IEC TR 63084

Edition 1.0 2017-06

TECHNICAL REPORT

colour inside

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-4316-9

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 8
1.1 General 8
1.2 Framework 8
2 Normative references 9
3 Terms and definitions 9
4 Abbreviated terms 13
5 I&C platform versus I&C system 15
5.1 General – Structure of the platform qualification 15
5.2 I&C platform as an object of qualification – Conceptual design 16
5.3 Documentation of the I&C platform 16
6 Platform qualification 17
6.1 Organisation of the qualification 17
6.1.1 General 17
6.1.2 Parties involved 18
6.2 Scope of the qualification 19
6.2.1 Hardware modules 19
6.2.2 Operational system software 20
6.2.3 Application software 21
6.2.4 Tools 21
6.2.5 Integration to a representative system 21
6.3 Methods of qualification 22
6.3.1 General 22
6.3.2 Type testing 22
6.3.3 Operating experience 23
6.3.4 Analyses 23
6.4 Documentation of qualification results 24
6.5 Maintenance of qualification 24
7 Dependency on the platform through life-cycle of the I&C system 26
7.1 General 26
7.2 Models of cooperation between the parties of the I&C system project 26
7.3 Platform environment for implementation of applications 26
7.3.1 Platform supported procedures for I&C system implementation 26
7.3.2 Tool-based implementation – Kind of tools required 28
7.3.3 Application software development 28
7.4 I&C system integration, validation and commissioning 29
8 Conclusions 30
Annex A (informative) Issues of the Finnish licensing approach 31
Annex B (informative) Review of Areva's TELEPERM XS platform qualification 35
Annex C (informative) Review of Westinghouse ALS platform qualification 37
C.1 General 37
C.2 Introduction and ALS-background 37
C.3 Westinghouse’s life cycle management process 38
C.4 Standards, guidelines and regulatory compliance 38

C.4.1 Equipment qualification 38
C.4.2 Environmental qualification 38
C.4.3 Seismic qualification 38
C.4.4 EMC qualification 39
C.4.5 Fault/isolation qualification 39
C.4.6 Software qualification 39
C.4.7 Regulatory compliance 39
C.4.8 Review by NRC 39
C.4.9 Review of equipment qualification 39
C.4.10 Review of regulatory compliance 40
C.5 NRC conclusion 41
Annex D (informative) Review of CTEC's FirmSys platform qualification 42
D.1 General 42
D.2 IV&V procedure 42
D.3 Assessment criteria 43
D.4 Assessment scope 43
Annex E (informative) Review of SOOSAN ENS's POSAFE-Q platform qualification 44
E.1 Presentation of POSAFE-Q PLC 44
E.2 Equipment qualification 44
E.3 Software verification and validation 45
E.4 Reliability analysis 46
E.5 Regulatory compliance 46
Annex F (informative) Review of Rolls-Royce's Spinline platform type approval 47
F.1 Overview 47
F.2 Type approval 47
F.3 Type approval process 48
Bibliography 50

Figure 1 – Platform and application development process 15
Figure 2 – General overview of a typical qualification process 16
Figure 3 – Process for maintaining the platform qualification 25
Figure 4 – Life cycle procedures/tasks of the I&C system implementation 27
Figure 5 – Application development based on the project library (V-for vendor, O-for owner) 29
Figure B.1 – Software type test procedure 35

Table D.1 – Standards applied 43
Table F.1 – International IEC standards applied for the assessment 48

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL IMPORTANT TO SAFETY – PLATFORM QUALIFACTION 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 QUALIFACTION 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*