



Nuclear Power Plant Krško

Quality Assurance Specification


Nuklearna Elektrarna Krško MASTER DOCUMENT	
Date Received:	09 -11- 2017
Log Number:	247741

Generic Software Quality Assurance Program Requirements

QS-600
Revision 1

Safety Related

Prepared by:

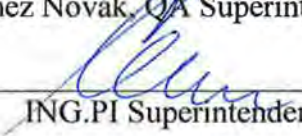

Damijan Gregorič, QA Lead Engineer

Date: 27 / 10 / 2017

Reviewed by:

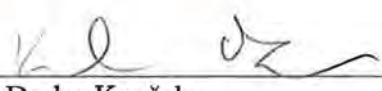

Janez Novak, QA Superintendent

Date: 8 / 11 / 2017


ING.PI Superintendent

Date: 8 / 11 / 2017

Approved by:


Darko Kavšek,
Quality and Nuclear Oversight Director

Date: 9 / 11 / 2017



RECORD OF CHANGE

Revision	Description of the Change
1	<p>Revision of the specification is based on recommendations in document INPO 12-014 <i>Nuclear Power Plant Software Quality Assurance</i> (Revision 1, April 2015). The revision of the specification is requested in NEK Corrective Action Program Request 2012-4380.</p> <p>The major changes in the specification:</p> <ul style="list-style-type: none">• Instead of the term Quality Assurance Program, the term Software Quality Assurance Program (SQAP) is used throughout the specification.• The definitions in section 2.0 are harmonized with definition in standards (ANSI N45.2.10-1973 and IEEE 610.5-1990), plant programs and plant procedures.• The section 4.0 (references) is new and contains all documents referenced in the specification.• Section 3.6 is corrected to emphasize Software Development Life Cycle as recommended in the document INPO 12-01.• In section 6.6.3, the required documents for Software Development Life Cycle are specified. The selection of required documents is based on the software quality level.• Sections 6.7, 6.12 and 6.13 are corrected in accordance with recommendation in the document INPO 12-014.
0	Initial issue.

TABLE OF CONTENTS

1. GENERAL.....	4
2. DEFINITIONS	4
3. ABBREVIATIONS:	6
4. REFERENCES.....	7
5. DOCUMENTS FOR SUBMISSION	7
6. SOFTWARE QUALITY ASSURANCE PROGRAM REQUIREMENTS	7
6.1. Organization	7
6.2. Software Quality Assurance Program elements	8
6.3. Software Design, Development, Modification and Testing (Software Development Cycle)	8
6.4. Procurement.....	9
6.5. Instructions, Procedures, and Drawings	10
6.6. Document and Records.....	10
6.7. Configuration Management.....	11
6.8. Control of Purchased Items and Services	11
6.9. Corrective Action	12
6.10. Software Error Management	12
6.11. Quality Assurance Records	12
6.12. Review and Inspection.....	13
6.13. Audits	14
7. NEK AUDITS.....	14

1. GENERAL

- 1.1. This specification establishes the Supplier's software quality assurance program requirements that shall apply to all activities affecting the quality of the items or services provided.
- 1.2. Supplier shall assure compliance with the requirements of this specification and all other codes or standards referenced herein and in the purchase order.
- 1.3. For Safety Related software and services on safety related item the following shall apply:
 - 1.3.1. Supplier shall assure compliance with the requirements of Title 10, Code of Federal Regulations, Part 50, Appendix B (10CFR50, Appendix B), "*Quality Assurance Criteria for Nuclear Power Plants*".
 - 1.3.2. The reporting and posting requirements of Title 10, Code of Federal Regulations, Part 21 (10CFR21), "*Reporting of Defects and Noncompliance*".
- 1.4. NEK shall have the right of access to enter the premises of the Supplier to witness inspection/test activities or to conduct surveillances or quality assurance audits.
- 1.5. Supplier shall assure that its Subsuppliers conform to the requirements of this specification.

2. DEFINITIONS

The word *shall* identifies mandatory requirements strictly to be followed in order to conform to this specification. The words *should* and *may* indicate optional requirements that are not required in order to conform to this specification.

Definition shall be as stated in ANSI N45.2.10-1973, "*Quality Assurance Terms and Definition*" and IEEE 610.5-1990, "*IEEE Standard Glossary of Data Management Terminology*" with the following exceptions:

- 2.1. **Application software** – Software specifically produced for the functional use of a computer system; software for structural analysis, process control, etc.
- 2.2. **Audit** – An independent review for assessing compliance with software requirements, specifications, baselines, standards, procedures, instructions, codes, and contractual and licensing requirements.
- 2.3. **Augmented quality item** – An optional subset of the classification Non Safety Related applied to any item that is subject to non-safety related regulatory requirements or special requirements (seismic tests, analysis reports, commercial QA program, manufacturing and QC inspection plan ...) imposed by NEK. Classification category AQ includes specific items which are very important for plant reliability and operability (design and manufacturing of those items is specific and complex).
- 2.4. **Configuration management** – The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the software development cycle, recording and reporting the status of configuration items and change requests.



- 2.5. **Critical digital asset** – Digital device or system that plays a role in the operation or maintenance of a critical system and can impact the proper functioning of the critical system. A CDA may be a component or a subsystem of a critical system, the CDA may itself be a critical system, or the CDA may have a direct or indirect connection to a critical system.
- 2.6. **Graded approach** – The selective assignment of the quality assurance elements the software must comply with, based on its assigned quality classification. The quality classification is determined by evaluation of the functional process(es) the software provides.
- 2.7. **Item** – An all-inclusive term used in place of any of the following: appurtenance, assembly, component, equipment, material, module, part, structure, subassembly, subsystem, system, or unit.
- 2.8. **Non-Safety related item** – Any item that does not perform a Safety Related function and the failure of which would not prevent the accomplishment of a Safety Related function.
- 2.9. **Quality assurance** – Planned and systematic actions necessary to provide adequate confidence that the computer software and hardware conforms to established technical requirements.
- 2.10. **Safety related item** – Any item used in a nuclear power plant that is relied upon during or following design basis events to ensure: the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and maintain it in a safe shutdown condition; or the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to those referred to in 10 CFR 100.11.
- 2.11. **Service** – Carrying out software development cycle activities on an item.
- 2.12. **Software development cycle** – The period of time between the decision to develop a software product and the delivery of software product. The specific SQAP should identify and document the software development cycle and accompanying development cycle phases to be used. Although the typical development cycle phases are identified below, many types of software development cycles may be defined. Phases associated with software development may include the following:
 - Planning evaluation of options and coordination of activities to ensure successful deployment of software
 - Requirements specific and measurable characteristics that describe the intended use and performance of software
 - Design the collection of information (requirements, architecture, etc.) that define software Implementation
 - Implementation the process of translating the Design into software components
 - Integration the process of combining software components with other software and/or systems and to reduce the introduction of undesirable characteristics (errors, anomalies, hazards, security threats)
 - Validation specific and measurable tests to demonstrate that software meets the Requirements



- Installation placing software into the operational computing environment, documenting its baseline configuration, and performing final acceptance testing
- 2.13. **Software error** – A discrepancy between the computed, observed, or measured value or condition, and the true, specified, or theoretically correct value or condition.
- 2.14. **Software quality assurance** – The program that establishes quality controls for the development, procurement, operation, use, maintenance, and retirement of software, commensurate with its importance to nuclear safety.
- 2.15. **Software** – Computer programs and data files that contain programmer-specified constants, flags and setpoints. Software includes programs that generate displays of plant system configurations, technical specification applicability, and similar items that operators and technical personnel rely on when operating the plant.
- 2.16. **Software tool** – Refers to all computer programs, procedures and/or data files containing programmer specified constants, flags, and set-points. This includes programs that generate displays of the plant system configurations, provide information about technical specification applicability, and similar items relied upon by operators and technical personnel to operate the plant. All program files, sets of instructions and data files are considered as software, no matter if they are stored as a firmware or if they are stored as a data in a computer (PLC, controller) memory or other memory storage device.
- 2.17. **Testing** – The process of exercising or evaluating a system or system component by manual or automated means, to verify that it satisfies specified requirements or to identify differences between expected and actual results.
- 2.18. **Validation** – The process of providing evidence that the software and its associated products satisfy system requirements, allocated to software, at the end of each life cycle activity, solve the problem (e.g., correctly model physical laws, implement business rules, use the proper system assumptions) and satisfy intended use and user needs.
- 2.19. **Verification** – The process of providing objective evidence that the software and its associated products conform to requirements (e.g., for correctness, completeness, consistency, accuracy) for all life cycle activities during each Software Development Cycle phases; satisfy standards, practices, and conventions during Software Development Cycle phases; and successfully complete each Software Development Cycle activity and satisfy all the criteria for initiating subsequent life cycle activities (e.g., building the software correctly).

3. ABBREVIATIONS:

10CFR21	abbreviation for reference 4.2
10CFR50, Appendix B	abbreviation for reference 4.1
ANSI	American National Standard Institute
AQ	Augmented quality
SQA	Software Quality Assurance
SQAP	Software Quality Assurance Program
SR	Safety related
NEK	Nuklearna elektrarna Krško – Krško Nuclear Power Plant

4. REFERENCES

- 4.1. Title 10, Code of Federal Regulations, Part 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants"
- 4.2. Title 10, Code of Federal Regulations, Part 21, "Reporting of Defects and Noncompliance"
- 4.3. ASME NQA-1-2008, Addenda 2009/2011 "Quality Assurance Requirements for Nuclear Facility Applications"
- 4.4. ANSI N45.2-1977, "Quality Assurance Program Requirements for Nuclear Power Plants"
- 4.5. ANSI N45.2.9-1979, "Collection, Storage, and Maintenance of Quality Assurance Records for Nuclear Power Plants".
- 4.6. INPO 12-014; Nuclear Power Plant Software Quality Assurance; Revision 1; April 2015
- 4.7. Title 10, Code of Federal Regulations, Part 73, "Physical Protection of Plants and Materials"
- 4.8. Regulatory guide RG 5.71, Cyber Security Programs for Nuclear Facilities, January 2010
- 4.9. Engineering Services Manual ED-11, Process Computer Configuration Control Program, rev. 2, June 2017
- 4.10. Security Manual SP-3, Cyber Security Program, Revision 1, Nuclear Power Plant Krško, February 2016
- 4.11. ESP-2.912, Documentation of New Application for Process Control and Process Computer Systems, current revision, Nuclear Power Plant Krško
- 4.12. ESP-2.950, Process Computer Design Change, Nuclear Power Plant Krško
- 4.13. ESP-2.602, Plant Design Modification, Nuclear Power Plant Krško

5. DOCUMENTS FOR SUBMISSION

Supplier shall submit for NEK review one controlled copy of the final approved Supplier's Software Quality Assurance Program (SQAP) for the scope of work to be performed.

6. SOFTWARE QUALITY ASSURANCE PROGRAM REQUIREMENTS

Supplier shall develop and implement Software Quality Assurance Program (SQAP) consistent with the requirements defined herein. As a minimum, the program shall address the following quality assurance criteria:

6.1. Organization

The organizational structure, functional responsibilities, levels of authority, and lines of communication for personnel performing activities that affect quality shall be documented in organizational charts and/or written procedures.

- 6.1.1. Supplier's Quality Assurance personnel shall have sufficient and well defined responsibility, authority, and organizational freedom to identify and evaluate quality problems, to demand implementation of approved corrective action, and to verify implementation of corrective actions. Such



persons or organizations shall report to a management level such that required authority and organizational freedom are provided, including sufficient independence from cost and schedule considerations.

- 6.1.2. Supplier's personnel responsible for verifying that Supplier's work conforms to the established requirements shall not have direct responsibility for the work performed.

6.2. Software Quality Assurance Program elements

The documented Software Quality Assurance Program (SQAP) shall be planned, implemented, and maintained to identify the items and services to which it applies.

- 6.2.1. The SQAP shall define scope and applicability of the SQAP.
- 6.2.2. The SQAP shall provide and document criteria to classify software to reflect in quality levels using a graded approach in accordance with NEK procedure ESP-2.950 (reference 4.12).
- 6.2.3. The program shall provide for planning and accomplishing activities affecting quality under suitably controlled conditions.
- 6.2.4. The program shall provide for any special controls, processes, and skills necessary to attain the required quality and provide for verification of quality by test, as necessary.
- 6.2.5. The program shall provide for indoctrination and training of personnel performing activities affecting quality to assure that suitable proficiency is achieved and maintained.
- 6.2.6. Supplier's management shall regularly review the status and adequacy of the documented quality assurance program.
- 6.2.7. Measures shall be established for the control and distribution of the documented quality assurance program.

6.3. Software Design, Development, Modification and Testing (Software Development Cycle)

Supplier's SQAP for controlling activities in software development cycle according to its quality classification shall satisfy the following requirements:

- 6.3.1. Identify and document the procedures for software design, development, modification and test activities.
- 6.3.2. Design development and modification activities shall satisfy the requirements of NEK Engineering Service Manual ED-11 (reference 4.9).
- 6.3.3. Those activities shall be prescribed to ensure that requirements of this specification and all other codes or standards referenced herein and in the purchase order are correctly transferred into Software Development Cycle.
- 6.3.4. The Software Development Cycle shall assure secure cyber environment in accordance 10 CFR 73.54 (reference 4.7) and RG 5.71 (reference 4.8). Those requirements are encapsulated in NEK Security Manual SP-3 (reference 4.10)
- 6.3.5. Identify and document the procedures by which technical and management reviews are conducted and documented to verify the software development



cycle activities utilized to demonstrate acceptable performance and the correctness of documentation, prior to the delivery of program capabilities to the customer.

- 6.3.6. Identify and document the procedures used to formally approve or certify the acceptability of performance, correctness of documentation and attainment of program requirements.
- 6.3.7. Require monitoring to assure compliance with its procedures.
- 6.3.8. Software development cycle documentation standards and practices to be used for software design, development, modification and test for all software shall be referenced or documented in the SQAP. The SQAP shall reference or document the procedures to be applied to assure compliance with standards, practices, and delivery of correct documentation and change information to the NEK.
- 6.3.9. The SQAP shall require independent review of documentation and designation of Supplier's approval authority.
- 6.3.10. Acceptance tests should be carried out at the vendor's facility and at the customer's facility to demonstrate that the software performs as expected.
- 6.3.11. The program shall identify and document the evaluation, review, change, test and acceptance of software tools used in software development cycle as part of the software development cycle.

6.4. Procurement

Supplier's SQAP for controlling procurement documents shall satisfy the following requirements:

- 6.4.1. Applicable design bases, quality assurance requirements, and other requirements necessary to assure adequate quality shall be included or referenced in documents for procurement of items and services.
- 6.4.2. Procurement documents shall require Subsupplier to have a quality assurance program consistent with the applicable requirements of this specification.
- 6.4.3. The procurement documents shall provide for access to the Subsupplier facilities and records for inspection or audit by the Supplier.
- 6.4.4. Procurement documents shall identify the documentation required to be submitted.
- 6.4.5. Procurement documents shall include Supplier's requirements for reporting and approving disposition of nonconformance.
- 6.4.6. A review of the procurement documents shall be performed to assure that the documents include appropriate technical and quality requirements.
- 6.4.7. Procurement document changes that affect technical or quality specifications shall be subject to the same degree of control as used in preparing the original document.

6.5. Instructions, Procedures, and Drawings

- 6.5.1. Instructions, Procedures, and Drawings prescribing software development cycle shall be reviewed, approved, and controlled.
- 6.5.2. Supplier shall assure that documented instructions, procedures, or drawings prescribe all software development cycle activities.
- 6.5.3. Instructions, procedures, or drawings shall include appropriate quantitative or qualitative criteria for determining that software development cycle activities have been satisfactorily accomplished.
- 6.5.4. Instructions, procedures, or drawings shall define development cycle requirements based on the software quality level category.
- 6.5.5. Instructions, procedures, or drawings shall provide guidance for managing software errors.
- 6.5.6. Instructions, procedures, or drawings shall contain QA record storage requirements for software development cycle documentation
- 6.5.7. SQA procedures should identify roles and responsibilities for those who develop and/or procure, own, maintain, and use quality software.

6.6. Document and Records

Supplier shall assure that Software development cycle documents, including changes, are reviewed for adequacy, approved for release by authorized personnel, and properly distributed to and used at locations where the prescribed activity is performed.

In the software development cycle that is applied by Supplier the name of the particular documents and the number of documents can differ from the requirements in this specification. In that case the correlation shall be established between software development cycle documents required by this specification and software development cycle documents applied by Supplier.

- 6.6.1. Software development cycle documents changes shall be reviewed and approved by the same organization that performed the original review and approval, unless other organizations are specifically designated.
- 6.6.2. Procedure governing document control shall be established and provide for:
 - 1. identification of individuals or organizations responsible for preparing, reviewing, approving, and issuing documents and revisions thereto,
 - 2. identifying the proper documents to be used in performing the activity,
 - 3. coordination and control of interface documents,
 - 4. ascertaining that appropriate documents are being used,
 - 5. establishing distribution lists.
- 6.6.3. Documents developed during the software development cycle to prove the quality of the software shall include one or more of the documents defined in NEK Engineering Service Manual ED-11 (reference 4.9) and NEK procedure ESP-2.912 (reference 4.11).



6.7. Configuration Management

- 6.7.1. Software Development Cycle Configuration Management shall comply with the requirement of NEK Engineering Service Manual ED-11 (reference 4.9).
- 6.7.2. The SQAP shall establish requirements for describing software to assure unique identification necessary to maintain configuration (name, version, platform ...).
- 6.7.3. The SQAP shall establish Software development cycle configuration change management control for ensuring the configuration control is maintained and that changes are evaluated and tested during the software development cycle activities (at the vendor facility) before the software is placed in service.
- 6.7.4. The SQAP shall reference or document the Supplier's procedures and controls for the control of configuration items, and permit traceability between configuration items of development cycle activities including development of upgrades for existing software, installation of new versions of software, or other activities that affect software version increments essential to establishing software baselines that define the basis for further development.
- 6.7.5. The SQAP shall establish baselines for software to define the basis for further development, allow control of configuration items, and permit traceability between configuration items.
- 6.7.6. The SQAP shall establish the requirements for configuration control of Software tools used in software development cycle. Changes to the software tool shall be evaluated for impact on the software product to determine the level of reviews and retesting that will be required. Software tools that do not affect the performance of the software need not be placed under configuration control.

6.8. Control of Purchased Items and Services

Supplier's program for controlling purchased items and services shall satisfy the following requirements:

- 6.8.1. The selection of Subsupplier shall be based on evaluation of their capability to provide items or services in accordance with the requirements of the procurement documents.
- 6.8.2. Methods to be utilized in evaluation of Subsupplier, and the results therefrom, shall be documented and shall include one or more of the following:
 - 1. Evaluating the Subsupplier's history of providing a product, which performs satisfactorily in actual use.
 - 2. Determining the Subsupplier's technical and quality capability by a review of its quality assurance program, and a direct evaluation of its facilities and the implementation of its quality assurance program.
- 6.8.3. Procedures shall be established and implemented for verification activities (surveillance, receipt inspection, and audit), as appropriate, to assure conformance of procured items and services to identified requirements.

- 6.8.4. Where acceptance is based on certifications from Subsupplier, the Supplier shall validate the certifications via surveillance, audit, and/or independent tests.

6.9. Corrective Action

Supplier shall assure that conditions adverse to quality are promptly identified and corrected.

- 6.9.1. In case of significant conditions adverse to quality, the cause of the condition shall be determined and corrective action taken to preclude recurrence.
- 6.9.2. Identification of significant conditions adverse to quality, the cause of the conditions, and the corrective action taken shall be documented and reported to appropriate levels of management. Follow-up action shall be taken to verify implementation of corrective action.

6.10. Software Error Management

- 6.10.1. The Supplier is responsible for analyzing software errors and notifying NEK of confirmed errors detected in Supplier software. The notification shall include a description of the error, advice on work-arounds for error avoidance, when applicable, a listing of all versions of the software that contained the error, when available, and the date the error was reported. Corrected errors will be noted.

1. Software error classification shall meet the following functional descriptions:
 - A. Problem results in incorrect answers.
 - B. Problem causes incomplete program execution or aborts.
 - C. Documentation of procedure file errors, inconveniences, or cautions, cannot be classified in either of the above definitions.
2. A copy of each error notification will be sent to the individual(s) identified in the procurement document.

- 6.10.2. The Supplier shall promptly notify NEK when software errors are confirmed and again when the errors are removed or corrected.

- 6.10.3. The Supplier shall maintain a log of all software errors detected in software.

- 6.10.4. If errors invalidate any sections of the verification report, such that a program user or calculation checker could not depend on specific sections of a verification report when making engineering designs and analysis, the Supplier shall promptly revise the verification report accordingly.

6.11. Quality Assurance Records

Supplier's SQAP shall establish the procedures to identify the specific records that will be generated and maintained during software development cycle activities and to prescribe their retention periods and storage requirements.

- 6.11.1. Define document control and records management requirements for software development cycle documentation.

- 6.11.2. Develop documentation sufficient to prove the quality of the software during its development cycle.
- 6.11.3. Records shall include drawings, specifications, purchase documents, work orders, material certifications, calculations, inspection and test reports, work procedures, nonconformance and corrective action reports, audit reports, and personnel, process, and equipment qualification records.
- 6.11.4. Inspection, test, and work performance monitoring records shall indicate the nature of observations, the acceptable limits of parameters checked, the qualitative or quantitative results, the actions taken in connection with any identified deficiencies, the date of the observation, and the identity of personnel involved.
- 6.11.5. Required records shall be legible, identifiable, and retrievable.
- 6.11.6. All maintained records shall have clear identification markings that can be traced to a specific job or item and be entered into a system that provides for timely retrieval.
- 6.11.7. Record retention periods and storage requirements for safety related software and services shall satisfy the requirements of ANSI N45.2.9-1979, *"Collection, Storage, and Maintenance of Quality Assurance Records for Nuclear Power Plants"*.

6.12. Review and Inspection

- 6.12.1. Seller's SQAP shall define the reviews and inspections to verify the software meets procurement specifications before it is released to NEK.
- 6.12.2. It shall establish controls to support reviews, testing and inspection of software and documentation prior to its release to NEK.
- 6.12.3. The supplier's SQAP shall reference or document procedures for assuring the accomplishment of the following:
 - 1. Analysis of software requirements to determine testability.
 - 2. Review of test requirements and criteria for adequacy, feasibility, and traceability and satisfaction of requirements.
 - 3. Review of test plans, procedures, and specifications to determine that the level of testing is sufficient to determine acceptable program performance.
 - 4. Verification that tests are conducted in accordance with approved test plans and procedures.
 - 5. Verification that test results are the actual findings of the tests.
 - 6. Review and verification of test reports.
 - 7. Ensuring that test-related media and documentation are maintained to allow repeatability of tests.
 - 8. The Supplier shall test all programs in a hardware and software environment equivalent to the operational environment at NEK.



6.13. Audits

Supplier's SQAP shall establish the measures for auditing the software development cycle process. The audit shall include the following assessments:

- 6.13.1. Measures are established to control software throughout the software development cycle.
- 6.13.2. Software development cycle activities are adequately and effectively reviewed.
- 6.13.3. Acceptance testing is adequate.
- 6.13.4. Measures are established and implemented to assure that software errors and failures from both internal and external sources are identified, documented, resolved, evaluated, assessed for impact on past and present applications, and resolved.

7. NEK AUDITS

- 7.1. NEK has the right to conduct an audit of Supplier's SQAP to determine Supplier's capability of satisfying quality assurance requirements herein and to verify that Supplier is implementing the SQAP as defined in Supplier's SQAP manual accepted by NEK. Supplier shall provide access to Supplier's facilities for the purpose of conducting an audit.
- 7.2. NEK may reject software, hardware and/or stop work, if it deems that software, hardware or service is not in accordance with the quality assurance requirements herein. Supplier shall not resume any work before completion off all corrective measures previously approved by NEK.