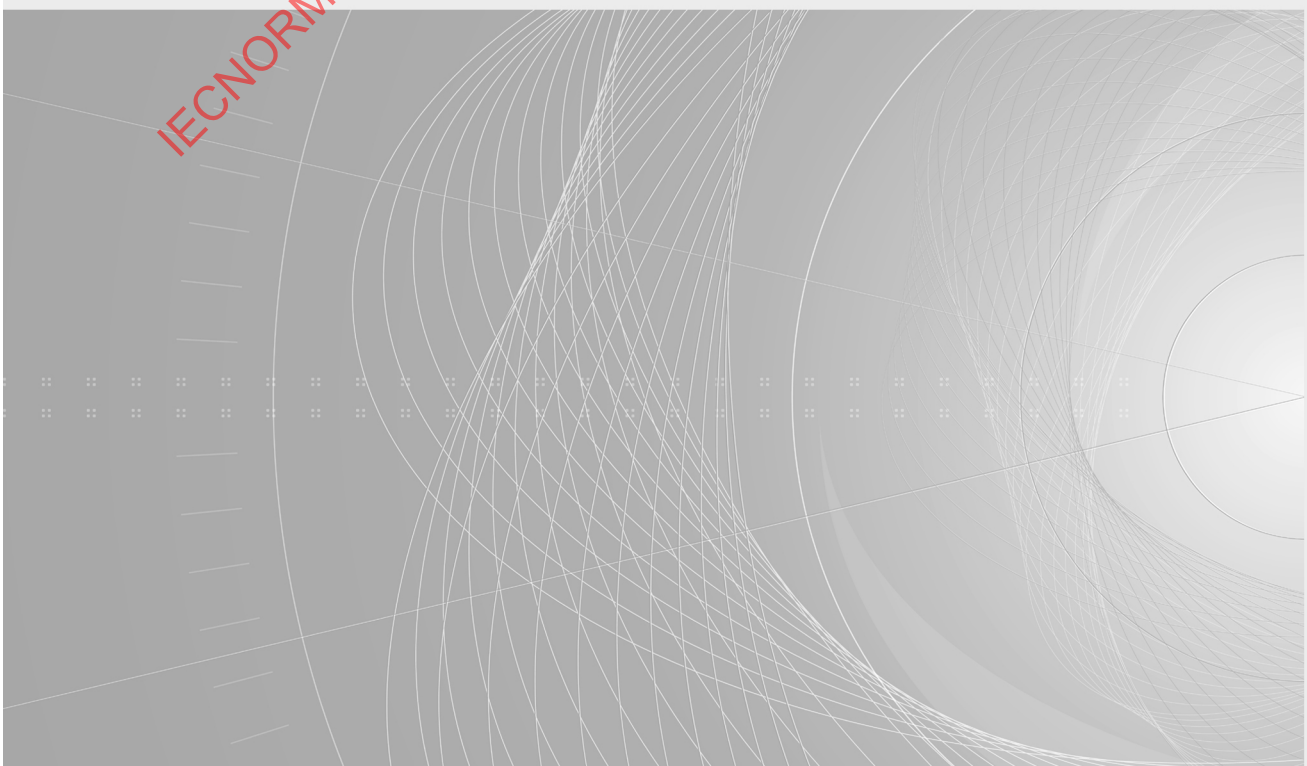
IEC TR 63084

Edition 1.0 2017-06

TECHNICAL REPORT

colour inside

Nuclear power plants – Instrumentation and control important to safety – Platform qualification for systems important to safety



IEC TR 63084:2017-06(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing 20 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
65 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC TR 63084

Edition 1.0 2017-06

TECHNICAL REPORT

colour inside

Nuclear power plants – Instrumentation and control important to safety – Platform qualification for systems important to safety

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-4316-9

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – PLATFORM QUALIFICATION FOR SYSTEMS IMPORTANT TO SAFETY

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC TR 63084, which is a technical report, has been prepared by subcommittee 45A: Instrumentation, control and electrical systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
45A/1106/DTR	45A/1141/RVDTR

Full information on the voting for the approval of this technical report can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Technical background, main issues and organisation of the Technical Report

It is recommended that platforms are used for the development and implementation of I&C systems. These platforms are understood here as a set of hardware and software components that may work co-operatively in one or more defined architectures (configurations).

Some I&C platforms were not conceived originally for the implementation of nuclear specific, safety applications. These I&C platforms have been proven and certified for industrial applications but the qualification for the nuclear safety application has to be demonstrated.

There are standards within SC 45A and in particular WG A3 which cover the development and qualification of computer-based systems and the corresponding application functions. However, it is not clear how the standards from SC 45A can be used on the qualification of I&C platforms.

Other relevant standards of SC 45A are in WG A7 (safety categories) and in WG A9 (qualification of electrical equipment).

Annexes are included to illustrate the approaches applied in different countries and their experiences.

This Technical Report is written to support decision makers related to the issues, goals and results of the platform qualification and the system qualification.

b) Situation of the current Technical Report in the structure of the IEC SC 45A standard series

IEC 63084 as a technical report is a fourth level IEC SC 45A document.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the Technical Report

It is important to note that a technical report is entirely informative in nature. It gathers data collected from different origins and it establishes no requirements.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies' documents (IAEA, ISO)

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPP; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, equipment qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and

in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPP), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPP, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPP, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPP and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA). At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, regarding control rooms, IEC 60964 is the entry document for the IEC SC 45A control rooms standards and IEC 62342 is the entry document for the IEC SC 45A ageing management standards.

NOTE It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC SC 45A to decide how and where general requirement for the design of electrical systems were to be considered. IEC SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 is now launched to cover this objective. When IEC 63046 will be published this Note 2 of the introduction of IEC SC 45A standards will be suppressed.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – PLATFORM QUALIFICATION FOR SYSTEMS IMPORTANT TO SAFETY

1 Scope

1.1 General

This Technical report provides an assessment framework and activities for efficient and transparent qualification of I&C platforms for use in nuclear applications important to safety, according to nuclear standards and state of the art. The assessment aims at a pre-qualification of I&C platforms outside the framework of a specific plant design. Qualification is assumed to be pre-requisite for allowing the particular I&C platform to be used for implementation of the safety classified I&C system. It is to enable parties implementing particular plant specific I&C systems to concentrate on application functions, while for basic system functions to rely on platform qualification.

The I&C platform qualification is based on evaluation of the hardware and software functions provided by the platform ensuring safe and cost-effective life-cycle support of I&C systems. That would include tools for software engineering and software development (software module libraries), code generation, validation, maintenance, etc.

Basic means of equipment qualification, as prescribed by the IEC/IEEE 60780-323, are through analysis, type testing and documented operational experience. Other documents applicable for qualification for nuclear use include IEC 61513, IEC 60880, IEC 62138, IEC 62566, IEC 62671 and IEC 61226.

The features of the I&C platform to be qualified will be identified in requirements on the I&C platform. The requirements can vary, but in essence are based on suppliers' claims on the product scope and functionality. Those claims are normally given in platform documentation such as system descriptions and supplier's requirements for design, implementation, verification & validation. They are all based on the appropriate IEC SC 45A standards and national regulations.

1.2 Framework

This document is organized as follows:

- Clause 5 addresses the role of the platform qualification, including the conceptual design and the documentation constituting the basis for the process of platform qualification.
- Clause 6 is the main clause of this document addressing the process and methods of platform qualification. Crucial aspects of documentation and maintenance of the qualification are included.
- Clause 7 addresses platform elements necessary for safe and efficient implementation and life cycle support of plant-specific I&C systems.
- Aspects of the I&C platform qualification are further developed and exemplified in annexes. Annex A lists licensing issues of the Finnish licensing approach. Annex B discusses the qualification of Areva's TELEPERM XS platform, actualized with notes on qualification from the Finnish Olkiluoto 3 NPP. Annex C discusses the qualification of Westinghouse's FPGA-based platform of modules type ALS (Advanced Logic System). Annex D discusses the qualification of CTEC's digital platform FirmSys for use in systems important to safety in NPP. Annex E discusses the qualification of SOOSAN ENS's POSAFE-Q platform. Annex F discusses the qualification of Rolls-Royce's digital safety I&C platform Spinline in the framework of the type approval for the ELSA project. The five examples given in Annexes B to F are all of platforms developed for nuclear application.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC/IEEE 60780-323:2016, *Nuclear facilities – Electrical equipment important to safety – Qualification*

IEC 60880:2006, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 62138:2004, *Nuclear power plants – Instrumentation and control important for safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62566:2012, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IEC 62645:2014, *Nuclear power plants – Instrumentation and control systems – Requirements for security programmes for computer-based systems*

IEC 62671:2013, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

IAEA SSG-39:2016, *Specific Safety Guide: Design of Instrumentation and Control Systems for Nuclear Power Plants*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1
application software library
collection of software modules implementing typical application functions

Note 1 to entry: When using pre-existing equipment (here platform), such a library is considered to be part of the system software and qualified as such.

[SOURCE: IEC 61513:2011, 3.3, modified – The parentheses "(here platform)" have been added to Note 1 to entry.]

3.2
assessment
systematic process that is carried out throughout the design process to ensure that all the relevant safety requirements are met by the proposed (or actual) design

Note 1 to entry: See independent assessment in 3.10 below.

3.3
audit
planned and documented activity performed by qualified personnel to determine by investigation, examination, or evaluation of objective evidence, the adequacy and compliance with established procedures, or applicable documents, and the effectiveness of implementation

Note 1 to entry: The term refers here to internal or external control of organisations on quality management, project management, and all other issues concerning safety requirements on nuclear processes.

Note 2 to entry: It is further assumed that the audited organisation provides "auditable data", i.e. technical information which is documented and organized in a readily understandable and traceable manner that permits independent review of the inferences or conclusions based on the information (see IEC/IEEE 60780-323).

3.4
automated code generation
function of automated tools allowing transformation of the application-oriented language into a form suitable for compilation or execution

[SOURCE: IEC 60880:2006, 3.5]

3.5
commissioning
process by means of which systems and components of facilities and activities, having been constructed, are made operational and verified to be in accordance with the design and to have met the required performance criteria

Note 1 to entry: Commissioning may include both non-nuclear/non-radioactive and nuclear/radioactive testing.

[SOURCE: IAEA Safety Glossary, 2007 edition]

3.6
equipment platform
set of hardware and software components that may work co-operatively in one or more defined architectures (configurations). The development of plant specific configurations and of the related application software may be supported by software tools. An I&C platform usually provides a number of standard functionalities (e.g. application functions library) that may be combined to generate specific application software

Note 1 to entry: An I&C platform may be a product of a defined manufacturer or a set of products interconnected and adapted by a supplier.

[SOURCE: IEC 61513:2011, 3.17, modified – The term "equipment family" has been replaced by "equipement platform" and by "I&C platform" in the definition. Note 1 and 3 have been removed and Note 2 has been adapted to I&C platform.]

3.7
Hardware Description Language
HDL
language used to formally describe the functions and/or the structure of an electronic component for documentation, simulation or synthesis

Note 1 to entry: The most widely used HDLs are VHDL (IEEE 1076) and Verilog (IEEE 1364).

[SOURCE: IEC 62566:2012, 3.6]

3.8
HDL-Programmed Device
HPD
integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools

Note 1 to entry: HPDs are typically represented by ASICs, FPGAs, PLDs or similar micro-electronic technologies.

[SOURCE: IEC 62566:2012, 3.7, modified – Notes 1 and 2 have been removed and Note 3 has been modified.]

3.9
I&C System
system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself

The term is used as a general term which encompasses all elements of the system such as internal power supplies, sensors and other input devices, data highways and other communication paths, interfaces to actuators and other output devices (see Note 2). The different functions within a system may use dedicated or shared resources.

Note 1 to entry: See also "system".

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: According to their typical functionality, IAEA distinguishes between automation / control systems, HMI systems, interlock systems and protection systems.

Note 4 to entry: In the scope of this technical report, the term I&C system is linked to the particular process, in contrast to the generic term of I&C platform.

[SOURCE: IEC 61513:2011, 3.29, modified – The words "and I&C function" have been removed from Note 1 and Note 4 has been added.]

3.10
independent assessment
assessments such as audits or surveillances carried out to determine the extent to which the requirements for the management system are fulfilled, to evaluate the effectiveness of the management system and to identify opportunities for improvement. They can be conducted by or on behalf of the organization itself for internal purposes, by interested parties such as customers and regulators (or by other persons on their behalf), or by external independent organizations

Note 1 to entry: This definition applies in management systems and related fields.

Note 2 to entry: Persons conducting independent assessments do not participate directly in the work being assessed.

Note 3 to entry: Independent assessment activities include internal and external audit, surveillance, peer evaluation and technical review, which are focused on safety aspects and areas where problems have been found.

[SOURCE: IAEA Safety Glossary, 2007 edition]

3.11
item important to safety
item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

[SOURCE: IAEA Safety Glossary, 2007 edition]

3.12
license
legal document issued by the regulatory body granting authorization to perform specified activities related to a facility or activity

Note 1 to entry: Any authorization granted by the regulatory body to the applicant to have the responsibility for the siting, design, construction, commissioning, operation or decommissioning of a nuclear installation. In IAEA usage, a licence is a particular type of authorization, normally representing the primary authorization for the operation of a whole facility or activity. The conditions attached to the licence may require that further, more specific, authorization or approval be obtained by the licensee before carrying out particular activities.

[SOURCE: IAEA Safety Glossary, 2007 edition]

3.13
operating experience
accumulation of verifiable operational data for conditions equivalent to those for which particular equipment is to be qualified

3.14
qualification
process of determining whether a system or component is suitable for operational use. The qualification is performed in the context of a specific class of the I&C system and a specific set of qualification requirements

Note 1 to entry: Qualification of I&C systems is always a plant- and application-specific activity while platform qualification relies to a large degree on qualification activities performed outside the framework of a specific plant design (these are called “generic qualification” or “pre-qualification”).

[SOURCE: IEC 61513:2011, 3.38, modified – Notes 1 and 2 have been removed and Note 3 has been revised.]

3.15
redundancy
provision of alternative (identical or diverse) structures, systems or components, so that any one can perform the required function regardless of the state of operation or failure of any other

[SOURCE: IEC 60880:2006, 3.29]

3.16
regulatory body
authority or system of authorities designated by the government of a State as having legal authority for conducting the regulatory process, including issuing authorizations, and thereby regulating nuclear, radiation, radioactive waste and transport safety

Note 1 to entry: For each Contracting Party any body or bodies given the legal authority by that Contracting Party to grant licences and to regulate the siting, design, construction, commissioning, operation or decommissioning of nuclear installations.

[SOURCE: IAEA Safety Glossary, 2007 edition]

3.17
system
set of components which interact according to a design, where an element of a system can be another system, called a subsystem

Note 1 to entry: See also "I&C system".

Note 2 to entry: I&C systems are distinguished from mechanical systems and electrical systems of the NPP.

Note 3 to entry: This IEC SC 45A definition is totally compatible with the sub-definition of "system" given in the frame of the 2007 edition of the IAEA Safety Glossary definition of "Structures, Systems and Components (SSC)".

Note 4 to entry: The term “system” is a very general term that is used for different objects. Examples are Reactor Trip Systems, Engineered Safety Actuation Systems, etc. But also Core Cooling systems, ventilation systems, etc. are systems. The IEC SC 45A standards provide requirements and recommendations for such systems.

Note 5 to entry: Systems can be built from equipment platforms.

[SOURCE: IEC 61513:2011, 3.56, modified – Notes 4 and 5 have been added.]

3.18
type test
demonstration of the capability of a type of equipment to meet specified requirements by subjecting a representative item, or number of items, of the type to a set of physical, chemical, environmental or operational conditions

3.19
validation
process of determining whether a product or service is adequate to perform its intended function satisfactorily. Validation is broader in scope, and may involve a greater element of judgement, than verification

[SOURCE: IAEA Safety Glossary, 2007 edition]

3.20
vendor
design, contracting or manufacturing organization supplying a service, component or facility

Note 1 to entry: The organization able and capable to provide required services and accepting contracted responsibilities bound to those services.

Note 2 to entry: An alternative term which may be used in this report is “contractor”, referring to the supplier quoting, contracting, manufacturing and installing the I&C equipment for systems important for safety. It means as well that contractor is a certified vendor.

[SOURCE: IAEA Safety Glossary, 2007 edition]

3.21
vendor qualification
process of determining whether a vendor is suitable for delivery, technical support and maintenance of the equipment and services contracted formally by the nuclear plant operating organization

Note 1 to entry: Formal contracting means in this context as being able and competent to fulfil all by contract defined responsibilities.

3.22
verification
confirmation by examination and by provision of objective evidence that the results of an activity meet the objectives and requirements defined for this activity

[SOURCE: IEC 62138:2004, 3.35, modified – The reference to ISO 12207 at the end of the definition has been removed.]

4 Abbreviated terms

ALS	Advanced Logic System® Platform
ASIC	Application Specific Integrated Circuit
BTP	Branch Technical Position
CFR	Code of Federal Regulations
CPLD	Complex Programmable Logic Device

CPU	Central Processing Unit
CTEC	Company Profile-China Techenergy Co., Ltd.
DI&C	Digital Instrumentation and Control
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPR	European Power Reactor
EQ	Equipment Qualification
FPGA	Field Programmable Gate Array
GDC	General Design Criteria
GRS	Gesellschaft für Anlagen- und Reaktorsicherheit (Association for plant and reactor safety)
HDL	Hardware Description Language
HPD	HDL Programmed Device
I&C	Instrumentation and Control
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
ISG	Interim Staff Guidance
ISO	International Organization for Standardization
ISSN	International Standard Serial Number
ISTec	TÜV Rheinland ISTec GmbH – Institut für Sicherheitstechnologie
IV&V	Independent Verification and Validation
KTA	Nuclear Safety Standards Commission (Kerntechnischer Ausschuss)
LOP	List of Open Points
NIST SP	National Institute of Standards and Technology, Special Publication
NPIC&HMIT	Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
OBE	Operating Basis Earthquake
PLC	Programmable Logic Controller
PLD	Programmable Logic Device
POSAFE-Q	Qualified Poscon Safety PLC
PSAR	Preliminary Safety Analysis Report
QA	Quality Assurance
RFI	Radiofrequency Interference
RG	Regulatory Guide
SC	Sub-Committee
SSC	Structures, Systems and Components
SFS-EN	European standard implemented in Finland
SRP	Publication under Systematic Review
SSE	Safe Shutdown Earthquake
TXS	TELEPERM XS
V&V	Verification and Validation

WG Working Group

5 I&C platform versus I&C system

5.1 General – Structure of the platform qualification

The subject of this document is the qualification of platforms to obtain a pre-qualification that can be credited for the implementation in I&C systems important to safety. The pre-qualification will still require that application-specific qualification for an I&C system is performed. The aim is to confirm the compliance of the evidence of pre-qualification with the requirements for nuclear use of the existing I&C system, and the engineering processes for generation of the application specific aspects of the I&C system. The qualification process will identify and repair the gaps identified.

When a platform is used on an application, the properties of the platform provide constraints on the application. These constraints are realized by using the requirements for the platform as inputs into the design and implementation phases of the application. By applying the platform requirements, the features of the platform are used during design and implementation phases of the application. During integration of the application the production modules from the platform are integrated into the system. The system is then tested and installed in the plant. This life cycle is shown in Figure 1. The left part of Figure 1 shows a process for platform development, and the right part, for the application development (see also Clause 7).

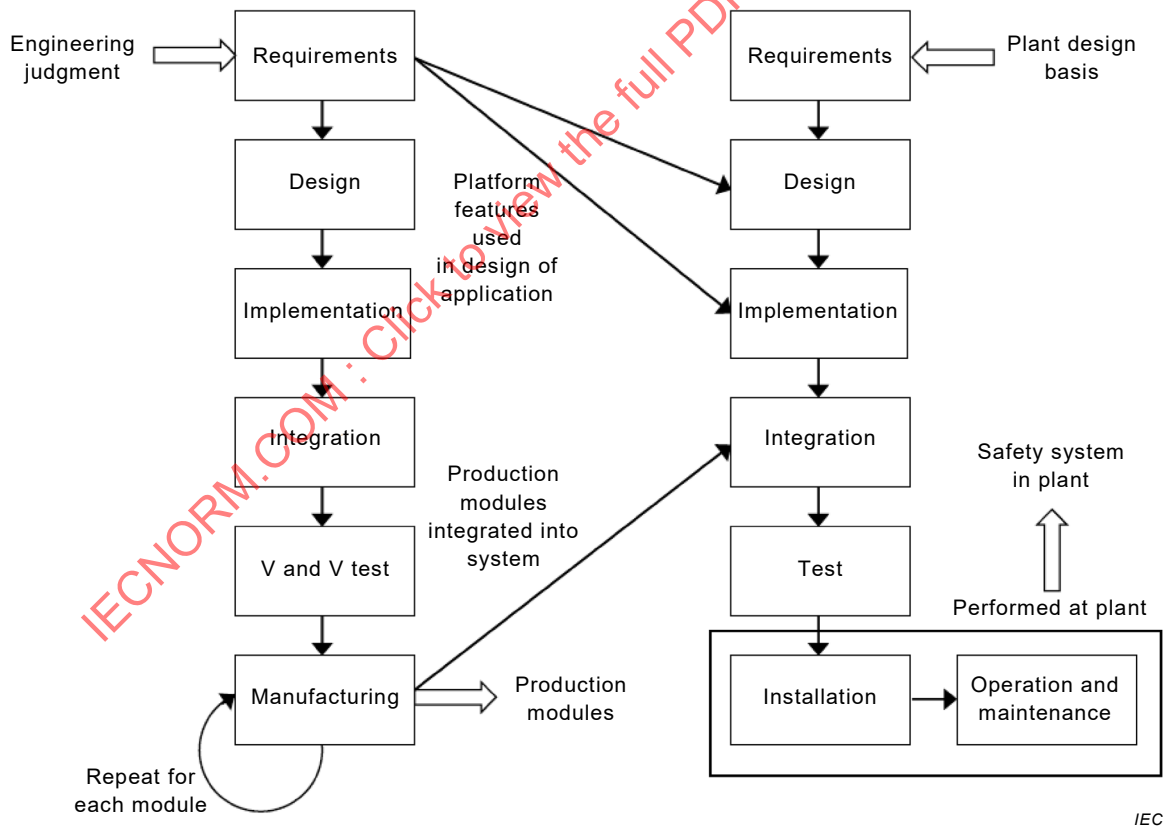


Figure 1 – Platform and application development process

Since the platform is developed prior to use in a plant application, the development of the platform requirements must use engineering judgment to foster the enveloping requirements. For this reason, platforms are not driven directly by any plant safety requirements, but the developer must be informed on how it will be used in order to provide features that will be required in various applications.

Platform qualification comprises the hardware modules (including compliance with the applicable environmental conditions), the software modules and the application software development environment (tools). The separate module qualification is usually complemented by hardware/software integration qualification.

The general overview is given in Figure 2. Based on the intended safety class of I&C systems to be implemented by the I&C platform the qualification of the platform is carried out as the first level in a two level approach (see Figure 2). The second level deals with the application-specific qualification of the I&C system, this is not in the scope of this document.

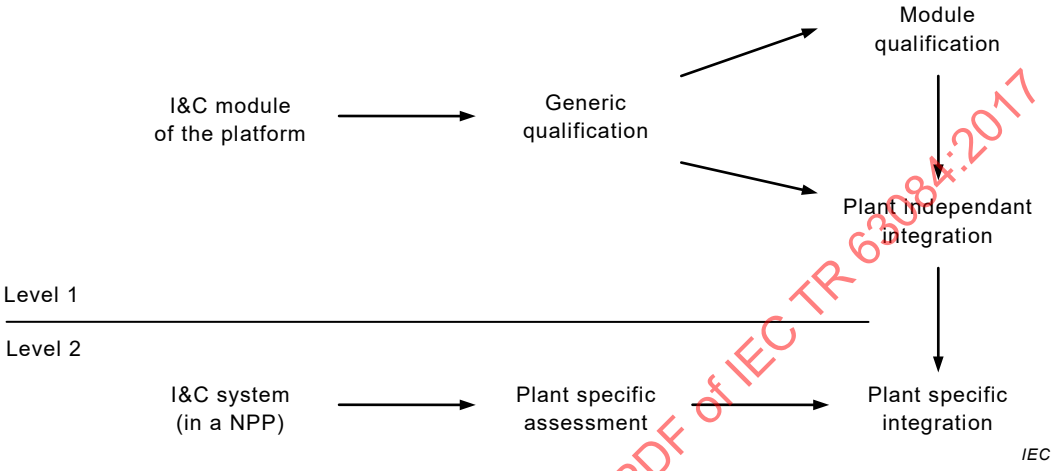


Figure 2 – General overview of a typical qualification process

On the first level compliance of the individual hardware and software modules of the I&C platform is evaluated with suppliers' system descriptions and with general requirements for design, implementation and verification & validation provided by the appropriate IEC SC 45A standards. These requirements are essential to establish the fundamental features of the I&C platform. Usually these fundamental features are validated by means of representatively integrated I&C systems (configurations of interconnected modules). The aim of that evaluation is to determine the I&C platforms' basic suitability for I&C systems of a certain safety class as early as possible.

5.2 I&C platform as an object of qualification – Conceptual design

Due to the fact that I&C standards normally are written for I&C systems it is necessary to interpret/adopt the requirements and recommendations given for I&C systems to I&C platforms. That is expected to ensure that platform qualification provides a pre-requisite for the safety system qualification as shown in Figure 2. The benefit for the system qualification resides in the fact that platform modules are tested and analysed prior to I&C system implementation without need for repeating tests and analysis. It is clear, that the generic platform qualification can only support but not replace the I&C system qualification.

Platform qualification is accordingly a pre-requisite for selecting and purchasing an I&C platform for a plant-specific I&C system. All evaluations described in this report are meant to facilitate purchasing processes by deciding if scope and reliability of the platform correspond to needs and requirements of the I&C system to be implemented.

5.3 Documentation of the I&C platform

The I&C platform can be qualified only if properly documented. Documentation of the platform is to be discussed with the vendor, but generally the following items will be expected:

- A general description of the product with references to all material allowing detailed insight into product operation.

- Vendor's product warranty obligations.
- List of standards and regulations defining basis for product development, including vendor's formal commitment to compliance with the requirements of the listed standards.
- (Access to) conceptual design and manufacturing drawings and schemes of components, sub-assemblies, circuits, etc. All with descriptions and explanations necessary for the understanding of those drawings and schemes.
- Platform software architecture, the level of access to the code of modules will be dependent on the class of intended use.
- Information on manufacturer's software development environment, procedures and software tools; the level of detail will be dependent on the class of intended use.
- A description of the vendors (and/or sub-suppliers as appropriate) manufacturing processes, hardware design processes, and hardware testing techniques used for creating the hardware of the I&C platform.
- Information on security of the product development processes.
- Documentation of V&V procedures. Here both access to records of unit tests and of validation tests at the final product integration. Information on validation methods and tools included.
- Records of product maintenance, product failures etc. (necessary for evaluation of operating experience).

In addition to the above technical documentation, the vendor will be expected to provide general information on organisation(s) responsible for the platform procurement processes, including level of crucial staff expertise.

6 Platform qualification

6.1 Organisation of the qualification

6.1.1 General

The process of the platform qualification[1] shall be formally organised according to commonly established management methods prescribed for safety related projects in IAEA guides (e.g. SSG-39) and in IEC standards (e.g. IEC 61513). These methods are summarized in the following:

- There must be a clearly identifiable party taking initiative and responsibility for the qualification process. That party may be the plant owner, vendor or I&C branch representative (e.g. independent assessor or regulator). The qualification project group – a qualification body, could then be established (of parties as in 6.1.2).
- Specification of platform requirements must be given for example as a platform concept report; this report identifies the safety needs of the target or market industries and clients. The platform concept decisions are market driven, based on what functionality the vendor decides to implement.
- Qualification scope and plan must be defined and documented; indispensable for the qualification is that the hardware and software components, and their constituents, are uniquely identifiable.
- Processes and methods of qualification/certification are specified and established.
- Presentation of results is agreed upon, including documentation and scope of qualification/certifications to be issued.

[1] An example of such a process is the type approval approach defined by the Finnish regulatory body (see Annex A). Type approval verifies that the product and its implementation meet the applicable technical requirements

It is recommended that all demonstrations, both those proposed by the vendor and those required by qualification body, be planned. The plans are expected to identify how the demonstration will be achieved by identifying the types of evidence that will be used, and how and when this evidence is to be produced. Planning is particularly important in case safety and security issues are concerned.

6.1.2 Parties involved

The following parties (depending on the qualification objective) are involved in the process of platform qualification:

- Platform vendor (see definition 3.20)

  It is advisable to remember that product development, manufacturing, distribution, and maintenance is often done by different organisations. In such cases the vendor will be a main contractor legally representing all those organizations.

- Independent assessor

  An authorized or accredited organization assigned to and responsible for independent assessment (see definition 3.10) of the I&C platform. It will be accordingly an organization determining if claims and proofs of the vendor are adequate (sufficient) and trustworthy. The authorization or accreditation can be granted by national accreditation bodies as an essential means of providing evidence of the competence of conformity assessment organizations.

- Regulatory body (see definition 3.16)

  The involvement of the regulatory body may be optional depending on national practice.

- Plant operating organisation – plant owner that is responsible for the plant and its particular I&C project where the I&C platform may be used.

  The involvement of the plant operating organisation may be optional depending on national practice.

As roles and positions of the parties are concerned, note the following:

- The qualification process covers both vendor's organization and vendor's product – I&C platform. Both stages of qualification may require different competences of the qualifying party.
- Plant owner will normally be recipient of platform qualification allowing him selection of the platform fulfilling his plant I&C requirements. The owner may also take an active role in the qualification by ordering that from an independent assessor or by assignment of its own experts.
- Depending on the party initiating the qualification, the result can be generic for the platform or valid specifically for particular kinds of I&C systems.
- The independent assessor (see definition 3.10) has to be agreed by all parties involved in the process.

The independent assessor is knowledgeable and competent for the complexity of I&C platform, and has an acceptable period of experiences in platform domain. He/she may not be responsible for any part of the platform development life cycle such as procurement, design, implementation and testing phases.

Independent assessor, regulator and owner are expected to be represented by qualified experts, i.e. individuals who, by virtue of certification by appropriate boards or societies, professional licences or academic qualifications and experience, are duly recognized as having expertise in a relevant field of specialization.

Vendors can be qualified by studies of the selected issues of their organisations, e.g. evaluation of vendor's records on execution of projects of product development, design, manufacturing, deliveries, service and maintenance. Ways of vendors' qualification can be found in major I&C producers' rules for sub-supplier qualification (see Bibliography).

6.2 Scope of the qualification

6.2.1 Hardware modules

Evaluation and assessment of hardware modules is expected to demonstrate that their characteristics comply with the I&C platform requirements specification. Indispensable for this is to have well-documented hardware modules allowing evaluation of:

- The ability of the hardware module to perform the specified functions.
- Susceptibility of the hardware module to environmental conditions (temperature, moisture, vibration, electro-magnetic influences).
- The ability of the evaluated hardware module to function under all environmental conditions claimed by the supplier, and following IEC/IEEE 60780-323 and other identified standards.
- The reliability and maintainability of the evaluated hardware module.
- The correct version of the firmware (as identified by configuration management), if used (the correct performance of the firmware is part of the software qualification).

Assessing the vendors manufacturing processes, hardware testing techniques, and hardware design process must also be considered. Matters to be addressed include the use of certified components (versus counterfeit components), supply chain integrity, hardware testing to ensure operability, conformance to requirements, and quality. Hardware design must ensure that unintended functions and failure modes are not introduced in the design.

The usefulness of operating experience, possibly previous non-nuclear qualifications or certificates may be taken into account. Complementary testing and analyses of selected modules will be recommended.

Some electronic boards embed Hardware Description Language Programmed Device (HPD) ensuring electronic functions. For software components, the HPD development documentation is assessed for conformity with the engineering procedures, and the recommendations and requirements of, e.g., IEC 62566. The assessment procedure is structured according to the logic software life cycle development phases (design flow) that is described in the following three paragraphs.

The development of a board including a HPD is governed by a global process for the board as a whole which includes a specific process for the HPD development by itself. The final validation step of the HPD development is performed on the “real target” (HPD with the implemented functions on the board). This specific process aims to validate the design and functions of the “customized” HPD.

Once the HPD is developed and validated, the board by itself and as a whole is managed and qualified like any other boards (type testing, environmental, seismic, etc.).

Development documents are checked against general development principles like top-down design, modularity, etc. The development document is assessed for formal and functional consistency. Formal consistency implies, for example, meaningful identification, consistent use of references, clear structure and comprehensible document text including illustrations. Functional consistency is assessed for the development document itself as well as for the phase transitions. This implies, for example, the check of correct and complete transition of functional and non-functional requirements between the documents of subsequent development phases. For this issue emphasis is placed on the test execution of all essential requirements. Functional consistency comprises also the presence of certain information in the development documents, e.g. timing behaviour, internal and external interface description, failure behaviour, self-tests, etc.

6.2.2 Operational system software

The operational system software, i.e. software running on the target processor during system operation, such as operating system, input/output drivers, exception handler, communication software, application-software libraries (e.g., functional blocks library), on-line diagnostic, redundancy and graceful degradation management is in the scope of a platform qualification.

The software V&V activities comprise the verification of development documents (life cycle documentation) and the validation of the completely coded software components. Verification requires assessing and evaluating whether the documents themselves are consistent with the specifications of national and international standards as well as internal guidelines and rules of the software designer. Furthermore, the documents have to be assessed and evaluated to what extent they concur with the requirements established in the preceding phases. In case of generated software code, verification activities can combine development phases.

Validation requires assessing and evaluating whether the software meets the requirements stated in the requirement specification. Validation comprises extensive tests of the software.

The V&V activities are performed as reviews, analyses and tests. There are numerous methods and techniques to realize these activities. Annex E (informative) of IEC 60880:2006 and Annex G of the standard IEEE Std 1012™-2004 provide comprehensive discussion of V&V methods.

The requirements specification is the first and essential part of the development of software components and systems. It must define the functional, technical and qualitative requirements for the component to be developed. Additionally, it has to specify the quality assurance measures as well as acceptance conditions. In case of software components, their role within the system has to be presented. Dependent on the safety requirements there are gradations with respect to content and methods for the development and V&V activities.

The review tasks concerning the requirements specification may be organized in three steps. At first the consistency check demonstrates the transparency and the consistent usability of the document. The check of completeness related to content shows that the component description is comprehensive and sufficient. Finally, evidence is provided that the layout format suits for the technical realization of the required functions.

The review tasks as described for the requirements specification can be transferred to the documents of the subsequent life cycle phases, i.e. the preliminary design, the detailed design and the test documentation. The review tasks depend on the organization of the specific phase model of the development life cycle.

As part of the overall software life cycle development process cyber security requirements must be included as part of the design. This includes developing and planning, including cyber security requirements in the product design, and implementing and testing that the requirements are met. Guidance may be taken from IEC 62645 and the NIST SP 800 series documents. The review task confirms the cyber security requirements have been identified and met.

For the V&V of coded program parts the test of the programs is of decisive importance. This includes the selection of suitable test cases and the observation that the behaviour is compliant to the requirements. For the effective preparation of testing of the programs (selection of an exhaustive test set for a defined test strategy) a series of complementary and additional program analyses can be foreseen, besides the actual tests for correctness and robustness. Therefore, the review of the test specification and test report includes not only the check of the planned and executed program tests (test strategy, selection of test cases, test execution, test evaluation) but also the assessment and evaluation of the program analyses to be applied.

Analyses have to be carried out to check the formal and technical traceability of the functional and non-functional requirements. The formal traceability is related to the complete transition of the requirements during all phases of the development life cycle. The requirements are traced downwards to the final software code and upwards to the V&V activities. Traceability includes demonstration that all testable requirements are tested and allows knowing which testable requirements are covered by each test. The technical traceability is related to the consistency and plausibility of the contents of the derived/refined requirements, design decisions or other phase outputs. Consistency and plausibility are analyzed with respect to the preceding phase and between the phase outputs themselves.

For the transfer of the program design into the source code language a set of rules has to be obeyed in the context of “good programming style” in order to obtain improved readability, modifiability and testability. Some requirements, e.g. the limitation to certain language constructs, are a necessary precondition for specific validation techniques and effective program testing. The review task will confirm the coding rules have been identified and followed.

6.2.3 Application software

Usually application software is specific for I&C systems and not a generic part of the platform. Nevertheless, specific developments of a platform may exist, e.g. a neutron-flux measurement system based on a more general platform. In this case, parts of the application software can be in the scope of a platform qualification. For more information about application software development, see 7.3.3.

6.2.4 Tools

The qualification of tools depends on the required reliability and risk of errors and faults to be introduced by the tools, and the extent to which the tools’ outputs will be verified. Guidance is provided in IEC 60880 and IEC 62138.

The qualification of tools considers their coverage of the safety life cycle phases (completeness of the tools provided) where benefits to the assurance of quality and to the reliability of the functions important to safety can be obtained. Clarity in handling instructions and interconnectivity are of interest, as well.

Tools having impact on the implementation of the application software (e.g. code generators) need to be included in the qualification process. These tools will be evaluated in order to confirm that they are functionally and qualitatively suitable for performing their tasks. The tools used to produce the code of the application software will be evaluated according to, e.g., Clause 14 of IEC 60880:2006. For software tools with no impact on the application software (e.g. documentation tools) the qualification approach relies on application of the ISO 9001 development process.

6.2.5 Integration to a representative system

Hardware and software components relevant for a representative I&C system are integrated to be tested in order to demonstrate the operability of the software/hardware complex and generic platform characteristics. The representative system would be configured according to qualification expectations (specification), and typical usage of the platform.

Platform characteristics can be confirmed as generic ones if they are valid independent from the configuration of the hardware and software components. If this is not the case, the qualification result is restricted to the corresponding configuration for which the platform characteristic is valid.

6.3 Methods of qualification

6.3.1 General

According to IEC 61513, it is good practice to perform qualification in well-defined stages, i.e. by taking credit from platform qualification (see Figure 2).

Type testing, operating experience and analysis are the basic means of the qualification prescribed by the standards IEC IEEE 60780-323, IEC 60880, and IEC 62138. Modules are generally qualified by type testing or a combination of methods, e.g. evaluation of operational experiences, audits, analysis, additional testing, etc.

The methods of qualification will rely generally on review and evaluation of platform development processes, as well as on general evaluation of platform functions and capabilities.

It is essential to start qualification from review of platform information provided by (required of) the vendor (see 5.3). That review is expected to be done in close cooperation with the vendor ensuring access to all information required by the assessing parties.

Special attention will be paid to application development environment (see 7.3.3) where the qualification may be enhanced by the following guidance:

- Prepare specification (list) of the required environment properties (see Clause 6) complemented with information on platform documentation and on the particular requirements of the qualifying parties.
- Start qualification with vendor's demonstration of platform properties.
- Follow demonstration by the audit of the issues selected at the demonstration.
- Allow representatives of the qualifying parties short training and “hands on” experience of the application environment chosen for the representative system (see 6.2.5).
- Define test cases for detailed evaluation of selected environment features.
- Refer to earlier projects of plant I&C systems, paying special attention to the occurrence of late changes in specifications and scope of the field tests required.

6.3.2 Type testing

The concept of type testing was originally developed for the qualification of hardware modules. It is based on the idea of testing representative samples of modules. This concept has been also adapted to software modules as far as applicable.

The basic goal of type testing is the separation of tests and inspections which are independent of a specific plant from those which are plant specific due to the specific design of the I&C system. Having type tested modules allows reliance on the accordance of this module with the specification of their functional properties in the data sheet or in the software development documents. Moreover, tests and inspections can be performed independently from and in advance of employing them in the plant. Even more important is the fact that the type testing procedure has to be executed only once. Each subsequent employment in an I&C system can refer to the type testing, which has been performed successfully. Thus the use of type tested modules renders a solid basis for I&C system reducing the amount of tests and inspections for a specific plant and induces a clear structure for the licensing process of an I&C system.

The qualification results for all hardware and software modules necessary for the implementation of the I&C system need to be controlled under configuration management according to 6.3.2.3 (System configuration management plan) of IEC 61513:2011 at system or platform level and to 5.6 for software. This is in order to be able to identify that the deliverable target platform including software products and hardware equipment is the same as the one qualified through test.

Qualification is performed in accordance with the specified applicable industry codes and standards to ensure that the platform modules will function as required.

The qualification effort depends on the envisaged usage of the platform, i.e. whether it is intended to be used for class 1, class 2, or class 3 I&C systems. According to IEC 61513 the software design and V&V effort can be graded. For class 1 systems the criteria and the requirements of IEC 60880 apply. For class 2 and 3 systems the criteria and the requirements of IEC 62138 apply.

6.3.3 Operating experience

Effective operating experience requires adequately documented data which reflect the relevant operational conditions and performance, and thus their usefulness. The past operational conditions and performance have to be assessed with respect to the actual conditions and performance of the equipment under qualification. Thus the use of operating experience is limited to these circumstances.

For the use of operating experience the standards and guidelines do not provide concrete support. Alternatively tests and certification are recommended. Operating experience can be credited to compensate gaps revealed in the quality of the product. Often operating experience is taken as a confidence-building measure in the overall qualification process.

Statistical testing to obtain operating experience data has shown to be not a viable approach.

Vendor is expected to be able to present all data on platform operational safety performance. It will be advisable that records of platform performance are graded according to pre-defined sets of performance indicators. Records of safety incidents are of the utmost interest, including human errors linked to wrong application of the platform. All vendor's data on the operational performance will be expected to be available to the qualifying group, and past and present users of the platform be encouraged to give references.

In case of newly developed I&C platforms, operating experience may be gained by using the platform at first in lower classified systems.

6.3.4 Analyses

Qualification by analysis – following IEC/IEEE 60780-323 – requires a logical assessment or a representative model of the modules to be qualified. The model is based on physical laws of nature, results of test data, operating experience, and condition indicators. Analysis of data and tests for material properties, equipment rating, and environmental tolerance can be used to demonstrate qualification. However, analysis alone cannot be used to demonstrate qualification.

There is a variety of techniques to analyse hardware and software modules. They are needed only from case to case. The techniques can be grouped into:

- Proofs (from simple algorithm checks to formalized mathematical deductions).
- Static analyses (examinations of the program code; from simple standard tests to complex path analyses).
- Dynamic analyses (observation and recording of the runtime behaviour; from simple time measures to the analysis of the real-time behaviour).
- Testing (from specifying simple test patterns to the development of complex test strategies).

The formal correctness would build on the proof of the algorithmic solution being correct with respect to a specified requirement (of the module specification). This technique is not feasible in full scope due to missing tool support.

Static program analyses examine development documents or program texts without execution of the programs themselves. The objectives of static program analyses can be different e.g., to check the compliance with programming rules, to visualize the structure of the program system, to reveal weak points and deficiencies in the control and data flow, or to prepare program testing.

Dynamic program analyses examine programs by observing the runtime environment. The goals of dynamic program analyses can be e.g., plausibility check at assertions, or monitoring of the runtime behaviour and performance measuring.

Program testing aims at selecting test cases such that a high certainty for the reliable operation can be obtained from the behaviour of the tested data. Therefore a test strategy, i.e. a methodical and goal-oriented selection of test data has to be strived for which complies, as far as possible, with the concept of testing the functionality covering all requirements and operational demands. Criteria for the selection of the test cases can be obtained from the list of requirements (functional testing) or from the organization and structure of the program text (structural testing).

6.4 Documentation of qualification results

The qualification results are recorded in Lists of Open Points (LOPs). The LOPs can be structured in tables of

- minor issues (e.g. typing errors, form errors);
- requests (e.g. wrong descriptions of technically correct items, inconsistent or insufficient descriptions);
- key issues (e.g. non-conformance with IEC standards or equipment characteristics).

The LOPs are clarified with the developer/supplier of the I&C platform. Any remaining non-conformities will be documented in the final qualification report. The final qualification report summarizes the qualification activities and results, and gives an evaluation of the overall platform quality and provides possible recommendations. In case of successful qualification certificates are issued corroborating suitability of the I&C platform for specific usage. The specific usage includes the applicable safety classes.

The result of qualification is documented and certificates may be issued, in case of successful qualification result.

6.5 Maintenance of qualification

The validity of the platform qualification and of the corresponding certificates is usually time limited, and is revalidated at the end of the validity period. Platform qualification may be sustained for modified hardware and software modules if the differences are of minor nature. Minor changes could be e.g., a hardware layout modification or simply the expiry of the certificate. The modifications have to be evaluated with respect to the components' function and interfaces. The accumulation of many minor changes on the same part can result in the need for supplementary qualification.

Major changes such as a new hardware module, or a limited modification in software functional requirements or in qualified generic parts of the platform can result in a supplementary qualification. Essential changes as in hardware or software design criteria or properties, or a new CPU can result even in a new platform qualification. Figure 3 illustrates a process for maintaining the platform qualification.

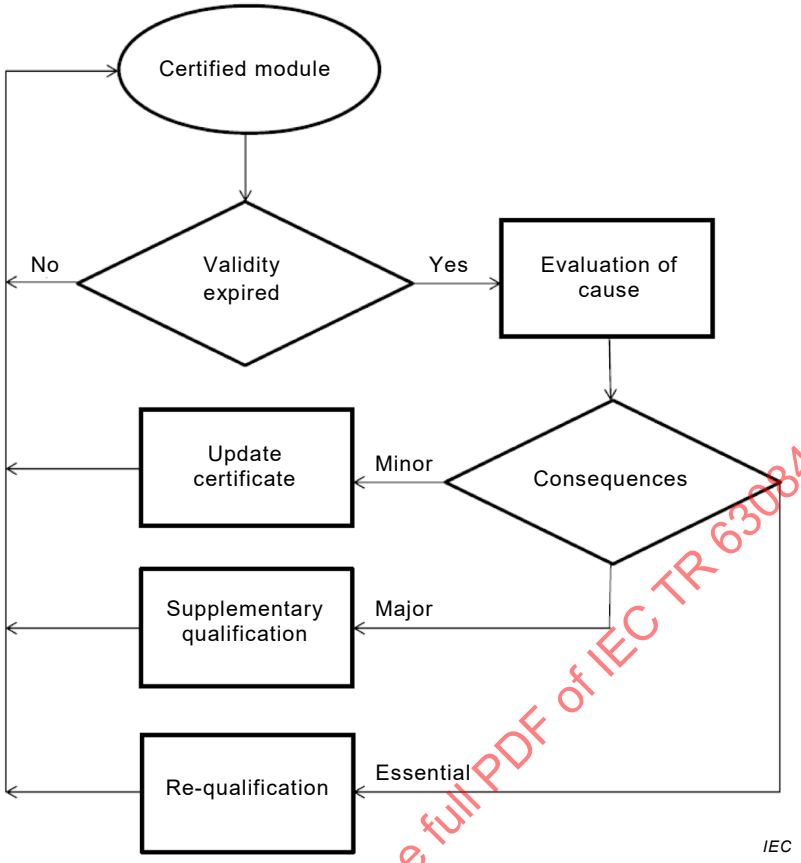


Figure 3 – Process for maintaining the platform qualification

There might be, of course, other reasons questioning the platform qualification, e.g., changes in manufacturers or supplier's competence, or serious incidents coupled to platform properties. In addition, new standards and regulations may invalidate a previously obtained platform qualification.

Notwithstanding that it is the duty holder (the plant operator / holder of the permission to operate) that is responsible for maintaining the qualification once a system based on the platform has gone into service, others can contribute to this activity.

The responsibilities and obligations to maintain the platform qualification could be prescribed – on behalf of the regulator – between the supplier and the independent assessor of the platform. The independent assessor could keep itself apprised of any changes in the standards and regulations indicating that the qualified design may no longer comply with the applicable requirements. On the other hand the supplier would inform the independent assessor of any modification to the qualified design that may affect the conformity with essential safety requirements or the conditions for validity of the certificate.

All maintenance has to be documented through maintenance plan and records of actual maintenance activities. The issues addressed in the maintenance plan are expected to follow requirements of the IEC 61513. It is recommended to establish that all changes, corrections of the I&C platform features important for safety, even if minor, are handled formally; i.e. through formal hardware or software modification requests followed by the well-defined procedures reflected in configuration management system.

Subject to national regulatory requirements it is recommended that, in the event that the parties agree that the owner takes over all I&C system support, the vendor would hand over to the owner development and configuration management environment for the actual platform.

7 Dependency on the platform through life-cycle of the I&C system

7.1 General

Definition 3.6 (see IEC 61513) describes the platform as not only equipment of hardware and software executing I&C functions but even a product providing environment for smooth and safe implementation of I&C systems. Implementation refers there to all phases of a system life cycle, as e.g. presented in IEC SC 45A standards by the traditional “V-cycle”.

When evaluating the platform, it is advisable to pay special attention to the following aspects. Though the aspects might be beyond the scope of this technical report experiences show that they are worth being taken into account in order to achieve smooth and safe implementation of I&C systems.

- Cooperation of the parties involved in I&C system implementation (see 7.2).
- Features of the application implementation environment (see 7.3).
- System integration, validation and commissioning (see 7.4).

7.2 Models of cooperation between the parties of the I&C system project

I&C system implementation involves primarily the utility (owner), the supplier (vendor) and the regulator. The platform has to be qualified in frames of agreement between those parties, providing means for their smooth cooperation.

Traditional models of cooperation would build on the strict division of responsibilities between the owner and the supplier. Owner specifies requirements, which vendor is contracted to fulfil. The problem of this model is that the owner while specifying, is as yet not familiar with the platform. The contracts are then often renegotiated to adopt owner's requirements to particular platform and conflicts arise as both parties lack complete information and focus claims on added/unfulfilled functionalities, with project management fully occupied with solving conflicts.

An alternative model would be joint user-supplier organisation for a specific I&C project or even for a set of projects. The organisation would be based on an early agreement to base I&C on the pre-qualified platform, e.g. pre-qualified according to IEC SC 45A or IEEE standards. However, experiences show that national regulations or different interpretation of standards is also a source of significant problems so it cannot be assumed that choosing a pre-qualified platform will completely solve the qualification problem. This means that the qualification of the platform has to be considered in the frame of an I&C system project even using a pre-qualified platform. The platform's capabilities are used to align individual business objectives with common strategy to achieve best possible results of I&C implementation. The essential part of such partnership would be platform capabilities facilitating early identification of risks and rewards allowing those to be continuously identified and shared according to predefined rules.

Still another option would be standardised application implementation environment available for the owners, prior to final purchase of the particular platform.

7.3 Platform environment for implementation of applications

7.3.1 Platform supported procedures for I&C system implementation

Development of I&C platforms results in provision of automatic tools and services enabling safe and efficient handling of various life-cycle stages of I&C system.

Figure 4 may be used as a guide and an example of such a development. The engineering procedures for the implementation of I&C systems are related there to a classical “V-cycle” introduced in IEC 60880.

The left part side shows the “specification activities”, which are in the focus of whole I&C implementation. Those activities result in:

- requirement specification;
- specification of I&C system including the conceptual design;
- detailed specification of I&C functions and architecture, addressing both system hardware and software;
- specification of test cases to verify the design targets.

The detailed design of I&C system is related to tasks of software engineering, grouped there in the lower box of Figure 4. The same results allow now detailed design of I&C hardware equipment and then manufacturing and installation of the same in the factory.

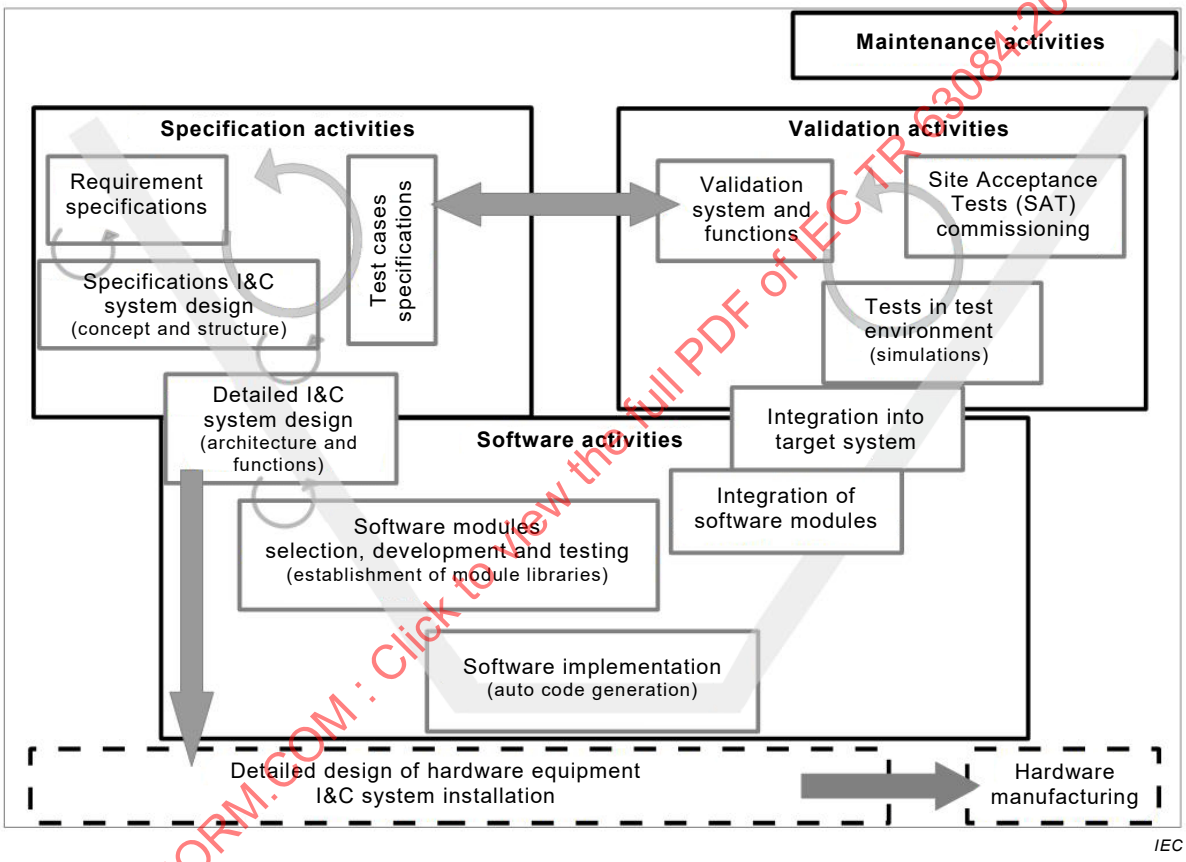


Figure 4 – Life cycle procedures/tasks of the I&C system implementation

The platform will be expected to support the validation activities of I&C system completely now with software modules integrated in the hardware. Those activities, as at the right upper box of Figure 4, can be run:

- at the factory, in the test field environment during system integration, for the verification of pre-defined performance of the I&C system (e.g. CPU-loads of processing units and bus loads);
- in the test field environment, after software integration into the complete target system addressing adequateness of the I&C system design (e.g. redundancies, fault tolerance);
- on site, by validation of on-site functionality and performed by site acceptance tests on the target system installed in the plant.

The validation activities require normally the target system and availability of the process controlled. The platform would be expected to mitigate it by provision of the process simulation environment.

The activities to maintain platform qualification are described in 6.5. Depending on the maintenance task all or only part of the life cycle phases of Figure 4 might be affected. E.g., for a change of the software requirements specification, the whole software development process for any part of the I&C system impacted by the change have to be re-examined.

7.3.2 Tool-based implementation – Kind of tools required

The platform supported procedures discussed above are implemented through various tools. The following are examples of recommended tools:

- Tools for simulation of the process controlled enabling development and early validation of I&C control functions (preferably available already for the requirements specification).

  NOTE The requirements specification can be presented in form of models of both the process and I&C functions.

- Handlers (translators, compilers) of graphical specification languages ensuring formal environment for detailed specifications, structuring and architecture of application bound I&C hardware and software systems. Here as well design tools for I&C functions and I&C system:
- Automatic source code generators and compilers, directly from the formal specifications.
- Test tools for validation of the requirement specification of the target code.
- Test tools for validation of the integrated I&C system.
- Tools for handling test cases for verification of engineering activities relevant to safety.
- Management tools for effective management of all project data, preferably configuration management prescribed by IEC standards. Methods for software authentication in the target system.

7.3.3 Application software development

Application development environment of the platform may be further evaluated on the following issues:

- The environment is expected to build on the application functions' modularity.
- The platform operation system is expected to ensure standardised access to intelligent drivers, sensing devices, actuating devices, communication channels/protocols, etc. The interface between the system software and the application software has to be completely defined and documented.
- The environment is expected to support documentation of application modules and module architecture (e.g. comments, explanatory text in module code).
- The concept of parameter configurable software may be supported: typically software that already exists but is configured for the specific application by using simple parameter values and/or an application oriented input language.
- Library modules have to benefit from an adequate level of defensive programming at the application level, in particular with respect to the “within range” validation of their input parameter values, the detection of anomalies and the generation of safe outputs.
- System for detection and safe reaction on module/system failure modes is expected.
- Features facilitating static analysis and testing of application software are expected to be available under the full range of specified operating conditions.
- Support for development and usage of module templates is expected. The template packaging would ensure limits to the maximum size of the module and confine changes/failures to a single or to a small number of modules.
- Modules are expected to be defined in a way allowing unit tests, i.e. in isolation from other module parts and from other modules.

It is essential that the platform will provide means facilitating application development based on the concept of libraries, as presented here in Figure 5.

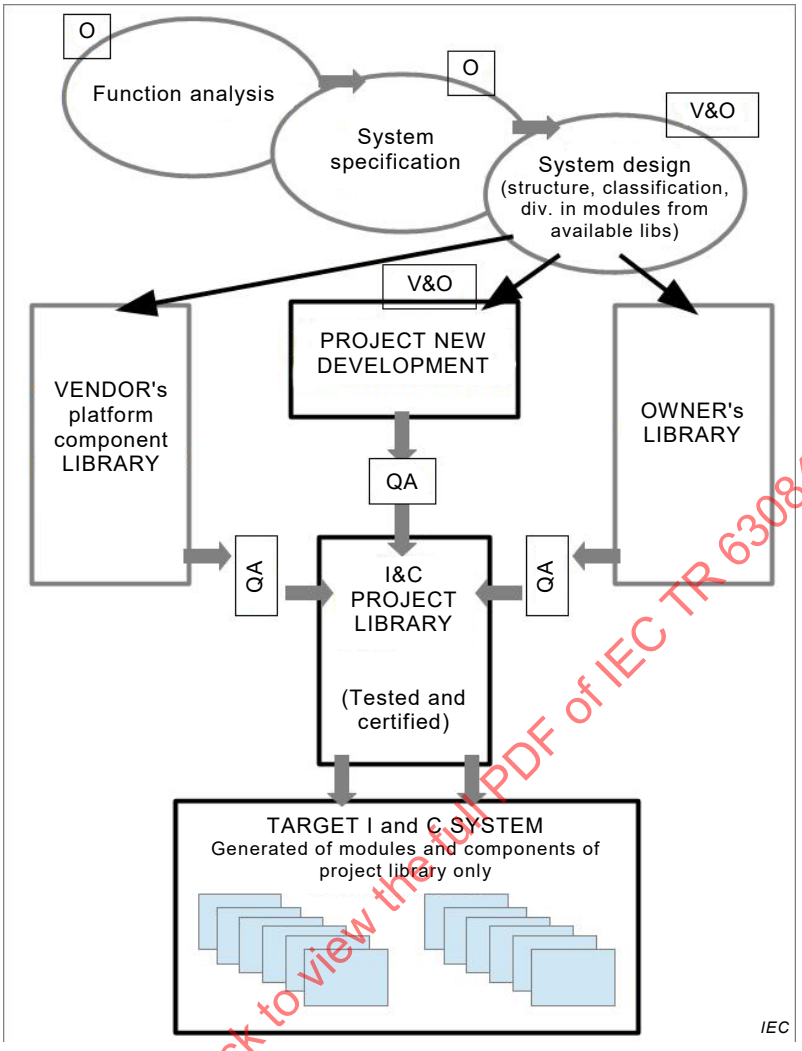


Figure 5 – Application development based on the project library (V-for vendor, O-for owner)

The user would be able to build “project library”, established for the particular I&C system. It would be supported by platform specific components (vendor's library) and platform features supporting owner new developments and eventual establishment of plant specific modules (owner's library). The owner's library will be then available for continuous improvement and validations through operating experience, ensuring basis for all ongoing I&C projects.

7.4 I&C system integration, validation and commissioning

Final implementation of tested and accepted source code is done in testing site by compiling and loading of the code to the target system. The I&C platform would be evaluated for efficient and secure means of code loading and for availability of integrated test environment comprising simulation and fault monitoring functions.

As the I&C implementation process is concerned, special attention would be paid to platform's ability to facilitate handling of test-scripts specifying test cases. Selection and evaluation of tests would be facilitated through simulation based factory testing and the choice of tests which would be processed again in the plant. Such duplicate use of the test-scripts would enable comparison between testing of the application software on simulators and system validation at in-field testing and commissioning of the integrated target system.

Platform environment for test-scripts handling would facilitate preparation of validation and commissioning plans.

I&C platforms with means for that approach would allow deep understanding of controllers and processes and by reducing in-plant testing, enhance safety and reduce costs.

8 Conclusions

This technical report provides an assessment framework and activities for efficient and transparent qualification of I&C platforms for use in nuclear applications important to safety. The assessment aims at a pre-qualification of I&C platforms outside the framework of a specific plant design.

Due to the lack of consensus, the topic is not yet amenable to standardization. At the present time, there is apparently no consensus to define a commonly accepted approach for I&C platform qualification. The whole process of I&C platform qualification has different meaning in different countries. There are, for example, different perceptions of the involvement of regulators and plants in the process. The dilemma is increased by the huge number of both national and international guides and standards.

On the other side, I&C platform qualification supports efficiency by enabling parties implementing particular plant specific I&C systems to concentrate on application functions, while for basic system functions to rely on platform qualification.

One proposal that arose during the generation of this report was to use the technical report as an explanatory basis for the new work item proposal on commercial grade item dedication made during the 2014 Las Vegas meeting.

The working group WG A3 will monitor the possibility to launch – in the future – the development of a standard on the topic covered by this technical report.

Annex A
(informative)

Issues of the Finnish licensing approach

Annex A examines the issues of the Finnish licensing approach. As such, the “shalls” and “shoulds” used in the text of Annex A do not represent requirements or recommendations of this document.

Typical use of I&C platform qualification results is in the licensing process of I&C systems.

Licensing an I&C platform is usually part of licensing a new safety related I&C system or part of licensing a major change in a safety related I&C system. It should be noted that the same platform can be used in more than one system forming the functional chain or can even be used in several parallel systems. In the last alternative the restrictions coming from the plant defence-in-depth and diversity requirements must be observed.

A platform to be licensed usually has previous qualifications for the same or more usually for some earlier version of the platform.

In a system quality and/or qualification plan the licensee presents to the licensing authority (Regulatory body, see definition alternative 2 in IAEA Safety Glossary) how the platform of a safety related I&C system is to be qualified and licensed.

The preliminary safety analysis report of a new or renovated safety related I&C system is usually accompanied with the documents of the I&C platform generic qualification if the platform is already chosen.

In some Finnish projects it has been convenient to divide the plant specific qualification and licensing into two phases: the preliminary and final suitability analysis. The licensing requirements presented hereafter follow that two phase practice.

When the I&C platform is chosen for a certain safety related application, the licensing of it starts with presenting to the regulatory body the preliminary qualification documentation in the preliminary suitability analysis:

- requirement specification for equipment specific for the intended location of use;
- in safety class 1 (IAEA safety class), an evaluation report from the review of the requirement specification of the I&C equipment (here “equipment” can mean the whole platform or the platform qualification can be divided to parts like the main PLC modules and the priority modules.)
- verification of the suitability of the component;
- description of the component;
- description of the manufacturer;
- quality plan, if required;
- qualification plan, if required;
- information and plans concerning type approvals and tests as well as the standards, organizations and accreditations used in them.

Requirement specification (these are the requirements set by the intended place of service in the system where the item of the equipment is to be installed):

- A requirement specification shall be prepared when selecting or procuring I&C equipment in safety classes 1 and 2.

- The requirement specification of I&C equipment in safety classes 1 and 2 shall indicate the properties required from the equipment at the intended location of use (such as the functional requirements, performance and reliability requirements, requirements set by environmental conditions and operation conditions, and requirements concerning connections, periodic tests, maintenance, information security, qualification, and service life).
- The requirement specification of I&C equipment in safety classes 1 and 2 shall indicate the safety classification and seismic classification of the component.
- The requirement specification of I&C equipment in safety classes 1 and 2 shall indicate the essential safety standards applied to the component and the deviations to their requirements.
- The requirement specification of I&C equipment in safety classes 1 and 2 shall indicate the requirements regarding the component presented in the quality plan of the system and its components.
- The requirement specification of I&C equipment in safety classes 1 and 2 shall indicate the requirements regarding the component set forth in the system or component qualification plan.
- The requirement specification of I&C equipment in safety classes 1 and 2 shall be maintained throughout the design, manufacture and operation period of the system.
- The final requirement specification of I&C equipment in safety class 1 or 2 shall be detailed enough in order to allow for the traceable verification of the compliance to the requirements in question of the final product.
- The requirements of I&C equipment in safety classes 1 and 2 shall be unambiguous and shall not contain conflicting information.
- The requirements of I&C equipment in safety class 1 or 2 shall be traceable to their higher-level requirements (such as system level requirements, facility level concept requirements, etc.).
- The requirement specification of I&C equipment in safety class 1 shall be assessed by an expert that has not been involved in the design of the item in question. The assessment shall demonstrate that the requirements set for the product meet the higher-level requirements.
- In safety class 1, a report shall be prepared on the assessment of the requirement specification of I&C equipment presenting the observations made during the assessment and a justified conclusion regarding the accuracy, scope and consistency of the requirement specification.
- The assessment report on the requirement specification of I&C equipment in safety class 1 shall be updated when the requirement specification is modified.

Suitability assessment:

In the preliminary suitability analysis, the suitability of the component shall be verified by comparing the rated values with the requirement specification. In the necessary scope, the following characteristics of the component shall be examined:

- functional features and performance;
- reliability;
- endurance of environmental conditions;
- electrotechnical dimensioning and protection;
- operation of the component in case of disturbances or transients in the electrical network;
- the applicability of the standards used in the design and manufacture of the component;
- testability and maintainability;
- service life.

Description of the manufacturer:

A report of the manufacturer and the manufacturer's prerequisites for manufacturing the product in question according to the quality management requirements for the specific type of equipment shall be presented in connection with the preliminary suitability analysis. Special attention shall be paid to the following:

- the manufacturer's organisation;
- the manufacturer's competence for manufacturing the product;
- the manufacturer's management system, its assessment method and assessment results.

In connection with the start of cabinet furnishing or installations (depending on the project specific requirements) the final suitability analysis would be presented:

- qualification results including qualification test results, EMC properties, analyses and type approval if required;
- independent review of the acceptability of the qualification measures, if required;
- any measures related to the follow-up of the storage life, service life and ageing of equipment and materials;
- a summary of the results of quality management during manufacturing, if needed;
- a summary of the results of factory tests, if needed (if the component in question is not serially manufactured);
- any deviations from the information presented in the preliminary suitability analysis of the component, and justification of their acceptability;
- a review of the effectiveness of quality management during design and manufacture, if needed: I&C equipment in safety class 1;
- a software evaluation, if needed.

Qualification results:

In connection with the final suitability analysis, the component shall be demonstrated to fulfill its rated values on the basis of the validation. Special attention shall be paid to the following:

- qualification test results;
- compatibility with the electrical network;
- qualification to environmental conditions;
- EMC properties;
- analyses related to qualification;
- operating experience feedback;
- type tests and type approval;
- software qualification.

Type approval:

The prerequisite for the type approval of equipment shall be a type inspection certificate issued by a third party confirming the acceptability of the design and implementation of the equipment against the equipment rated values. A third-party assessment of the type conformity of the quality assurance-based production process, or a third-party certificate of conformity that confirms the type conformity of the manufactured equipment based on product-specific inspection and testing, shall also be required. The type inspection and verification of conformity shall follow modules B and D of Decision 768/2008/EC of the European Parliament and of the Council. Module F may be used instead of module D.

The third party authorized to perform the type inspection and type conformity assessment of a component shall be a certification body that has been accredited for the conformity evaluation of the applied standards under standard SFS-EN ISO/IEC 17065, or an inspection organization accredited for a similar task under standard SFS-EN ISO/IEC 17020. In order to supervise the testing, the certification body or inspection organization shall have applicable qualifications under standard SFS-EN ISO/IEC 17025. The certification body or inspection organization shall also be a notified body appropriate for the task.

The accreditation decision pertaining to the organization performing type inspections and type conformity evaluations shall be appended to the preliminary suitability analysis.

In the type inspection, the third party shall inspect the component as a combination of design type and product type as referred to in module B of the Decision.

The type inspection certificate or appendices thereto shall indicate all the information confirmed with a type inspection (technical breakdown) and any limitations on operation required to assess the acceptability of the component for its intended use.

A document prepared by a third party concerning the approval of the quality system pursuant to module D of the Decision shall be appended to the type approval documentation.

If module F of the Decision is used, the conformity certificate issued on the basis of product-specific inspections and testing shall indicate the following:

- the unique identifiers of the delivery batch, and the unique identifiers of the components inspected from the delivery batch;
- inspections performed and tests supervised by a third party (scope of product-specific inspection) in order to confirm the conformity to requirements of the delivery batch;
- the conformity certificate shall refer to the type inspection certificate, and it shall confirm that the components in the delivery batch correspond to the component type for which the type inspection certificate has been issued.

The type approval of a component containing software-based technology shall cover the assessment of both software and hardware.

Annex B
(informative)

Review of Areva's TELEPERM XS platform qualification[2]

The development of a software-based safety I&C system needs careful consideration of a qualification plan from the very beginning and is a long-term process. The concept of the new digital safety I&C platform TELEPERM XS (TXS) was evaluated by GRS/ISTec as a third-party independent assessor in 1992. Based on agreed principles for digital I&C systems, the digital platform TXS was developed. It is characterized by a set of fixed reusable software modules (operation system, function block library, etc.) as well as by the specification of design tools for plant-specific application (graphical editor, code generators, etc.).

Such a system allows the qualification process to be split into two phases, the plant-independent generic qualification (qualification of the I&C platform), and the plant-specific qualification of the particular I&C realizations (with all the plant I&C functions).

The qualification process of the I&C platform TXS consisted of detailed analyses of the output of all development phases of the different modules (hardware, software and tools) by independent experts. Using a representative system configuration, a generic integration test was performed to demonstrate the applicability of the modules and their interrelations. The goal is to confirm all the application-independent platform properties and to show the correct behaviour.

The type test of the modules included hardware type test and software type test. Hardware type test is well-defined by the German national standard KTA 3503 “Type test of electrical modules of the reactor protection system”. For the software type test, the procedure shown in Figure B.1 has been established considering IEC 60880 and requirements of KTA 3503 accordingly applied to software.

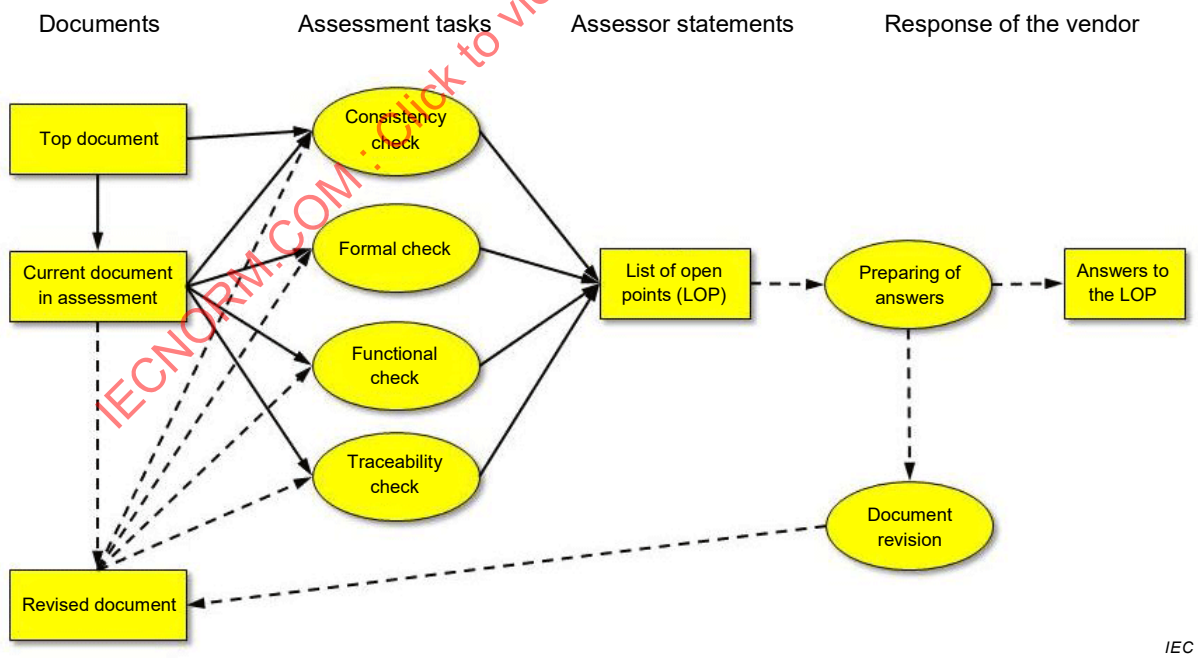


Figure B.1 – Software type test procedure

2 This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the companies named.

During the software type test, at first all manually developed software modules were qualified. These modules are not modified during the application software generation. Therefore, the plant-independent system software is already validated during the type test procedure. Only the automatically generated application software must be evaluated during the plant-specific software qualification. The code generators were included in the software type test.

With the plant-independent system test, the vendor demonstrates that the hardware and software modules can be integrated to a representative I&C system. During this test, system properties like the deterministic time behaviour, the constant CPU load, the constant communication load, the independence of the system behaviour from input signals, etc. were verified. The assessment of the plant-independent system test was focused to the completeness of the test cases, the accurate test implementation, and the evaluation of the test results. The specification and code generation of the software for the plant-independent system test was part of the evaluation of the engineering workstation. As a result, the essential platform properties were certified by the assessors. In addition, recommendations for V&V measures to be performed during plant-specific assessments were listed.

Design phases related to a new EPR plant safety I&C system and its platform:

The preliminary safety analysis report (PSAR) and associated topical reports:

- Role of the safety I&C platforms in the I&C architecture and the allocation of plant safety functions.

Design of I&C architecture:

- Functions allocated to I&C systems and their interfaces;
- Environmental requirements and protection against internal and external hazards for systems;
- Performance and independence requirements of the functions;
- Requirements of communication between the I&C systems, user interfaces and field equipment.

Design of an I&C system:

- Internal sub systems and functions allocated to them;
- System structure to fulfil the environmental, safety, performance, independence and interface requirements for the system and its subsystems and their interfaces;
- Equipment of the system and requirements for them.

Choice of the I&C equipment:

- The equipment specifications indicate that an individual item of equipment or needed configuration of an I&C platform fulfil the requirements set by the system design e.g. the equipment is suitable for a certain plant location of use;
- The item of equipment or the I&C platform is qualified so that there is enough confidence on the specifications e.g. type approval.

In the PSAR phase, some preliminary information of the possible I&C platform can be presented: possible previous qualifications, operational experience and generic qualifications.

During the design of I&C architecture and system, a preliminary suitability analysis of the I&C platform is generated indicating that it is capable of executing the allocated functionalities with required performance (including communication features) and has the required withstanding for environmental, safety, isolation and communication separation requirements. This is indicated with the equipment specifications, manuals and previous qualifications.

In the final suitability analysis, the choice of the equipment is justified with the up to date and project specific qualifications and analysis of suitability to the intended plant location of use.

Annex C
(informative)

Review of Westinghouse ALS platform qualification[3]

C.1 General

Annex C provides a review of Westinghouse ALS platform qualification. As such, the "shoulds" used in the text of Annex C do not represent recommendations of this document.

C.2 Introduction and ALS-background

The ALS platform is a logic based platform which does not utilize a microprocessor or software for operation, but instead relies on a simple hardware architecture. The logic is implemented using field programmable gate array (FPGA) technology. The ALS platform is nuclear safety related (Class 1E) and has been developed by Westinghouse Electric Company[4], a 10 CFR Part 50, Appendix B supplier.

In late 2003, Wolf Creek Nuclear Generating Station had a need to replace the safety-related I&C systems due to reliability and obsolescence issues. Based on this need and the fact that no viable solutions existed in the market place, Wolf Creek began working towards a new approach. In early 2004, Wolf Creek partnered with CS Innovations on a new approach to replacing safety related I&C systems. As a result of this partnership, the ALS architecture was proposed as a general safety platform to target the U.S. Nuclear Power Plant (NPP) Safety Related I&C System market.

The ALS platform is designed as a universal safety system platform. The ALS provides advanced diagnostics and testability features. The reliability of the system increases due to the simplicity of the ALS architecture and incorporation of advanced design processes for system development. Issues associated with future obsolescence are solved by incorporating a simplified board level design and maintaining proven logic in an abstracted form in the event that the underlying hardware is required to be updated in the future. This eliminates the issue of essentially starting from scratch with each update.

The ALS is a modular platform where generic modules, referred to as ALS boards, can be combined in various configurations to solve a wide variety of nuclear safety applications. This also provides scalability allowing for a single system upgrade up to a full set of safety system upgrades using the same ALS platform.

The ALS platform incorporates two possible levels of diversity: Core Diversity and Embedded Design Diversity.

The first level, Core Diversity, is implemented for each of the FPGAs on all of the ALS boards. The diversity between the two cores is achieved by changing the logic implementation during the synthesis and Place & Route process. The second level of diversity, Embedded Design Diversity, implements additional design diversity. The final result is two diverse FPGA images, A and B, which implement the same functionality in a diverse manner.

---

3 This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the companies named.

4 The ALS platform was originally developed by CS Innovations, a 10 CFR Part 50, Appendix B (Reference 1) supplier, which later became a wholly owned subsidiary of Westinghouse Electric Company. The subsidiary no longer exists and the product is now fully owned, developed and maintained by Westinghouse Electric Company.

The level of diversity employed for a particular application is determined by the complexity of the application.

C.3 Westinghouse's life cycle management process

The ALS platform development were structured to follow a traditional waterfall life cycle that includes a top-down requirement and specification development, design implementation, and a bottoms-up verification and validation (V&V) effort at each level of integration. Prototyping activities and in-process quality assurance efforts were executed integral to the development stages.

The documentation needed for licensing [by the NRC] was developed according to ISG-06, Interim Staff Guidance 6 – Task Working Group #6: Digital I&C Licensing Process, Revision 1 (Initial Issue for Use), ML110140103, U.S. Nuclear Regulatory Commission.

V&V activities were performed in a bottoms-up fashion that progresses from the FPGA digital logic programming level, to the board level, and then to the system level. V&V was performed by the Independent Verification and Validation (iV&V) team which constitute the formal iV&V process. Westinghouse's iV&V team is independent in management, schedule, and finance.

C.4 Standards, guidelines and regulatory compliance

C.4.1 Equipment qualification

The ALS test program for equipment qualification includes the following:

- Environmental qualification;
- Seismic qualification;
- EMC qualification;
- Fault/isolation qualification;
- Software qualification.

C.4.2 Environmental qualification

The ALS platform hardware was qualified for Class 1E applications installed in a mild environment. To comply with the requirements of GDC 4, 10 CFR 50.49, and IEEE 603-1991, the qualification program was performed in accordance with IEEE Standard 323-1974 and IEEE Standard 323-2003.

C.4.3 Seismic qualification

The ALS platform hardware was qualified for Class 1E safety functions and operations per IEEE Standard 344-1987.

Clause 4 of IEEE Standard 344-1987 and Clause 5 of IEEE Standard 344-2004 state that the seismic qualification of Class 1E equipment should demonstrate an equipment's ability to perform its safety function during and after the time it is subjected to the forces resulting from one safe shutdown earthquake (SSE). In addition, the equipment must withstand the effects of a number of operating basis earthquakes (OBEs) prior to the application of an SSE.

To demonstrate that the ALS platform hardware functions during a seismic event, the test specimen was subjected to a series of seismic simulation tests using a tri-axial seismic shake table. These tests included resonance search tests, five OBE tests, and an SSE test.

C.4.4 EMC qualification

The ALS platform hardware was qualified for electromagnetic compatibility per Regulatory Guide 1.180 Rev. 1. The specific test methods found in MIL-STD-461E and the IEC 61000 series that have been endorsed by Regulatory Guide 1.180 are applied to the ALS platform hardware. These tests are reasonable methods of evaluating the effects of conducted and radiated electromagnetic interference (EMI), radiofrequency interference (RFI), and power surges on safety related I&C systems.

C.4.5 Fault/isolation qualification

The ALS platform hardware was qualified for safety/non-safety (Class 1E/Non-1E) and inter-divisional interfaces per Regulatory Guide 1.75 Rev. 3 and IEEE 384-1992 for independence of Class 1E circuits.

C.4.6 Software qualification

The ALS platform software has been verified and validated in accordance with Regulatory Guide 1.168 Revision 1 and IEEE 1012-1998.

Software verification and validation (V&V) is a technical discipline of systems engineering. The purpose of software V&V is to help the development organization build quality into the software during the software life cycle. The software V&V processes determine if development products of a given activity conform to the requirements of that activity, and if the software satisfies the intended use and user needs.

C.4.7 Regulatory compliance

To fulfil the regulatory requirements the ALS-platform was designed to fulfil the following standards and guidelines:

- IEEE 603 – IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations
- IEEE 7-4.3.2 – Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations
- DI&C-ISG-04 – Highly-Integrated Control Rooms – Communications Issues
- BTP 7-14 – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- BTP 7-19 – Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems
- Regulatory Guide 1.152 – Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
- DI&C ISG-06 – Digital I&C Licensing Process

C.4.8 Review by NRC

The ALS-platform has been reviewed and approved by the NRC – U.S. Nuclear Regulatory Commission.

C.4.9 Review of equipment qualification

The NRC reviewed the “ALS Topical Report,” “ALS EQ Plan,” and “ALS Platform EQ Summary Report” and determined the manufacturer’s equipment qualification conforms to Regulatory Position 1’s preference for type testing, as provided in the RG 1.209, “Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants,” because the ALS platform manufacturer performed type testing on seven standardized circuit boards, a backplane, and a chassis using a set of FPGA programs representative of production FPGA programs. The NRC further determined whether

the manufacturer documented its equipment qualification in a manner that supports evaluations by applicants and licensees to determine whether the ALS platform equipment qualification meets its environmental qualification program and demonstrates its plant-specific safety equipment's safety functions will remain functional during and following its design basis events.

C.4.10 Review of regulatory compliance

C.4.10.1 Compliance to IEEE 603

The platform topical report was evaluated against its ability to support the application-specific system provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." The NRC staff's evaluation is based on the guidance contained in SRP Chapter 7, Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std 603," which provides acceptance criteria for this standard.

The NRC determined the ALS platform supports meeting various sections and clauses of IEEE Std 603-1991, an applicant or licensee referencing the ALS Safety Evaluation Report should identify the approach taken to meet each applicable clause of IEEE Std 603-1991. The applicant or licensee should consider its plant-specific design basis because the "ALS Topical Report" scope is limited. The Safety Evaluation report does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. Therefore, an applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std 603-1991 clause to its application-specific ALS-based safety system or component. Also the applicant or licensee should demonstrate the plant-specific and application-specific use of the ALS platform meets the applicable IEEE Std 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

C.4.10.2 Compliance to IEEE 7-4.3.2

Equipment based on ALS platform components is intended for use in safety systems and other safety-related applications. Therefore, the platform topical report was evaluated against its ability to support the application-specific system provisions of Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." RG 1.152, "IEEE Standard Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," states conformance with the requirements of IEEE Std 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for meeting the Commission's regulations with respect to high functional reliability and design requirements for computers used in safety systems of nuclear power plants. The NRC's evaluation is based on the guidance contained in SRP Chapter 7, Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," which provides acceptance criteria for this standard.

The NRC determined the ALS platform supports meeting various sections and clauses of IEEE Std 7-4.3.2-2003. An applicant or licensee referencing The Safety Evaluation Report should identify the approach taken to meet each applicable clause of IEEE Std 7-4.3.2-2003. The applicant or licensee should consider its plant-specific design basis, because the "ALS Topical Report" scope is limited. The Safety Evaluation Report does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with their direct and indirect consequences. The applicant or licensee should identify its plant-specific design basis for its safety system application and the applicability of each IEEE Std 7-4.3.2-2003 clause to its application-specific ALS-based safety system or component.

C.4.10.3 Additional compliance

Compliance to DI&C-ISG-04, BTP 7-14, BTP 7-19, Regulatory Guide 1.152 as well as DI&C ISG-06 and other referenced standards and guidelines has also been reviewed by the US NRC staff and further information to be found in "U.S. Nuclear Regulatory Commission Safety

Evaluation for Topical Report 6002-00301 “Advanced Logic System Topical Report” “: http://pbadupws.nrc.gov/docs/ML1321/ML13218A979.pdf.

C.5 NRC conclusion

During the review, several requests for additional information were submitted by the NRC and were responded to by the applicant. During the review process, the NRC additionally performed audits at several of the facilities involved in the development of the ALS-platform.

The NRC staff determined the ALS platform, consisting of standardized circuit boards, their design features, and the processes to produce them support meeting the applicable regulatory requirements for plant-specific and application-specific use within safety-related I&C systems when each plant-specific and application-specific use meets the limitations and conditions defined. The NRC staff determined the ALS platform can be used in safety-related systems to provide reasonable assurance of adequate protection of public health, safety, and security, which applies current and applicable regulatory evaluation criteria. On this basis, the NRC staff determined the ALS platform is acceptable for use in safety-related I&C systems.

Annex D
(informative)

Review of CTEC's FirmSys platform qualification[5]

D.1 General

China Techenergy Co. Ltd. (CTEC), a joint venture co-funded by China Guangdong Nuclear Power Group and Beijing Hollysys Co. Ltd., does engineering design of digital I&C systems, system integration, and technical service for nuclear power plants.

CTEC has developed the digital instrumentation and control (I&C) platform FirmSys to be used in systems important to safety for nuclear power plants (NPP). In order to qualify the FirmSys platform for the international market, CTEC asked ISTec to carry out – as third party – the independent verification and validation (IV&V) of the FirmSys platform software.

D.2 IV&V procedure

The IV&V was performed by ISTec and assisted by the V&V team of CTEC. The V&V team of CTEC is independent from the development team of CTEC. ISTec has been responsible for the overall IV&V works and results approval. Any issues raised by the IV&V tasks were collected in Lists of Open Points (LOP). The LOP collected the IV&V findings in tables of minor issues, requests and key issues. Compliance with standard requirements is documented in specific tables of the LOP.

All open points have been clarified by the development team of CTEC. The clarification results were verified and closed by ISTec assisted by the V&V team of CTEC. The overall software assessment activities and assessment results were compiled in assessment reports. The assessment reports summarize the contents of the LOPs and give the assessment conclusions. In addition, the assessment reports give detailed reference to the assessed documents and code files. The referenced data is uniquely identified by checksums using the method of RIPEMD-160. Together with the assessment reports ISTec issued certificates. The certificates corroborate the basic suitability of FirmSys platform concept and software, and the FirmSys software safety modules for the use to implement the software of I&C functions important to safety in NPP.

The assessment was performed in form and content, applying the requirements of the standards given in Table D.1 and with respect to the consistent transition of one phase to the other within the software safety life cycle. In order to locate potential deficiencies all assessed documents were subjected to:

- formal check;
- consistency check, and
- functional check.

In addition, the following analyses were performed for the development documents:

- criticality analysis;
- requirements allocation analysis;
- traceability analysis;
- interface analysis;

5 This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the companies named.

- hazard analysis;
- security analysis, and
- Risk analysis.

For the test documents, the following analyses were applied:

- Traceability analysis;
- Hazard analysis;
- Security analysis, and
- Risk analysis.

D.3 Assessment criteria

The detailed assessment has been carried out in order to prove compliance of the software and its development life cycle with the requirements based on the international standards as listed in Table D.1. In case of IEEE Std 7-4.3.2™-2010 also the differences to the former version from the year 2003 were taken into account during assessment.

Table D.1 – Standards applied

No.	Standards
1	IEC 61513:2011, Nuclear power plants – Instrumentation and control important to safety – General requirements for systems, Ed. 2.0, 2011-08
2	IEEE Std 7-4.3.2™-2010, Standard criteria for digital computers in safety systems of nuclear power generating stations, 2010-08
3	IEC 60880:2006, Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, Ed. 2.0, 2006-05
4	IEC 62566:2012, Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions, Ed.1.0, 2012-01
5	IEEE Std 1012™-2004, IEEE Standard for Software Verification and Validation, 2005-06

The international standard IEC 61513:2011 provides requirements on system aspects of digital I&C systems important to safety. The international standard IEEE Std 7-4.3.2™-2010 mainly focuses on safety systems of NPP. Of particular importance for the assessment are the international standards IEC 60880:2006 and IEEE Std 1012™-2004. IEC 60880:2006 provides requirements for the software of computer-based I&C for safety systems of NPP. IEEE Std 1012™-2004 describes processes and activities for software V&V depending on the software integrity level. IEC 62566:2012 describes development requirements of programmable devices which are based on hardware description language (HDL) and are important to NPP safety I&C system performing category A functions.

D.4 Assessment scope

The assessment has been applied to the development documentation and test documentation of the FirmSys platform concept and software, the software safety modules, the CPLD logic software in net communication modules, code transformation modules of the engineering workstation software, and of the function block library of application software. These documents cover relevant process and product issues.

The IV&V procedure contained activities for requirements analysis, design, coding and testing. The activities were organized according to the software life cycle phases as applied to the FirmSys platform concept and software, and to the software safety modules.

Annex E
(informative)

Review of SOOSAN ENS's POSAFE-Q platform qualification[6]

E.1 Presentation of POSAFE-Q PLC

POSAFE-Q, which meets international standards such as IEEE 7-4.3.2 and EPRI TR-107330 is a safety grade Q Class 1E PLC-based I&C platform for nuclear power plant. Therefore hardware platform was qualified and system software running on it was reviewed by CT, IT, ST and SIT. Additionally the verification and validation according to international standards by IEEE 1012 and IEEE 1074 was conducted to ensure the highest level of availability, safety and reliability. POSAFE-Q also went through a variety of analysis procedures including reliability analysis, safety analysis, and EQ (Equipment Qualification) testing and analysis. Based on all of these efforts, POSAFE-Q has been certified for its reliability and safety by the authorized institutions.

E.2 Equipment qualification

The POSAFE-Q qualification program as below is applied to ensure the operation in generic plant condition and plant-specific operating conditions according to the relevant international standards:

- Environmental qualification;
- EMC qualification;
- Seismic qualification.

a) Environmental qualification

The POSAFE-Q hardware was qualified for Class 1E applications installed in a mild environment. The qualification was performed in design temperature, pressure and humidity including aging analysis in accordance with IEEE Standard 323.

b) EMC qualification

The POSAFE-Q hardware was qualified for electromagnetic compatibility in accordance with Regulatory Guide 1.180, EPRI TR-102323 and IEC 61000 series in order to show that I&C platform including hardware and software is fault-free from conducted and radiated electromagnetic interference (EMI), radiofrequency interference (RFI), and power surges.

c) Seismic qualification

The POSAFE-Q hardware was qualified for Class 1E safety functions and operations per IEEE Standard 344. According to IEEE Standard 344, seismic qualification of Class 1E equipment demonstrated an equipment's ability to perform its safety functions before, during and after Operating Basis Earthquake (OBE) and Safe Shutdown Earthquake (SSE). To demonstrate the physical and functional integrity of POSAFE-Q PLC platform during a seismic event, the test specimen was subjected to a series of seismic simulation tests including resonance search tests, five OBE tests, and one SSE test using a tri-axial seismic shake table.

6 This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of the companies named.