characteristically for that category are for example services for methodical design specification, automatic document generation or verification and validation.

Qualification procedure. The basic data for the qualification are the services of the classification matrix presented in table 1. The grading concerning the safety relevance illustrated in chapters 3.2 and 3.3 is reflected

in staggered requirements for the quality and reliability of the corresponding services. Compliance with these requirements is the criteria for acceptance of the ITE for the use in the respective safety category.

Necessary methods and actions are composed according to the requirements of the different safety categories. The differences in the compositions of the safety categories render a basis for extracting those methods and actions which should be applied for changeover from one safety category to another.

The qualification of the services of the ITE is carried out in three main steps (fig. 1). In a first main step compliance with general requirements for the design of ITE are analyzed. Aim of that analysis is the earliest possible determination of its basic suitability.

Before the assessment can be started the unique identification of the services – as relatively formal but important step - has to be carried out. A qualification process can only take place if it is applied to uniquely defined qualification items. This means that code and corresponding documentation are unambiguously identifiable and in close relation. Furthermore, they have to be controlled by configuration management from the very first and also later in case of modifications.

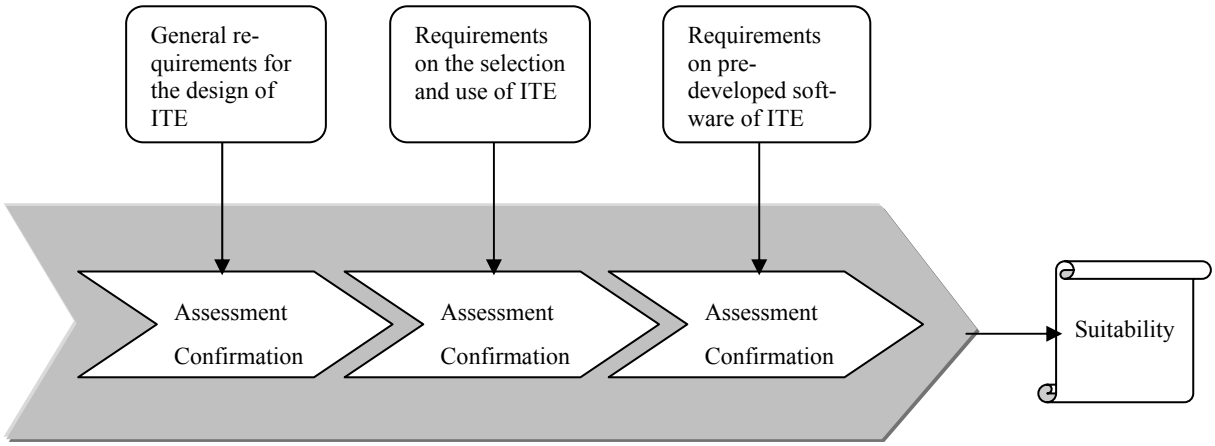

Fig. 1. Qualification procedure

After an affirmative result of the assessment of the general requirements a detailed investigation of the services of the ITE is performed in order to locate potential deficiencies and to evaluate compensating measures. This qualification takes place in the next two main steps

Dependent on the safety category of the target system implemented by the ITE the international standard IEC 62138 [1] supplies requirements on the selection and use of ITE. These requirements are applied to the services and assessed accordingly in the second main step.

After successful termination of the second main step, the services of the ITE that have an impact as pre-developed software on the quality of the target system are finally analyzed in detail dependent on their safety relevance.

The analysis is based on the requirements of the international standard IEC 62138 [1] on pre-developed software and on the process for providing evidence of correctness for pre-developed software described in the standard.

Ideally, pre-developed software should perform in a new environment exactly the same functions for which it was developed, according to the same quality requirements. But this is not the case in many real world applications. Therefore, one or more of the following facts have to be taken into account:

– Missing elements of the development process.

– Lacking product documentation or insufficient quality of it.

– Past operational profile different to new application.

– Only a (small) part of the pre-developed software is needed in the new application (unused code).

– Unknown functionality in the pre-developed software (not documented functions).

The advantage of pre-developed software may be a widespread and/or frequent use with positive result.

That means a long operational time free of failures or with admissibly few failures. Such operational times can only be stressed if

– sufficient data material has been collected;

– the data collection has been assessed as dependable and

– the evaluation of the data has been carried out with statistical validity.

The confirmation of such times of operational experience can partly substitute lacking documentation. Furthermore, there is the possibility to reproduce lacking documentation of properties and development phases of the product with the help of reengineering techniques.

Conclusions

Different ITE have been investigated and classified according to their services. These ITE provide methods that the designer is aware and which help him finding his way easily. For the use in nuclear projects with safety relevance additional requirements have to be fulfilled.

The single phases of the software lifecycle are supported in different depth. Support for the requirements phase is lacking. That concerns the formal description of both requirements and restrictions. The assistance of the validation phase concentrates on the debugging and simulation of the application software within the ITE.

None of the investigated ITE provides means for the management of test data and test results and the recording of test runs. Possibilities to generate and deduce test data, test cases and test requirements for the test at the target system are also not provided.

Experiences gathered so far point out that the technical value of an ITE is not the only crucial factor rather their qualified application has to be assured.

A scientifically sound assessment framework has been developed that allows a comprehensive qualification of ITE with respect to their suitability for the application in safety-relevant domains. The capability of the assessment framework has been validated with an ITE of an I&C platform.

As example application a power range monitoring system of a nuclear installation has been considered.

Where required, additional independent qualification tools has been identified, implemented and tested as prototypes.

It has not been the intention to qualify an ITE within the project but selected examples of different ITE have been used to demonstrate the suitability and significance of the methods developed.

Acknowledgements

The project has been funded by the German Federal Ministry of Economics and Technology under the project number 1501280. It has been conducted by the Institute for Safety Technology (ISTec) GmbH as project manager, together with the technical service organization TÜV NORD SysTec as subcontractor, and the Institute for Energy Technology (IFE).

References

1. IEC 62138, “Nuclear Power Plants – Instrumentation and Control important to safety – Software aspects for computer-based systems performing category B or C functions”. – 2004.

2. IEC 61226, “Nuclear Power Plants – Instrumentation and Control systems important to safety – Classification of instrumentation and control functions”. – 2005.

3. Miedl H. “Qualification of Integrated Tool Environments (QUITE) for the Development of Computer-Based Safety Systems in NPP”, EHPG Meeting at Sandefjord. – Norway. – 2004.

4. Miedl H., Märtz J. “Qualification of Integrated Tool Environments (QUITE) for the Development of Computer-Based Safety Systems in NPP”, NPIC&HMIT Conference at Albuquerque, USA. – 2006.

Поступила в редакцию 16.02.2007

Рецензент: д-р техн. наук, проф. В.М. Харченко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков.