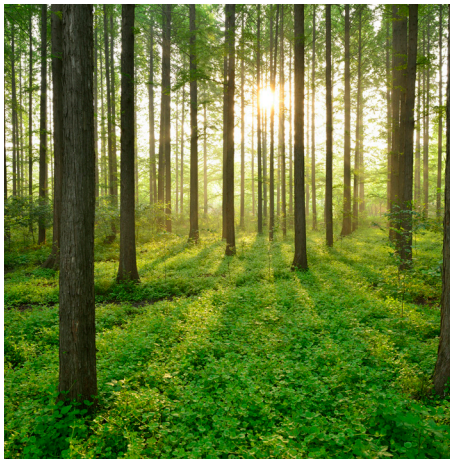
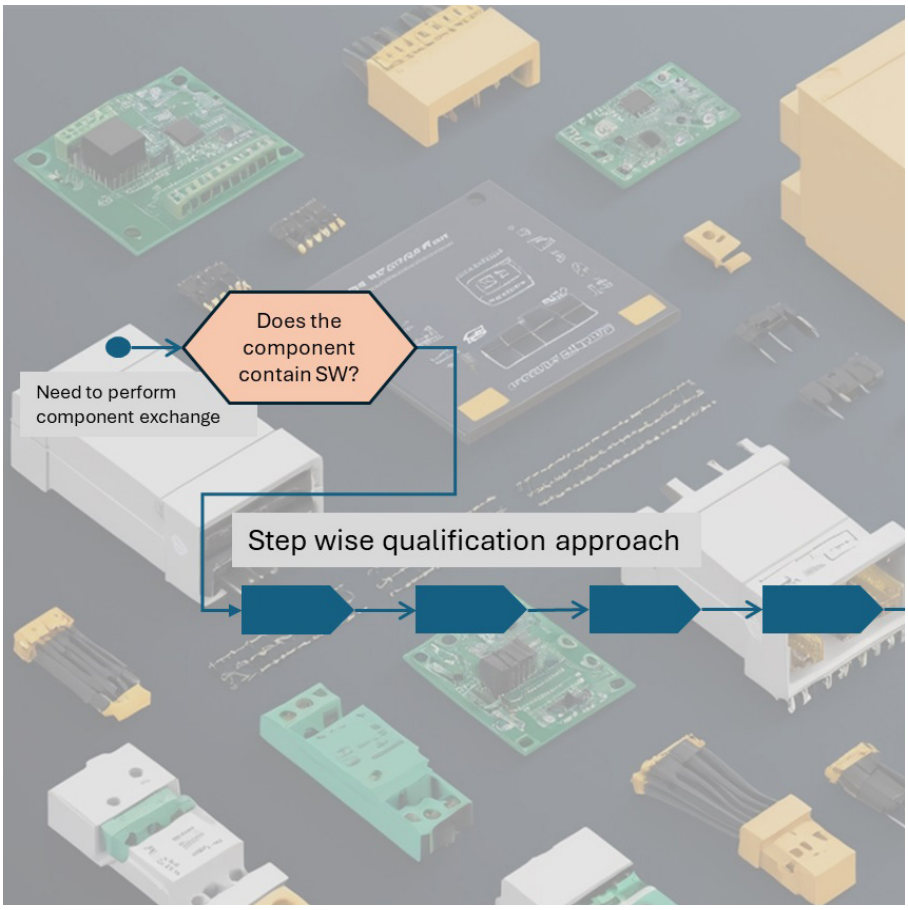
QUALITY ASSURANCE STRATEGIES WHEN UPGRADING DIGITAL I&C DEVICES

REPORT 2024:1036



ENERGIFORSK NUCLEAR SAFETY RELATED I&C, ENSRIC



Energiforsk

Quality Assurance Strategies when upgrading Digital I&C Devices

Step wise qualification for components containing software in a project process compatible with Nordic conditions.

MARIE-LOUISE AXENBORG & PONTUS RYD, SOLVINA AB

ISBN 978-91-89919-36-5 | © Energiforsk July 2024

Energiforsk AB | Phone: 08-677 25 30 | E-mail: kontakt@energiforsk.se | www.energiforsk.se

Foreword

The Energiforsk Nuclear Safety Related I&C (ENSRIC) Program aims to increase the knowledge of aspects affecting safety, maintenance and development of I&C systems and their components in the Nordic nuclear power plants. Part of this is to investigate possibilities to facilitate and simplify the work that is performed in the nuclear business.

Modern digital equipment contains different kinds of hardware components and software that require upgrades or new versions on a regular basis. These upgrades and exchanges produce a risk of introducing defects or unintentionally changed functionality. This study was initiated to identify, evaluate and recommend methods for handling upgrades and exchanges that minimize these risks, while taking plant safety, time and cost into account.

The study was carried out by Marie-Louise Axenborg and Pontus Ryd, Solvina AB. The study was performed within the ENSRIC Program, which is financed by Vattenfall, Uniper, Fortum, TVO, Skellefteå Kraft and Karlstads Energi,

These are the results and conclusions of a project, which is part of a research programme run by Energiforsk. The author/authors are responsible for the content.

Summary

Digital equipment often has functional advantages compared with analogue counterparts but at the same time carries increased risk of introducing defects or unintentionally changed functionality into the plant. Furthermore, equipment with software often requires regular maintenance in terms of minor upgrades or new software versions. The nature of software-based components also brings risks of functional impact that raises questions above the component level with possible system or plant level functional impact and must thus be handled as such. This requires a process that also take this into account and are not covered by the traditional hardware-oriented component level qualification and change approaches. Since the supply of equipment developed according to nuclear standards for nuclear applications is limited, it's necessary for NPPs to use commercially available components provided by suppliers who are not adapted to nuclear specific standards and not used to the nuclear specific requirements, which poses additional challenges to the qualification.

This project was initiated to evaluate possibilities for standardized methods and approaches for cost-effective management of upgrades and exchanges of components containing software and provided by suppliers. The methods should ensure that no new defects or unwanted changed functions are introduced into the NPP.

Based on feedback from interviews, own and international experience we believe that it is not possible to provide a generic "recipe" when it comes to components containing software as it depends on several factors including both component and Supplier qualities as well as NPP owners previous experience and capabilities. Instead, qualification activities are related to a generic process for upgrading digital I&C device to provide a simplified support for qualification in different project phases. The method is applicable to both safety, safety related and non-safety components and should be applied with a graded approach. It can be used to enhance or develop the NPP own processes for handling components that contains software.

Keywords

Nuclear, software, component, qualification, configuration management

Sammanfattning

Digital utrustning har ofta funktionella fördelar jämfört med analoga motsvarigheter men medför samtidigt förhöjd risk att fel eller oavsiktligt ändrad funktionalitet införs i anläggningen. Dessutom kräver utrustning med mjukvara ofta regelbundet underhåll i form av uppgraderingar eller nya mjukvaruversioner. Mjukvarubaserade komponenter medför också risker för funktionell påverkan utöver komponentnivå även på system- eller anläggningsnivå och måste hanteras därefter. Det krävs en process som tar hänsyn till detta vilket inte de traditionella hårdvaruorienterade kvalificerings- och ändringsprocesserna på komponentnivå gör. Eftersom utbudet av utrustning som utvecklats speciellt för kärnkrafttillämpningar enligt kärnkraftsspecifika standarder är snävt begränsat blir det nödvändigt för kärnkraftverk att använda kommersiellt tillgängliga komponenter som tillhandahålls av leverantörer som inte är anpassade till kärnkraftsspecifika standarder och inte vana vid de kärnkraftsspecifika kraven vilket skapar ytterligare utmaningar för kvalificeringen.

Detta projekt initierades för att utvärdera möjligheter till standardiserade metoder och tillvägagångssätt för kostnadseffektiv hantering av uppgraderingar och utbyten av komponenter som innehåller mjukvara och tillhandahålls av leverantörer. Föreslagna metoder ska säkerställa att inga nya fel eller oönskat ändrad funktionalitet introduceras i kärnkraftverket.

Baserat på feedback från intervjuer samt egna och internationella erfarenheter tror vi att det inte är möjligt att ge ett generiskt "recept" när det gäller komponenter som innehåller mjukvara eftersom det beror på flera faktorer inklusive både komponent- och leverantörskvaliteter samt kärnkraftsägarens tidigare erfarenhet och förmågor. Istället föreslås en generisk process för att ge ett förenklat stöd för kvalificering i olika projektfaser. Den kan användas för att förbättra eller utveckla kärnkraftverkets egna processer för hantering av komponenter som innehåller mjukvara.

List of content

1 Introduction

1.1 BACKGROUND

The turn from analogue to digital equipment has been ongoing in Nuclear Power Plants (NPPs) for several years. Digital equipment often has functional advantages compared with analogue counterparts but at the same time carries the risk of introducing defects or unintentionally changed functionality into the plant. Furthermore, equipment with software often requires regular maintenance in terms of minor upgrades or new software versions. The nature of software-based components also brings risks of functional impact that raises questions above the component level with possible system or plant level functional impact and must thus be handled as such. This requires a process that also take this into account and are not covered by the traditional hardware-oriented component level qualification and change approaches currently applied. Driven mainly by availability, and to some extent by cost, it is necessary for NPPs to use commercially available components provided by suppliers who are not adapted to nuclear specific standards and not used to the nuclear specific requirements. The use of commercial components poses challenges in the design and qualification process to get the correct and sufficient information to facilitate and maintain qualification of the component in the NPP application to be able to assure that the intended system function will be correctly implemented with the new component in place. During the latest years much research has been done on developing methods for safety demonstration of large instrumentation and control system exchange projects as well as on justification of commercially available components.

This project was initiated to evaluate possibilities for standardized methods and approaches for cost-effective management of upgrades and exchanges of components containing software and provided by suppliers. Methods should ensure that no new defects or unwanted changed functions are introduced into the NPP.

1.2 SCOPE AND METHOD

The scope of this study was to identify examples of exchanges of components containing software and evaluate related applied methods for quality assurance and qualification. Purchasing aspects to evaluate in order to manage future updates should be evaluated and it should be evaluated how graded approach could be applied. Significant risks and risk mitigation measures should be identified.

For the purpose for this report “components containing software” is used as a collective term where the component could be a COTS or nuclear specific and the software might be a pre-developed software (PDS), e.g. FW, libraries or software tools, or customized application software.

Information was gathered based on interviews with NPPs and Suppliers who recently have been engaged in related exchange or upgrade projects with NPPs.

An analysis was performed based on previous research results combined with information from interviews. A generalized method for step wise qualification of upgrades of exchanges of components containing software is suggested based on the analysis. The method is applicable to both safety, safety related and non-safety components and should be applied with a graded approach.

1.3 LIST OF ABBREVIATIONS

Term	Explanation
CatA/B/C	safety category A/B/C (IEC)
CCF	Common Cause Failure
CM	Configuration Management
COTS	Commercial-Off-The-Shelf
EYT	non-nuclear safety (Finnish safety classification)
FW	Firmware
IAEA	International Atomic Energy Agency
I&C	Instrumentation & Control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
LTS	Long Term Support
NPP	Nuclear Power Plant
PDS	Pre Developed Software
QA	Quality Assurance
QC	Quality Control
SC	Safety Class
SIL	Safety Integrity Level
SSM	Strålsäkerhetsmyndigheten (Sweden)
SSG	Specific Safety Guide
STUK	Radiation and Nuclear Safety Authority (Finland)
SW	Software
TVO	Teollisuuden Voima Oyj
WENRA	Western European Nuclear Regulators Association

2 Analysis

2.1 SUMMARY OF EXISTING GUIDANCE AND PREVIOUS RESERACH

This section summarizes aspects and gives a high-level introduction to prerequisites and previous research on topics relating to qualification of systems and components containing software.

One of the basic challenges with exchange and upgrade of components containing software is connected to safety classification as e.g. described in Safety Classification for I&C Systems in Nuclear Power Plants [1]. The current status of safety classification for I&C Systems in NPPs poses difficulties as there are different standards (IAEA, IEC, etc.), inconsistency between international and local regulations, ambiguous requirements, incomplete rules and criteria for other I&C functions and backup systems. The approach for safety classification of I&C systems has evolved in recent years following the release of the standards IEC 61226 and IAEA SSG-30. Whereas previously, safety classification of an item reflected its importance to safety, nowadays it is derived from the categorization of the safety significance of the process or function carried out by that item. In the Nordic nuclear industry context categorization according to IEC (CatA, CatB, CatC and non-categorized) comparable with Finnish SC2, SC3, EYT/STUK and EYT, and IEEE (1E (safety-related) and 2E) are most frequently used, see Table 2 in [1].

To introduce increased consistency and mutual acceptance in current practices the Western European Nuclear Regulators Association (WENRA) has published updated versions of Common positions [2]. The intension being to coordinate regulators and safety experts, to be a supporting reference in safety demonstration of safety of software-based systems and to provide guidance for manufacturers and major I&C suppliers. These publications constitute bases for the QA strategy for qualification of digital COTS components presented in this report.

In previous work ENSRIC presented a guide for how to plan and perform safety demonstration for instrumentation and control systems in nuclear power plants [3]. The method was developed with focus on large modernization and new build projects but with the intent also to be applicable with a graded approach also for small exchange projects.

The IAEA member states have published guidance in how to justify the use of digital COTS components in NPP safety systems intended as a basis for IAEA member states to develop or improve their specific processes [4].

ENSRIC has performed work to review the use of COTS digital devices in Safety critical industries [5]. Furthermore, the use of software certification of COTS equipment has been reviewed [6]. One main conclusion from these reports was that the justification approach for COTS use in NPP safety systems is challenging much due to the comparatively small business case, suggesting that increasing harmonization of approaches between countries and licensees would increase business case and overcome market constraints.

In a working group meeting on COTS software qualification [7] ENSRIC collected experiences from the Nordic NPPs on qualification of equipment containing software. Some notes from the meeting are included in the NPP experiences chapter below.

2.2 NPP EXPERIENCES

Interviews were planned and performed with the different NPP owners in the ENSRIC group, including Forsmark, Ringhals, Oskarshamn, Fortum and TVO. In preparation of the interviews a Questionnaire was sent out and interviewees were asked to send answers in advance of the interview.

Interviews were performed in 2 hours video meetings with selected representatives from the NPP and two persons from Solvina. Answers in the Questionnaire were discussed and further developed where needed.

Thirteen examples were identified including component exchanges (analog to digital), model upgrades, SW or FW upgrades and complete control system (platform) exchanges. Most examples are technology developed for conventional, i.e. non-nuclear industry. Four different suppliers were identified including ABB, Siemens, Areva/Framatome, Mirion. NPP application areas are main process control system, turbine control system, relay protection and safety system monitoring equipment. .

2.2.1 Typical QA approaches and qualification records

Some typical records and approaches were mentioned during interviews and in the meeting on COTS software qualification [7] as summarized and listed below:

- Operating experience from other industrial applications.
- Time delayed installation.
- Third party certification, e.g. SIL classification or type approvals
- Locked firmware versions and requalification when upgrading firmware.
- Supplier certification e.g. to ISO 9000
- Benchmarking with other NPP for qualification of the same product.
- Using long time support (LTS) versions.
- Pay Suppliers to perform pre-qualification as basis for contracting.
- Require the Supplier to perform CCF analysis.

Typically, the following standards are used by the Nordic NPP in qualification of software; nuclear standards including IEC 60880, IEC 62138, IEEE 7.4.3.2 and industrial standards including IEC61508, ISO 9001.

2.2.2 Experiences and lessons learned

One strategy is to work with locked firmware version, demanding requalification when upgrading to a new firmware version. Also, NPP strive to use long time support (LTS) versions of software.

For component exchange qualification is normally performed by QC department while qualification of system or platform exchanges is more complex and therefore handled by engineering experts in the project.

It is easier to perform qualification when the same product and/or supplier is involved a second time (e.g. model upgrade).

The NPP change processes and simplified processes for maintenance exchanges do not provide enough support for qualification at component exchanges where components contain software.

NPP processes for maintenance does not always prevent unplanned upgrades of software, it has happened that new software has been installed "as a service" when other maintenance was done, without any prior evaluation or impact analysis.

It is often challenging to get sufficient information and documentation from suppliers. Suppliers are not used to provide the expected qualification records. Often information about performed changes in new versions is very difficult to obtain with sufficient detail.

2.3 SUPPLIERS EXPERIENCES

Contact information was received from NPPs, where possible. In many cases contact was taken only via suppliers or NPP purchase department and no direct contact to engineering or quality department. A video meeting was arranged and questions were sent in advance of the meeting. Below are summarized results of these discussion. The interview questions are listed in Appendix B.

2.3.1 ABB

Anders Bäck and Anders Kettis from ABB division Energy Industries, business area Process Automation.

ABB has done an extensive work to develop their development process according to SIL certification (IEC 61508). The SIL standard and requirements assures a rigorous development process with strict change control. Impact analysis is performed for sub-supplier version upgrades traced by article number.

Long time support software versions are based on Windows LTS version and are not used for safety control systems.

SIL together with operating experience could be an acceptable justification approach at least for lower NPP safety classes but maybe not for 1E/SC2/CatA.

It is important that the NPPs can define complete requirements not only for the detailed technical part but also for qualification. The requirements need to be clear and complete in the contractual basis and they need to be clear and relevant to be accepted by sub-suppliers and ABB also internally.

It will be difficult for NPPs to include component qualification in temporary projects. Instead, it is suggested to initiate continuing collaborations with suppliers to be able to assure i.e. control change and configuration control at all levels to

assure successful system and plant implementation and to facilitate future maintenance. In this way it should be possible to identify a list of active and controlled commodity products.

There are many different levels of complexity in software from non parametrizable to complex programmable systems. It might be possible to define different levels with some kind of graded approach.

2.4 RESULT - QUALIFICATION OF COMPONENTS CONTAINING SOFTWARE IN THE NORDIC NPP CONTEXT

For components containing software the method for qualification needs to be adapted depending on several aspects and related risks. Equipment software can appear in a wide range complexity from simple electronic contactor to a programmable application software. The application area in the plant can vary. The software can be developed through a well controlled development process with configuration control with changes documented in detail, or there might be no documented development process or change log available. The supplier might be able to provide information from years of operating experience or there may be no operating experience available. The nature of software-based components also brings risks of functional impact that raises questions above the component level with possible system or plant level functional impact and must thus be handled as such. A standardized method or approach for qualificaiton need to take all these aspects into account and it need to be integrated with the purchasing and development process for effective and cost-efficient management.

One key conclusion from interviews with NPPs as well as with Suppliers is that one success factor is to establish good contact and collaborations with the Suppliers in an early stage. To be successful and efficient in handling upgrades and exchanges it is also recommended for the NPP to have a controlled configuration management process in place to facilitate impact analysis and traceability from first implementation and through future upgrades.

3 Generic process for Qualification when upgrading Digital I&C Devices

In this project we related the qualification activities to a generic process for upgrading digital I&C devices, see Figure 1. The idea with the process is to provide simple guidance for qualification in the context of a general project process and to visualize the need for a different approach when it comes to qualification of components containing software, see Table 1. A general process implemented and applied in the Nordic NPPs might facilitate harmonization and thereby potentially improve business case and overcome market constraints regionally.

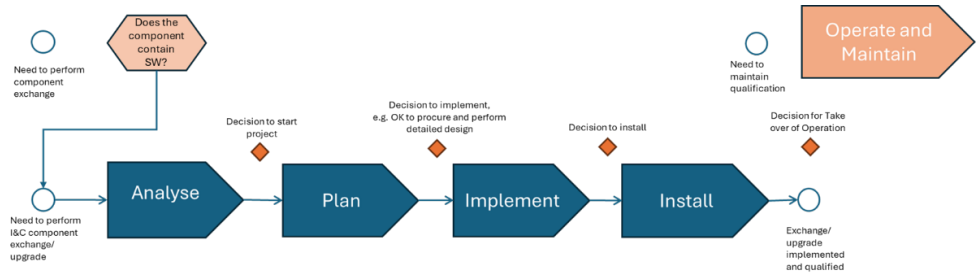


Figure 1 Generic project process where aspects of qualification need to be addressed in all phases. When performing a component exchange the question if the component contain SW should always lead to the general process and the guidance for qualification.

The process starts with the question "Does the intended component contain software? If the answer is "yes" the guidance given in the process should be applied in every occasion. In this context software should be interpreted as any software-based part as for example firmware, base software (including module libraries) or application software. The suggested generic process is based on the normal project or plant change processes used at the NPPs as well as the safety demonstration approach described in Safety Demonstration Plan Guide [3]. It was customized to serve the purpose of smaller component exchange or software upgrades. Effort is put in highlighting the Supplier part and contribution to the qualification. The same process is applicable for all safety categories and graded approach can be applied by relaxed requirements or level of detail on traceable documentation of qualification records for lower safety categories. The objective of qualification is defined for respective phase in the process and qualification output are exemplified. The evaluation result (suitability assessment) from the phase might/should be basis for decision to proceed to the next phase.

In the **Analysis** phase the Supplier and the component suitability should be identified among different alternatives with basis in component and Supplier capabilities. Considerations made during the analysis phase will facilitate a successful and effective qualification process throughout the component life cycle. As highlighted in IAEA Technical Document [8] the suitability evaluation method should be based on previous experience of the Supplier and the specific component.

In the **Plan** phase the qualification effort is focused on qualification of the component itself, compiling available information and records from the Supplier and plan for possible production of records that the Supplier cannot provide. Qualification in the **Implementation** phase should compile the qualification of the component with the planned application in the plant and in the **Installation** phase the qualification should cover the component as installed in the plant. During the lifetime of the component the qualification of the component need to be **maintained** via active configuration management, in planned activities (e.g. software upgrades) and documented.

Table 1, Generic Process for Qualification when upgrading Digital I&C Devices see also Appendix A for a larger version incl. supporting text.

	Analyse	Plan	Implement	Install	Operate & Maintain
Phase purpose	To perform analysis and pre-study for the project	To perform project planning, basic design and to contract supplier.	To perform detailed design, procure, manufacture and receive product and to prepare for installation.	To install and perform final testing, commissioning and final documentation	To perform operation and maintenance through the system lifetime.
Qualification purpose	To sort out which product and supplier will best meet the identified needs incl. product and Supplier capabilities.	To compile documentation and prepare the qualification basis for the product.	To compile documentation and prepare the qualification basis for the product in its specific application in the NPP.	To compile documentation of the final qualification for the product as installed in its specific application in the NPP.	To preserve/maintain the qualification during the product lifetime
NPP activities	• Identify product and project scope and interfaces. • Identify applicable requirements. • Identify possible solutions and products. • Identify possible suppliers. • Collect different supplier provision of generic qualification records and processes. • Assess vs risks and identify additional qualification activities and records needed. • Suggest and select product and supplier as well as overall approach/project.	• Project planning • Safety classification and graded approach • Identify inputs & requirements. • Basic design • Specify/select product / technical solution. • Specify/plan method for qualification (see[1],[2]) • Contract supplier • Supplier works oversight • Author Preliminary suitability assessment	• Detailed design incl. plant integration design (both technical and organizational readiness). • Supplier works oversight (additional qualification tests, manufacturing, supplier testing/FAT etc) • Shipping permit • Receiving inspection (product with associated qualification records etc) • Gather documentation, author Suitability assessment and request permit to install	• Installation • Inspections • Post installation tests • Receiving organisation readiness confirmation • Archive relevant documentation, handover to operations and end Project	• NPP Configuration and change management. • Archive possible impact analyses from changes concluded not challenging existing qualification
Supplier typical qualification records	E.g. Quality/safety management system (IMS) description; Qualification process, process for continuous CM; Generic Product qualification report/records; CE marking; third party certification; SIL classification/certificates	E.g. Quality/Safety system manual & certificate (also sub suppliers as applicable); operating experience and other data/records; Product records remaining with possible additions needs with plan; commercial dedication	Possible additional tests and manufacturing records	Installation standards/procedures; inspection records	Operating experience from other applications, Product CM (changes/updates impact evaluations and communication)
Risks (seeRIL-1101[3], IEC TR 63192[4], Common position[5], Safety Demonstration Plan Guide[6], IAEA SSG-39[7])	CCF (external/internal events, cyber, CM, design/ manufacture[10]). Unclear scope/interfaces and interdependencies. Unclear or not complete-correct-consistent inputs and requirements. Unknown functionalities. Unclear/unknown versions and changes. NPP and product CM issues. NPP and Supplier capability/availability.	*In addition to the earlier:* NPP and Supplier contract understanding and commitment.	*In addition to the earlier:* Unclear/unknown changes Manufacturing (incl. sub suppliers) issues. NPP integration/interface design issues (installation, power supply, earthing, params etc).	Unintended impact from plant changes. Unwanted effects from updates/changes in product.	Unintended impact from plant changes. Unwanted effects from updates/changes in product. Obsolescence.
Risk mitigation	Evaluate, communicate and mitigate risks. Evaluate 3C interfaces, inputs, interdependencies & requirements.	NPP and Supplier/vendor CM (incl. SW & cyber). Contract also Supplier/vendor LTS for product (category/family).	NPP and Supplier/vendor CM (incl. SW & cyber).	NPP and Supplier/vendor CM (incl. SW & cyber).	NPP and Supplier/vendor CM (incl. SW & cyber).
NPP qualification output	Supplier and Product evaluation and project proposal.	Preliminary suitability assessment.	Suitability assessment (as intended to be installed)	Suitability assessment (as installed)	

[1] Suitability Evaluation of Commercial Grade Products for Use in Nuclear Power Plant Safety Systems, IAEA-TECDOC-2034
[2] Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital I&C Equipment for Use in Nuclear Power Plant Applications, IAEA Technical report No. NR-T-3.31
[3] Research Information Letter 1101: Technical basis to review hazard analysis of digital safety systems, USNRC, 2013
[4] Nuclear power plants - Instrumentation and control systems important to safety - Hazard analysis: A review of current approach, IEC Technical Report 63192
[5] Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations, WENRA
[6] Safety Demonstration Plan Guide, Report 2018:512, Energiforsk, 2018
[7] Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA SSG-39

4 Conclusion and recommendation

4.1 CONCLUSION

One of the objectives of this study was to identify and evaluate if there exist common standardized routines regarding Quality Assurance, Configuration Management and V&V for development of PDS or associated hardware at Suppliers, which can be applied for qualification. Based on feedback from interviews, own and international experience we believe that it is not possible to provide a generic "recipe" for this when it comes to components containing software as it depends on several factors including both component and Supplier qualities as well as NPP previous experience and capabilities. Instead, a generic process is proposed to provide a simplified support for qualification in different project phases. It can be used to enhance or develop the NPP own processes for handling components that contains software.

Component exchanges are often handled by maintenance department and qualification is performed by QC department, as opposed to larger projects e.g. exchanges of complete systems, where the project is driven by engineering department with other competences and often qualification is included as an integrated part of the project.

There is no such a thing as "1 to 1" or "component level only" exchange with components that include software. These components inevitably bring the dimensions of potential impact to system or plant aspects and must therefore be handled as such.

- For components containing software the qualification needs to go beyond the component specific qualities and also (or primarily) include the surrounding system functionality, interdependencies and limitations.
- Every new exchange or upgrade needs to be evaluated based on the specific context and complexity of the component and the application in the NPP. Therefore, it is not possible to recommend a general safe and cost-effective QA and V&V strategy based on the suppliers standardized procedures only.

Effective and efficient configuration management (CM) can address many of these issues. If the supplier control and report any upgrades or changes the NPP experts can perform impact analysis as part of the NPP CM and there decide on what activities need to precede a decision to update. With a categorization of different types of components containing software combined with the safety classification a graded approach-based handling should be in reach, allowing for making updates without complete requalification as the impact analysis in many cases can evaluate sufficiently – and provide a traceable record. Such NPP CM also integrates and handles the interfaces between component level and plant/system level impact of change very well.

In the NPP interviews performed, many examples were still related to platforms and larger I&C modernization projects even though the focus should be on components, so there may be further lessons to learn from more component level examples. Also, the limited number of relevant suppliers that could be reached

leave some room for possible further learning. It is however believed that the current general conclusion would remain valid – the simplest and most efficient way to handle these software containing components cannot rely on suppliers only, the NPP organisation must stay in full control and ensure adequate processes and capabilities.

4.2 RECOMMENDATIONS

It was mentioned several times by the NPP participants that a forum for collaboration and experience exchange among the Nordic NPPs around components containing software could be useful. It is recommended to establish such a forum or to discuss the topics from this report in an already existing forum, and the ENSRIC group could be a good starting point to initiate this. There could also be benefits from experience exchange e.g. with Energiforsk GINO that we have seen handles similar issues for the electric grid related components.

It is fundamentally important to establish practical and adequate configuration and change management at the NPP. Configuration management should cover plant, systems and components as a whole and as integrated with their associated documentation to an adequate level of detail based on graded approach principles. CM should be a basis for decisions on whether and when to update component embedded software or not, based on impact analysis of proposed change. This also need to be communicated to all involved parties and departments and endorsed by management.

Add the control question "does the component contain any PDS or software-based part" in the common change AND maintenance processes. Incorporate a work process for qualification when upgrading digital I&C device in internal change process and apply it with graded approach for all applicable upgrades and exchanges. It is recommended to use the proposed general process of this report to develop the NPP qualification and component exchange processes and procedures to better capture and cover the cases when software is involved – this will very often be the case going forward, since most plant components nowadays are difficult to get without any software-based parts included.

Establish good contact and collaborations with suppliers. Consider to establish or contract project independent collaboration with supplier to provide identified components or component families with increased quality assurance and change control. Identify the qualification method early in a project including documentation and information needed from the Supplier. Avoid Suppliers who can not support the chosen qualification method or have difficulties in providing good control and communication of changes and versions. Keep in mind that it is always the NPP organization that need to assess and decide on change at the NPP based on supplier input.

Future further work proposals:

- Categorize and group typical types of SW and further specify needed qualification activities based on complexity of SW with graded approach. The grouping in TBE 106 [9] might be a good starting point.

- Further develop the scope and format of the suitability assessment per phase and decision point. Should be performed with suppliers involved and preferably engaging all Nordic NPPs in workshops to reach common agreement.

References

[1] Safety Classification for I&C Systems in Nuclear Power Plants - Current Status and Difficulties, World Nuclear Association (WNA), 2020.

[2] WENRA, Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations, 2022.

[3] P. Ryd och M.-L. Axenborg, Safety Demonstration Plan Guide, Report 2018:512, Energiforsk, 2018.

[4] IAEA, Nuclear Energy Series No. NR-T-3.31, Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital Instrumentation and Control Equipment for Use in Nuclear Power Plant Applications, 2020.

[5] E. Butler, G. Fletcher, S. George och S. Guerra, COTS Digital Devices in Safety Critical Industries Use and Licensing, Report 2019:627, Energiforsk, 2019.

[6] S. Guerra, L. Hinde och B. Phillips, Software Certification in Nuclear I&C Components, Report 2022:878, Energiforsk, 2022.

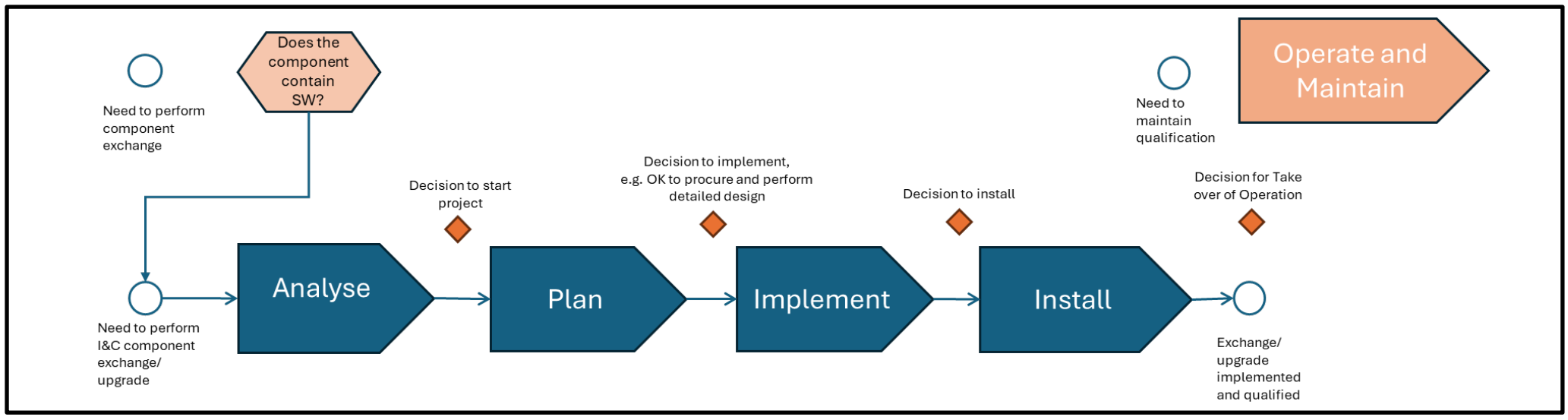
[7] Working group meeting on COTS software qualification, ENSRIC, 26.5.2021.

[8] IAEA, Suitability Evaluation of Commercial Grade Products for Use in Nuclear Power Plant Safety Systems, TECDOC-2034, 2023.

[9] OKG, Vattenfall och SKB, Technical Requirements for Electrical Equipment, TBE 106, 2024.

[10] USNRC, Research Information Letter 1101, Technical basis to review hazard analysis of digital safety systems, 2013.

Appendix A. Supplier Generic Process for Qualification when upgrading Digital I&C Devices



	Analyse	Plan	Implement	Install	Operate & Maintain
Phase purpose	To perform analysis and pre-study for the project	To perform project planning, basic design and to contract supplier.	To perform detailed design, procure, manufacture and receive product and to prepare for installation.	To install and perform final testing, commissioning and final documentation	To perform operation and maintenance through the system lifetime.
Qualification purpose	To sort out which product and supplier will best meet the identified needs incl. product and Supplier capabilities.	To compile documentation and prepare the qualification basis for the product.	To compile documentation and prepare the qualification basis for the product in its specific application in the NPP.	To compile documentation of the final qualification for the product as installed in its specific application in the NPP.	To preserve/maintain the qualification during the product lifetime
NPP activities	• Identify product and project scope and interfaces. • Identify applicable requirements. • Identify possible solutions and products. • Identify possible suppliers. • Collect different supplier provision of generic qualification records and processes. • Assess vs risks and identify additional qualification activities and records needed. • Suggest and select product and supplier as well as overall approach/project.	• Project planning • Safety classification and graded approach • Identify inputs & requirements. • Basic design • Specify/select product / technical solution. • Specify/plan method for qualification (see[8],[9]) • Contract supplier • Supplier works oversight • Author Preliminary suitability assessment	• Detailed design incl. plant integration design (both technical and organizational readiness). • Supplier works oversight (additional qualification tests, manufacturing, supplier testing/FAT etc) • Shipping permit • Receiving inspection (product with associated qualification records etc) • Gather documentation, author Suitability assessment and request permit to install	• Installation • Inspections • Post installation tests • Receiving organisation readiness confirmation • Archive relevant documentation, handover to operations and end Project	• NPP Configuration and change management. • Archive possible impact analyses from changes concluded not challenging existing qualification
Supplier typical qualification records	E.g. Quality/safety management system (IMS) description; Qualification process, process for continuous CM; Generic Product qualification report/records; CE marking; third party certification; SIL classification/certificates	E.g. Quality/Safety system manual & certificate (also sub suppliers as applicable); operating experience and other data/records; Product records remaining with possible additions needs with plan; commercial dedication	Possible additional tests and manufacturing records	Installation standards/procedures; inspection records	Operating experience from other applications, Product CM (changes/updates impact evaluations and communication)
Risks (seeRIL-1101[10], IEC TR 63192[11], Common position[12], Safety Demonstration Plan Guide[13], IAEA SSG-39[14])	CCF (external/internal events, cyber, CM, design/ manufacture[10]). Unclear scope/interfaces and interdependencies. Unclear or not complete-correct-consistent inputs and requirements. Unknown functionalities. Unclear/unknown versions and changes. NPP and product CM issues. NPP and Supplier capability/availability.	*In addition to the earlier:* NPP and Supplier contract understanding and commitment.	*In addition to the earlier:* Unclear/unknown changes Manufacturing (incl. sub suppliers) issues. NPP integration/interface design issues (installation, power supply, earthing, params etc).	Unintended impact from plant changes. Unwanted effects from updates/changes in product.	Unintended impact from plant changes. Unwanted effects from updates/changes in product. Obsolescence.
Risk mitigation	Evaluate, communicate and mitigate risks. Evaluate 3C interfaces, inputs, interdependencies & requirements.	NPP and Supplier/vendor CM (incl. SW & cyber). Contract also Supplier/vendor LTS for product (category/family).	NPP and Supplier/vendor CM (incl. SW & cyber).	NPP and Supplier/vendor CM (incl. SW & cyber).	NPP and Supplier/vendor CM (incl. SW & cyber).
NPP qualification output	Supplier and Product evaluation and project proposal.	Preliminary suitability assessment.	Suitability assessment (as intended to be installed)	Suitability assessment (as installed)	

[8] Suitability Evaluation of Commercial Grade Products for Use in Nuclear Power Plant Safety Systems, IAEA-TECDOC-2034
[9] Challenges and Approaches for Selecting, Assessing and Qualifying Commercial Industrial Digital I&C Equipment for Use in Nuclear Power Plant Applications, IAEA Technical report No. NR-T-3.31
[10] Research Information Letter 1101: Technical basis to review hazard analysis of digital safety systems, USNRC, 2013
[11] Nuclear power plants - Instrumentation and control systems important to safety - Hazard analysis: A review of current approach, IEC Technical Report 63192
[12] Licensing of safety critical software for nuclear reactors. Common position of international nuclear regulators and authorised technical support organisations, WENRA
[13] Safety Demonstration Plan Guide, Report 2018:512, Energiforsk, 2018
[14] Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA SSG-39

General

The overall generic change process figure starts with the question "Does the intended component contain software?" and if the answer is yes, the process and guidance given here should be applied. If the answer is no, then proceed with the normal component qualification/equipment level approach. "Contain software" should be interpreted as if the component/product at all contain any programmable/software-based parts – this can be firmware, base software (incl module libraries), application software etc. and there is a spectrum of variety, that one can group or categorize, e.g. non-changeable parameters/frozen configuration; adjustable parameters (simple), adjustable parameters (advanced), fully or partly configurable with adjustable parameters. Such grouping or categorization can be useful when deciding on how much scrutiny one must apply (graded approach) in the qualification and configuration management of the component with its software and, in the decision on how, if and where to apply the component. The important thing is that you are aware of any changes that you need to make impact analysis for your application based on. This can be rather straightforward and easy or more complex depending on the category of software containing component and on its application. The way software is used in the product also steer how much control the Supplier must have on its (incl. sub-suppliers) changes – the capability and communication of configuration control, for the NPP to at all be able to use the product.

Analyse

The Analyse phase should identify possible solutions (components) and Suppliers. The Supplier's portfolio, accessibility and capability should be investigated also taking into account aspects of maintenance and conditions for future upgrades. NPP own capabilities and maturity on configuration management, including software-based systems and components should be considered since it is an important pre-requisite.

The Supplier's provision of quality assurance including qualification of development processes as well as product qualification should be evaluated in as much detail as possible. Prior experience of the Supplier and product might be valuable and should be taken into consideration as part of the analysis.

Risks related to the Supplier and the product qualification should be evaluated and risk mitigation actions planned. Risks areas as a minimum to address are listed in the process overview table. RIL-1101 [10] appendix E1 gives a useful checklist of items/aspects to consider in this. The internationally reported experience on major hazards/risks is dominated by consequences from unclearly defined scope/interfaces/boundaries and thereby missed or misunderstood interdependencies, missing or unclear requirements and configuration/change management issues so focus on such aspects should be emphasized, both at NPP and Suppliers.

To finalize the evaluation the NPP should identify the possible gap between Supplier quality control and qualification records and what is needed to plan for to add (own work or include in contract) both regarding qualification but also long-time support (LTS).

NPP context, Supplier and product evaluation, should cover e.g.:

NPP:

- Documented and proven version handling (configuration management) of plant, systems and components specific for software containing components (incl. hardware, firmware, base and application software).
- Plant and system functional and physical interfaces, classification and dependability (CCF, failure handling, separation)

Supplier:

- Documented version handling (configuration management) of component including Software (incl. hardware, firmware, base and application software).
- Quality management system incl. Sub-supplier

Product:

- Product qualification documentation (e.g. Generic qualification report, CE marking, third party certification, SIL classification, manufacturing QC records or principles, operational experience).
- Reference deliveries
- How does the Supplier handle and communicate changes (e.g. algorithms, cycle times, filtering, parametrisation etc. could have unwanted impact that you as NPP need to control in your application)

Plan

The Plan phase plans the whole exchange, compiles documentation including qualification basis for the product and contracts the Supplier.

This includes specifying relevant inputs (plant interfaces/context – electrical, e.g. power supply, grounding - process/mechanical, e.g. pressures, quality class, dimensions - I&C, e.g. safety classification, defence-in-depth level, functionality, signalling, communication, interfacing digital devices, cyber security) with associated requirements and standards expectations. Identify any possible impact to basic plant design (architecture, functional, system). Specify the plan qualification method. Contract Supplier for cooperation in activities during the Plan phase as applicable.

Preliminary Suitability Assessment, should cover e.g.:

- Identified and confirmed inputs/context and requirements.
- General product qualification documentation (e.g. product specification, records of conformance to requirements, operational experience). Plan for possible complementing qualification activities.

- Lifetime support and plan for maintenance and upgrades (incl configuration management implementation).
- Preliminary evaluation of suitability for intended use and placement. (Evaluate and argue why and how the component should be fit for purpose and fulfils requirements in the intended NPP location/environment and functions along lifetime)

Implement

The implementation phase details and brings the "hands-on" readiness to install the component, including detailed installation design, finalization of any remaining qualification, the actual physical component at site and organizational readiness to install and then operate it in the NPP over its lifetime. Operation include aspects of maintenance and engineering.

Suitability assessment (as intended to be installed), should cover e.g.:

- Manufacturing and test records.
- Suitability evaluation of component in context of detailed design of plant installation and integration. (Evaluate/argue why and how the component will be fit for purpose and fulfils requirements in the intended NPP location and functions along lifetime)

Install

The Installation phase performs the installation of the component in its physical location in the NPP with the final inspections, commissioning tests etc. Additionally, the component is included functionally and "organizationally", i.e. in the documentation and configuration management as well as in the organizational handling (operations, maintenance and engineering including long term support).

Suitability assessment (as installed), should cover e.g.:

- Product serial numbers, software and file versions in NPP documentation under adequate configuration management.
- Installation/inspection and commissioning/test records.
- Suitability confirmation as installed. (Conclude and argue why and how the component is and will remain fit for purpose and fulfils requirements in the NPP location and functions along lifetime)

Operate and Maintain

Along the lifetime of the component when implemented in its NPP function and location, configuration and change control must be maintained. Even small changes in the product or in interfacing systems and functions may impact the functionality and performance in the NPP. Changes to look out for are e.g. changes

in sampling rates, cycle times, algorithms and other that could impact functionality or dependability, but also changes that could impact e.g. cyber security aspects.

Appendix B. Supplier interview questions

1. Generic change process with a focus on qualification when upgrading components with integrated software (process shown in draft version).

i. What do you spontaneously think about the layout of the table?

ii. As a supplier, do you have a "standard procedure" for QA, V&V and qualification?

iii. What standards do you follow, normally?

iv. Which qualification products do you usually produce / do you think are important for components with programmable technology (i.e. "Supplier typical items" in the table)

2. Configurations and change management

i. How are updates documented?

ii. What control do you have on version management (configuration and change control)?

iii. What information can the customer receive regarding introduced changes in new FW versions / base software versions / application-specific versions.

3. Strategies in development

i. How do you work with and follow up operating experience?

ii. How do you think about modularization and software libraries?

4. LTS (long term support)

i. What recommendations cannot give to KKV regarding what needs to be considered in order to effectively handle future updates (of f.a. software). How do you think about this yourself?

ii. Does support require that you do all the updates?

5. General reflections

i. What challenges do you see in supplying the nuclear power industry with components?

ii. What challenges do you see particularly linked to components with integrated software?

QUALITY ASSURANCE STRATEGIES WHEN UPGRADING DIGITAL I&C DEVICES

In this project we related the qualification activities to a generic process for upgrading digital I&C devices with the aim to provide a simplified support for qualification in different project phases. The suggested process activities can be used to enhance or develop the NPP own processes for handling components that contains software.