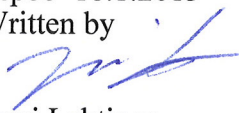
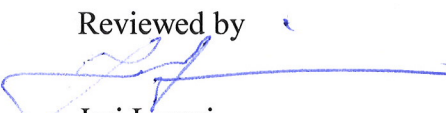
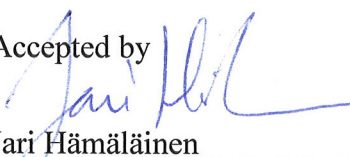




Development of a Review Technique for Conceptual Design Plans

Authors: Jussi Lahtinen

Confidentiality: Public

Report's title Development of a Review Technique for Conceptual Design Plans	
Customer, contact person, address VYR	Order reference 4/2012SAF
Project name Coverage and rationality of the software I&C safety assurance	Project number/Short name 73831 CORSICA
Author(s) Jussi Lahtinen	Pages 29
Keywords software inspection, review, reading technique, perspective-based reading, nuclear	Report identification code VTT-R-08337-12
Summary <p>Inspections and reviews are one of the most effective ways of detecting errors in software development. The methods are also cost-effective because defects can be spotted early in the development, and thus the cost of repairing the defects is lower.</p> <p>Reading techniques are procedures that are used in the inspection or review of a software artefact. The most common procedures are simple ad-hoc reading and a checklist-based reading technique. However, more advanced and detailed procedures have been created for various purposes. One of these advanced reading techniques is perspective-based reading, in which different reviewers examine the document from different perspectives. In this work we have applied perspective-based reading to the review process of design phase documentation, particularly conceptual design plans. We developed five review procedures (scenarios) that can be used for reviewing conceptual design plans. One of the developed reading scenarios was tested to review a real conceptual design document. The review was performed by an automation designer working in the project related to the case study. The reviewer made nine findings using the technique. In the reviewers own experience, the technique was helpful for finding defects and more effective than the technique usually used.</p>	
Confidentiality	Public
Espoo 18.1.2013 Written by  Reviewed by  Accepted by  Jussi Lahtinen Jari Laarni Jari Hämäläinen	
VTT's contact address VTT Technical Research Centre of Finland P.O. Box 1000, FI-02044 VTT, Finland Phone internat. +358 20 722 4520 Fax +358 20 722 4374	
Distribution (customer and VTT) SAFIR2014 Reference group 2	
<i>The use of the name of the VTT Technical Research Centre of Finland (VTT) in advertising or publication in part of this report is only permissible with written authorisation from the VTT Technical Research Centre of Finland.</i>	

Preface

This report has been prepared under the research project Coverage and rationality of the software I&C safety assurance (CORSICA), which is part of the Finnish Research Programme on Nuclear Power Plant Safety 2011–2014 (SAFIR2014). The research project aims to improve the safety evaluation of I&C systems in nuclear industry by improving consciousness of process assessment and rationality of integrated evaluation methods. This report describes the development of a review technique for conceptual design phase documentation. The review technique is based on perspective-based reading, and the report summarizes a case study where the approach was utilized.

We wish to express our gratitude to the representatives of the organizations who provided us with the case example and all those who have given their valuable input in the meetings and discussions during the project.

Espoo, December 2012

Authors

Contents

Preface	2
1 Introduction.....	4
2 Reviews and inspections	4
3 Reading techniques.....	6
4 Perspective-based reading.....	7
4.1 Scenarios.....	8
4.2 Scenario development	8
5 Case study description	9
5.1 Conventional review practices	9
5.1.1 Analysis of previous review practices	11
5.2 PBR scenario development.....	11
5.2.1 Step 1: Identification of review documents.....	11
5.2.2 Step 2: Stakeholder identification.....	12
5.2.3 Step 3: Identification of relevant information	12
5.2.4 Step 4: Creating scenario instructions	15
5.2.5 Step 5: Creating scenario questions	16
6 Testing the reading technique in practice	17
7 Results	18
7.1 Reviewer's experience about the technique.....	18
7.2 Effectiveness of the reading technique	18
7.3 Suggested improvements	19
8 Conclusions.....	19
References	20
Appendix A – Review scenarios	23
Appendix B – Interview questions to the reviewers	28

1 Introduction

In software development it is very useful to locate defects in the early phases of the development life-cycle. The cost of an error found in requirements specification is much less than an error that is found in the testing phase. The nuclear domain typically follows conservative life-cycle models that are quite inflexible, and this effect might be even greater when the development cycle is rigid.

Reviews and inspections are typically used to locate software defects in the early life-cycle phases. In an inspection, a group of people examine a software document such as a requirements specification or a design document, and try to find defects in the document using mainly their expert judgement. Some strategies for better defect detection in software inspection have been developed. The most effective strategies have been advanced reading techniques that are written for guidance or a procedure that the inspector should follow. Defect detection is more of an individual than a group activity, and the strategies that the individual inspectors use to understand and examine the artefact have great influence on the inspection results. Based on empirical research (see e.g. [Lahtinen, 2011] for a survey), the reading techniques that utilize different reviewer roles have been the most effective. Many variants to this approach exist. One variant is Perspective-Based Reading (PBR), in which the reviewer perspectives are derived from the stakeholders of the examined document.

In this work we have applied the generic PBR ideas to the review of nuclear domain conceptual design phase documents. As a result we have developed a review technique that consists of five different review perspectives. Separate review instructions (i.e. a scenario) were written for each perspective. The scenarios can be used in reviewing similar conceptual design plans with little change. One of the developed scenarios was tested to review a real conceptual design document. The review was performed by an automation designer working in the project organization related to the case study. The reviewer made nine findings using the technique. In the reviewer's own experience, the technique was helpful for finding defects and more effective than the technique usually used.

2 Reviews and inspections

Inspection is a well-defined process used for defect detection in software projects. Typically, inspected software artefacts include requirements, design documentation, test plans, and code. Similar techniques used in software projects include walkthroughs and reviews. For clarity, we refer to the definition in the IEEE Standard 1028-2008 [IEEE, 2008], which provides the following descriptions:

- An inspection is ‘a visual examination of a software product to detect and identify software anomalies, including errors and deviations from standards and specifications.’
- A walkthrough is ‘a static analysis technique in which a designer or programmer leads members of the development team and other interested parties through a software product, and the participants ask questions and

make comments about possible anomalies, violation of development standards, and other problems.’

- A review is ‘a process or meeting during which a software product, set of software products, or a software process is presented to project personnel, managers, users, customers, user representatives, auditors or other interested parties for examination, comment or approval.’

While inspections are more rigorous than reviews, the word review is used as a synonym to inspection in this work.

Inspections are very effective methods for defect detection. In addition, the effort required to perform inspections is rather low when compared to other defect detection methods, such as testing. A majority of studies indicate that inspections are very effective in detecting defects, and that the cost of defect correction, when using inspections, is much lower than if the defect was found in a later developmental phase:

- Fagan reported in his work that inspections detected 93% of all defects in a program by IBM. In two other projects, the effectiveness of inspections to detect defects was over 50% [Fagan, 1986].
- The code inspections used at HP typically found 60% to 70% of the defects [Grady and Slack, 1994].
- The ratio of fixing defects during inspection to fixing defects during formal tests varies from 1:10 to 1:34 according to [Kaner, 1998], 1:20 according to [Remus, 1984], and 1:13 according to [Kan, 1995].
- [Weller, 1993] reports that the time needed per defect in inspection is 1.43 hours (6 hours per defect in testing).

The first formally defined inspection technique was the Fagan inspection [Fagan, 1976], which has been used as a model for many subsequent inspection techniques. The Fagan technique is based on a team of reviewers following a step-by-step procedure (Figure 1).

The inspection team members play roles according their skills and knowledge. The team member roles defined by Fagan are: moderator, author, reader, and reviewer. The moderator manages the inspection team and coordinates the inspection process. The author is the programmer who is responsible for the work product under inspection. A reader is a person who paraphrases the work product during the meeting. A reviewer is a person who reviews the work product. A team member may play several roles.

Novel inspections are typically modified versions of the Fagan inspection. A particular software inspection can be characterised using a taxonomy of inspection approaches that has four dimensions: the technical, economic, organisational, and tool dimensions [Laitenberger, 2002a]. The novel inspection variants typically experiment by changing one or several aspects of the standard Fagan inspection.

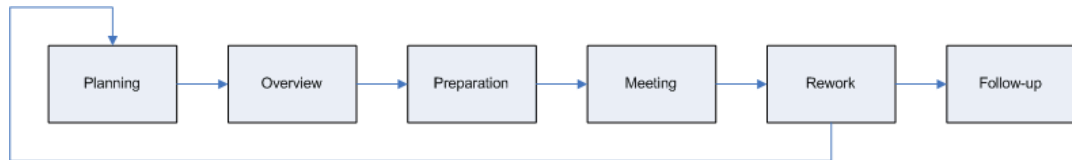


Figure 1. The Fagan inspection process

The influence of modifications on various inspection aspects has been studied. Studies such as [Porter and Johnson, 1997a] indicate that typical meeting-based review methods are neither more effective nor less effective than non-meeting-based review methods with respect to defect detection effectiveness. In fact, the non-meeting inspections found more defects, but there was no significant difference. In addition, the size of the inspection team and the coordination style of the inspection do not, apparently, increase the effectiveness of inspections [Porter and Votta, 1997b].

Instead, explicit training in program understanding improves inspection effectiveness [Rifkin and Deimel, 1994]. It seems that individual preparation for inspections is the most important element contributing to the effectiveness of the inspection [Christenson et al., 1990 and; Laitenberger et al., 2002b]. Defect detection is more an individual than a group activity, and the strategies that the individual inspectors use to understand and examine the artefact have great influence on the inspection results. Thus, advanced reading techniques that guide the individual preparation process can be useful in increasing defect detection effectiveness.

3 Reading techniques

A reading technique is a set of instructions given to the inspector in order to guide the inspection process. A reading technique can also be thought of as a defect detection strategy. The state-of-the-art survey [Lahtinen, 2011] discovered 13 reading techniques that are mentioned in literature:

1. Ad-hoc reading
2. Checklist-based reading
3. Reading by stepwise abstraction
4. Active design reviews
5. Defect-based reading
6. SBR based on function point analysis
7. Perspective-based reading
8. Perspective-Based Usability Inspection
9. Scope-based reading
10. Usage-based reading
11. Traceability-Based Reading
12. Abstraction-driven technique
13. Task-directed software inspection

The most popular reading techniques are ad-hoc reading and checklist-based reading. For a more comprehensive examination of the state-of-the-art of reading techniques, see [Lahtinen, 2011].

4 Perspective-based reading

Perspective-based reading (PBR) [Basili et al., 1996] is a reading technique used in software inspections. The idea of perspective-based reading is to examine a software artefact description from the perspectives of the artefact's stakeholders in order to identify defects.

Perspective-based reading has been applied to various software documents. At least requirements documents [Basili et al., 1996], design models [Laitenberger and Atkinson, 1999], and code documents [Laitenberger and DeBaud, 1997] have been inspected using PBR. PBR techniques are expected to reduce human influence on the inspection results, and increase the cost-effectiveness of the inspections.

Most empirical research papers indicate that PBR is significantly more efficient and cost-effective than traditional reading techniques (ad-hoc and checklist-based reading). For more details, see e.g. [Lahtinen, 2011].

One main idea of the perspective-based reading technique is the same idea as in all scenario-based reading techniques: to inspect a document from different reviewer perspectives. In PBR, the perspectives are derived from the stakeholders of the document, that is, the most relevant people that actually use the inspected artefact during its life cycle. The reasoning behind this is that a document is probably of high quality when potential stakeholders that use the document cannot detect any defects in it [Shull et al., 2000].

Perspective-based reading is typically performed by a team of reviewers (for example three reviewers). The reviewers focus on different aspects of the document. For example, one reviewer examines the document from a tester's perspective, one reviewer from the designer's perspective, and one reviewer from the user's perspective. Because different perspectives view different aspects of the document as important, the review group together can achieve higher overall coverage of the defects in the document. In addition, because each reader is responsible for only a narrow focused view of the document, any potential errors are analysed more rigorously.

The second key characteristic of the PBR method is the active role of reviewers in the inspection. The idea is that the reviewer creates a high-level version of a work product that the user would normally create from their perspective. For example, a reviewer working from a tester's perspective could create a high-level test plan for the system or part of the system. A reviewer working from a designer's perspective could create a high-level design model. A user perspective work product could be a user manual or a set of use-cases.

By creating work products based on the reviewed document, the reviewer is forced to actually think from the given perspective. The intention is that, by producing work products themselves, the reviewers obtain a more profound understanding of the system, and thus are able to detect more defects that are difficult to find and not just superficial errors.

4.1 Scenarios

The ideas of PBR (perspectives and reviewer work products) are manifested via the use of scenarios. A PBR scenario is a document of instructions that the reviewer uses, typically only a few pages long. A separate scenario is written for each perspective. The scenarios consist of specific and repeatable actions that the reviewer has to perform, and a set of questions that the reviewer should answer. As described earlier, the actions are related to producing high-level work products to gain an understanding of the product from a particular perspective. Questions about the activity or the work product are then answered to identify potential defects.

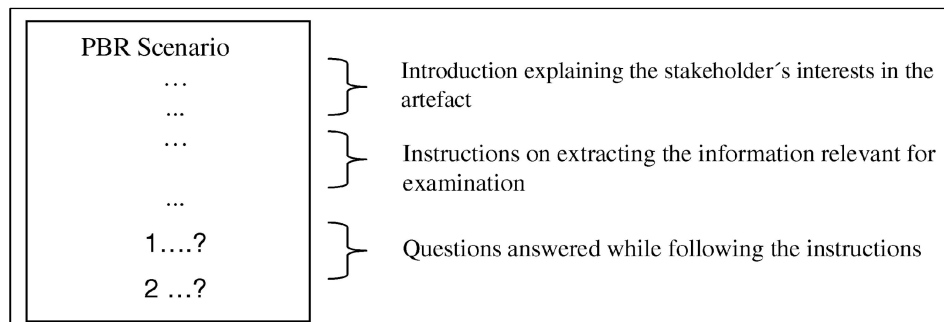


Figure 2. The PBR scenario structure ([Laitenberger et al., 2000])

The basic PBR scenario structure is illustrated in Figure 2. A scenario consists of three parts: an introduction, instructions, and questions.

4.2 Scenario development

The scenarios used in PBR depend largely on the examined document. For this reason the scenarios have to be created on a case by case basis. A process for developing new PBR scenarios is introduced in [Laitenberger and Atkinson, 1999]. The process consists of five steps:

1. Identification of review documents. As the inspected software artefact (e.g. a requirements specification of a particular subsystem) has been determined, the documents containing relevant information about that system need to be identified and gathered. The documents can be textual descriptions, design documents, or graphical models.
2. Stakeholder identification. The stakeholders that have a particular role in the software development process are specified. Possible roles include: the producer of the preceding description of the artefact, the producer of the subsequent description of the artefact, a tester, a maintainer, a user, and a domain expert. The most relevant stakeholders should be selected as the perspectives for the scenarios.
3. Identification of relevant information. The most important information for each perspective is identified. The stakeholders can be interviewed to get answers to questions such as: What does the particular stakeholder need to know about the document to complete their task? How is this information extracted from the document?
4. Creating scenario instructions. Now the scenario can be written. The introductory part of the scenario describes the interests of a stakeholder.

The instructions guide the reviewer to extract relevant information, as identified in the previous step. The instructions should be written in a detailed manner. The instructions should also demand that the inspector documents the work.

5. Creating scenario questions. Questions should be written based on typical problems in the particular environment. The questions should be such that they can be answered with the understanding achieved based on the extracted information. The questions should take into account all relevant defect types.

Once the scenarios have been established, they can be used on all documents of the same type. In practice, as the scenarios have been used in reviews, the scenarios should, if necessary, be modified and improved based on the experience of applying them.

5 Case study description

In order to evaluate the suitability of an advanced reading technique to the review process of nuclear domain system documentation, we performed a case study, in which a high-level design (a conceptual design plan) was examined. The purpose of the developed reading technique was to increase defect detection efficiency, and to take important review aspects into consideration that previously were ignored in the review process. We applied the ideas of the perspective-based reading, and modified the basic approach so that it would fit the case study. The previously used review techniques were reused as much as was possible, so that compatibility between the created technique and the conventional review technique remained as high as possible. Other than this, the PBR technique development process described in Section 4.2 was used. In what follows we first describe the previous review practice, analyse the benefits and limitations of this practice, and after that describe how the PBR development process was followed in the development of new instructions for reviewers. The resulting review instructions (scenarios) are in Appendix A.

5.1 Previous review practices

A checklist-based review procedure exists for various document types. The checklist covers many aspects of a document concentrating heavily on checking the correctness of the document's information and its references. There are also templates for review reports, with guidance on how to fill different fields in the report.

In addition to the checklist-based approach, it is also common practice to compare the document version to a set of other relevant documents. These documents include conceptual-level documentation, system-level documents, requirement specifications, and the minutes of technical meetings. The comparison is not instructed specifically because a generic guide for this purpose is difficult to come up with.

Review areas are also used in the review process. This means that several people typically review a single document so that different reviewers are responsible for

focusing on specific aspects of the document. The review areas depend on the reviewed document. For example, possible review areas are:

- Safety design
- Reliability
- Licensing
- Automation design
- MMI design
- Reactor physics
- Process design
- Electrical design
- HVAC design
- Radiation design
- Plant operation
- Installation and commissioning
- QA

The review areas are not given any explicit review guidelines. It is expected that the experts that perform the reviews are assigned to the review tasks that they are familiar with, and can perform the review from the given perspective.

Each document is assigned to a number of reviewers, but the particular review areas that are used are case-specific. Guidelines exist on how to choose the review areas based on the document's type. In addition to the review areas, each reviewer may be given a specific abstract document quality to consider. These document qualities include:

- Comprehensiveness (A document is comprehensive in relation to a reference document, if it includes all the relevant items of the reference document)
- Correctness (A document is correct in relation to a reference document, if the items it includes are similar to the items in the reference document. A document is correct by itself, if the assumptions in it are true)
- Consistency (A document is consistent, if it has no internal contradictions)
- Completeness (A document is complete, if it includes all the data that are expected in the next work phase)
- Unambiguity (A document is unambiguous, if its intended meaning is obvious)
- Up to date (A document is up to date, if it is based on up-to-date input data and all known changes are taken into account)
- Procedure compliance (the document complies with the consortium procedure, and with the system quality plan)
- Standard identification (the important standards are identified)

As an example, a single design phase document might be reviewed by two reviewers: a safety designer with an emphasis to document correctness, and an automation designer with an emphasis on consistency. Both reviewers follow the check-list based method, and apply the given roles and document qualities in an ad-hoc manner.

5.1.1 Analysis of previous review practices

The previously used review process is quite well described, and the used check-lists are very developed and thorough. The used check-lists take a wide range of aspects into consideration. The review process is also nicely fit together with changes in documentation. Additionally, the use of review areas and the definitions of different qualities that can be reviewed are probably beneficial to the efficiency in the reviews. These review areas roughly correspond to the perspectives of the PBR technique, and they can be used as a template for the reviewer perspective of our technique.

The checklist-based approach is good for finding certain kind of faults, and it is good for maintaining good document quality because simple mistakes are usually filtered. The disadvantage of the check-list based review method is that only defects of a particular type are detected (defects detectable by answering the checklist questions). Hard-to-find defects may often not be found. The checklist-based method can only find errors that have been previously been encountered or thought of as the list was written. Checklists can also be quite generic, and not address some particular case very well.

Many defects are such that they are encountered when a new work phase is begun, when the reviewed document is used for that work phase. These kinds of defects can be very case-dependent, and hard to find using a check-list based technique.

5.2 PBR scenario development

5.2.1 Step 1: Identification of review documents

The case study focused on the review of a conceptual design phase document called 'the conceptual design plan'. The document is used as input when the actual requirements specification and detailed design of the system is made. Typically, a conceptual design plan can include e.g.:

- the design principles related to the system,
- safety classification of the system, its functions and the used equipment,
- the importance to safety of the system,
- the purpose of the system,
- the main functions of the system, and their dependencies on other systems,
- the physical placing of the equipment to the plant, and structural descriptions,
- environmental constraints and requirements caused by other systems,
- connections between systems (signal transfer, interface descriptions),
- quality assurance procedures, and
- references to the preliminary qualification plan, and the preliminary safety analysis report.

Various conceptual design plans exist, and the conceptual design plans can differ from each other quite a lot. We used one particular conceptual design plan as the model for a typical conceptual design plan, and the PBR scenarios were developed based on that document. The exemplar document is written from the

perspective of automation technology. The document is part of safety automation renewal design. It describes the automation design principles related to a temporary control room that is needed while the main control room is being modified. The temporary control room is required to monitor and control the temperature of the refuelling water storage tank, in which the fuel has been transferred to.

5.2.2 Step 2: Stakeholder identification

The system development life-cycle is relevant to the Perspective-Based Reading technique, since the reviewer roles should be based on the relevant stakeholders that actually interact with the document in other (previous or future) development phases. It also relevant to know how the document is used in these future design phases so that this information can be used to guide the reviewer to see if the document is actually usable in this way.

In our case study the design phase of the system development life-cycle is divided into four consecutive sub-phases: feasibility study, preliminary design, basic design and detailed design. The system is implemented based on the detailed design. Verification is performed between two successive design phases, and before commissioning, the system is validated against the stakeholder requirements created in the preliminary design phase.

The feasibility study phase defines the justification for suggested system changes. Based on the feasibility study, a decision is made to begin the actual design of the new system.

In preliminary design, the desired system requirements, and constraints (stakeholder requirements) are composed. The information is used to evaluate alternative designs.

In basic design, the conceptual design of the system is selected and further defined. This includes the architecture of the system. One of the alternative design solutions is selected and design is continued based on the selection. The main output document of this phase is the conceptual design plan, in which the design is represented on a general level. The inputs for the document are the stakeholder requirement created in preliminary design. Other outputs of the basic design phase are a preliminary report on quality management principles and a preliminary safety analysis report.

After this, the detailed design phase begins. As input, detailed design uses the outputs of the basic design, and the stakeholder requirements. In detailed design, the final design is created whenever this is possible. The final requirements specification is also created in this phase based on the previously defined more general requirements. In addition, a V&V plan is written that makes sure that these requirements are present in the final system. Other outputs of the detailed design phase include a quality assurance plan, preliminary suitability analysis, system placing plan, structural design, and a safety analysis report.

In our case study, we need to identify the stakeholders of the conceptual design plan. The conceptual design plan is used to produce the detailed design of the

system. In addition to this, the conceptual design plan is sent to the regulator for inspection. Based on the particular conceptual design plan various different designers are needed for the following design phases. In our case study the most relevant designers are: an automation designer, a control room designer, safety designer, and an electrical designer. All these stakeholder roles are selected as a basis for a PBR scenario. In addition, the licensing/regulator aspects are also selected as one scenario. These roles exist as the review roles that have previously been used to review documents. The regulator role corresponds to the Licensing review area. In what follows we describe the development of the following scenarios:

1. Automation designer
2. Control room designer
3. Safety designer
4. Electrical designer
5. Regulator

Note that we have not included the perspective of a tester unlike in other perspective-based techniques handling design phase documentation. The reason for this is that the conceptual phase plan is not used in system validation. Instead, the validation is performed against other documentation such as the functional requirement specifications.

5.2.3 Step 3: Identification of relevant information

We analyse each perspective in order to describe what kind of information is relevant to them in a conceptual design plan. The relevant information analysis is based on interviewing five reviewers (one reviewer representing each of the perspectives: an automation designer, a control room designer, an electrical designer, a safety designer, and a reviewer focused on licensing). The reviewers were asked a list of questions (see Appendix B), and the relevant information was compiled based on the answers.

Automation designer

An automation designer creates a design for implementing the required functions and systems in practice and designs the required data transmission solutions, and connections between the devices and the control room. The most relevant information for the automation designer in the conceptual design plan consists of:

- Information about the required redundancies. Is there sufficient redundancy based on the safety classifications of the systems and functions? Is the redundancy designed correctly?
- Separation of systems. Are the different separation requirements of the systems met (physical separation, electrical separation). The automation designer makes sure that subsystems that belong to different safety classes are separate, and that the input/output signals of these systems are transferred via separate cables / media.
- Signal transfer to the control room. Based on the control room needs (displays, conventional controls) the relevant signals need to be arranged to the control room and organized to the correct positions. Automation design also makes sure that the necessary information can be transferred within the resources (enough signal values can be transferred to the control

room). The automation designer has to think about practical matters as well: Are the voltage levels sufficient to transfer all information via cables? Is the cable length exceeded, and are signal amplifiers required.

- Compliancy with other automation related documentation. Does the conceptual design plan require changes because automation requirements are not met? Are any automation specific changes that need to be made because of the conceptual design plan? Relevant documents include the control room conception design plan conceptual design plan, automation architecture description, accident management conception design conceptual design plan for accident management, control room documents vs. automation documents.
- Assumptions made. What are the assumptions made in the document that need to be taken into consideration in automation design. What are the assumed accident conditions that the control room shall manage?

Control room designer

The control room designer designs the layout of the control room, and creates the layout of the control panels. In addition to the ergonomic aspects of the control room, the control room designer is also responsible for writing operator guidance documentation, and designing the organization of the control room staff. In a conceptual design plan, the control room designer is mainly interested in information related to:

- Information related to the operational procedures written for the control room operators.
- The order of controls is important (in which order things are done).
- Constraints related to the positioning of controls, screens and panels. This includes ergonomic constraints, physical constraints in the control room, constraints derived from automation design, control room usability issues, cable separation requirements, and easiness of maintenance.
- Completeness of description related to necessary controls. Are all assumed operator tasks described?

Safety designer

The safety designer focuses on plant safety from the process point of view, even though all aspects of safety are covered. Many safety requirements have been set by the regulator, and the safety designer simply compares the system requirements to the regulator requirements, and translates these requirements to the various designers. The regulator has defined accident classes, and the manner in which the plant should prepare for anticipated events. The safety designer performs the safety analyses, and creates the safety classification of the systems. In a conceptual design plan, the safety designer focuses on:

- Completeness of the list of anticipated events/ accidents.
- Correctness and completeness of design requirements with respect to general safety constraints.
- The correctness of the translation of the regulatory requirements in the conceptual design.
- The correctness of regulatory requirements used as reference. Are the used requirements appropriate for the system?

Electrical designer

An electrical designer designs the electricity distribution required for the systems, e.g. control room equipment. The electrical engineer makes a list of equipment that need power and designs how that power is transmitted. In a conceptual design plan, the electrical engineer focuses on:

- Separation of different safety classes. It is important to design so that systems in different safety classes remain separate, and single fault tolerance is maintained. The failure of a single component in the electrical systems should not lead to the failure of a safety system.
- The distribution of reserve power.
- Power and voltage requirements of the various systems. These requirements have an influence on the selected equipment, and electrical interfaces.
- Constraints that may affect the placement of cables and the central electric units.

Regulator

The regulator reviews the design, and compares it against relevant standards and other guides. The set of relevant documents varies. The regulator is mainly interested in:

- Correctness and completeness of referenced standards and other documents.
- Adequacy of quality assurance.
- Comprehensiveness of other licensing documentation.

5.2.4 Step 4: Creating scenario instructions

The scenario instructions were created based on the interviews (see Appendix B). For the roles of automation designer, control room designer and electrical designer the idea in creating scenario instructions was to make the reviewer manually simulate the following detailed design phase, in which the conceptual design plan will be used as input. This way the reviewers find out how the information in the conceptual design plan suffices for the next work phase.

The automation designer uses the conceptual design plan as input to develop more detailed designs of the systems. For example, the physical signal transfer to the control room is designed, and the general requirements for assumed accident conditions in the conceptual design plan are implemented on different user interfaces.

The control room designer uses the conceptual design plan as input to make more detailed control room layouts, designs the operator guidance documentation, and the control room organization.

The electrical designer uses the conceptual design plan as input when the detailed electric distribution scheme is planned. This includes selecting appropriate

hardware, cable routing, placement of equipment, and designing reserve power systems.

Creating similar scenario instructions for the roles of regulator and safety designer is not as straight-forward. These roles are not traditional developer roles, and they use the conceptual design plan mainly to analyse its sufficiency. Safety designer and a regulator do not use the conceptual design plan in order to create some new work product that is directly used in the system development. Their job is just to review the conceptual design plan. The scenario instructions for the reviewers in these roles were created based on what the reviewers said in the interviews. The safety designer mentioned that one of the main tasks of the safety designer is to translate the regulatory requirements so that the designers can understand and implement them in their design. The person reviewing from the licensing / regulator perspective mentioned that the main concerns in that perspective are to make sure that the referenced standards and other documents are appropriate, and that the quality assurance practices are described sufficiently in the conceptual design plan. The instructions for the safety designer and regulator scenario were written so that these tasks are emphasized.

5.2.5 Step 5: Creating scenario questions

The final step in developing the PBR scenarios is writing the questions that the reviewer should think about when performing their reviews. The questions' intention is to emphasize certain viewpoints that should be considered by the reviewer (instead of explicitly asking about some details about the document as check-lists tend to do). The main question for all designer scenarios is whether the future work phases can be performed based on the conceptual design plan. In addition to this, aspects that the reviewers themselves emphasized in the interviews have been included in the questions (what do the reviewers normally ask themselves when reviewing a document).

In addition to input received from the interviews, some of the nuclear specific aspects were emphasized in the scenarios. In our previous work [Lahtinen, 2011] we have identified the following aspects as being specifically important to the nuclear domain:

- **Long system life-time:** A nuclear power plant (NPP) has quite a long operational life-time (~60 years. Renewal of systems within this period is often necessary. An existing system may have to be replaced or entirely new systems built. From the system renewal perspective, it is relevant that the requirements written for a system are easily extensible. Furthermore, it is relevant that the reasoning behind the written requirements is stated explicitly so that the requirements are not later casually changed or neglected.
- **Design process complexity:** The design process of an NPP-related system is a complex process. Many things have to be taken into consideration. Typically, systems are designed by many people together, responsible for different areas of the design. One person hardly has all the necessary knowledge and skills to evaluate all the relevant design aspects of a system at the same time. Instead of a single designer role, a nuclear-domain system has many designers with different expertise.

- **Regulator's role:** One special aspect of the nuclear-domain requirements is that they have to be approved by the regulator. In practice, this means that the requirements specification is reviewed by the regulator body. The objective of the regulator's review is to compare the requirements to the requirements given by law and by the Finnish YVL guides. The regulator wants to make sure that the main safety requirements and design principles are followed and that reactor safety is ensured. Other than that, the regulator probably focuses on the referred standards followed, and the overall quality of the documentation.
- **Importance of safety:** Another nuclear aspect is the great importance of safety. The "safety as high as reasonably achievable" principle is often quoted. The nuclear-domain safety precautions are manifold: the defence-in-depth principle calls for multiple protection measures that back each other up in case one measure fails. In addition, some protection measures are built in as redundant and diverse to achieve failure tolerance.
- **Contract work chains:** Construction of a nuclear power plant is a huge project. Some work is distributed to contractors. For example, the requirements specification might be given as input to a contractor to create some part of the system. The contractor might hire a subcontractor to perform the work. The requirements specification is given to the subcontractor. The potential problem is that the subcontractor might not be aware of all related nuclear-specific guidelines and design principles that are not explicitly mentioned in the requirements specification documentation. Considering this, it might be interesting to find out whether the individual requirements are such that they could have varying interpretations depending on the background of the reader. Could a person with no detailed nuclear-domain knowledge understand the requirements in a different way?

Design process complexity, importance of safety, and the regulators role are already taken into consideration in the selection of the reviewer perspectives. The long-system lifecycle concerns are related to the maintainability of the system. The reviewers should perhaps also try to analyse how system maintainability is addressed in the conceptual design plan. For this reason we also added questions related to system repairs and modifications. To emphasize the importance of maintenance related issues, these questions were also grouped together as a separate section of the scenario questions. Contract work chains are not especially covered in the scenarios because their importance in the conceptual design phase is probably quite small.

Finally, each scenario has a section "Outputs" that lists the documentation that the reviewer should produce during the review. The explicit list of outputs intends to emphasize the importance of documenting one's work properly.

6 Testing the reading technique in practice

The developed reading technique is such that it requires a certain amount of expertise, knowledge about the described system, and access to relevant background information, which is needed to perform the tasks that are part of the review. It is very difficult for persons outside the project organization to produce

the work products required in our technique. For this reason, testing the effectiveness of the technique cannot really be done by independent researchers. Regardless of this difficulty, we wanted to try out the developed technique in its real intended environment. We organized a review, in which an actual conceptual design plan that had been developed in the project was reviewed by an automation designer using the corresponding reading scenario. The automation designer had ca. five years of experience as an automation designer, and had some previous experience with reviewing similar documents from the automation designer's perspective. The reviewed document was the conceptual design plan that was used as an example when the reading technique was developed, except the used revision was more recent (a draft version was used for the development of the reading technique). The time given for the review was two hours.

We used the lab package developed for the empirical investigation of perspective-based reading [Basili et al., 2011] as reference when conducting the review. We first gave the reviewer a short introduction into the perspective-based reading, and ensured that the basic ideas of PBR were understood. After this, the reviewer read the conceptual design plan and performed the tasks required by the reading scenario. Review findings were documented on a separate form. The reviewer wrote down a description of the findings classified each finding (Omission / Ambiguity / Incorrect fact / Extraneous / Positive finding / Miscellaneous). After the review, the reviewer filled out a feedback form about the performance and efficiency of the used technique, and effectiveness of the technique compared to a traditional review. The reviewer was also briefly interviewed for general feedback.

7 Results

The results in this section are based on feedback from the reviewer. We describe what the reviewer's experience was about using the technique, how effective the reviewer thought the technique was, and finally discuss some suggestions made by the reviewer to improve the technique.

7.1 Reviewer's experience about the technique

The reviewers understanding of the used reading scenario was very good by her own account. She found the technique somewhat useful, and found that the reading scenario was helpful for finding defects in the conceptual design plan. The questions in the scenario were generally quite helpful as they gave the reviewer hints about what aspects (e.g. maintenance aspects) of the document to consider.

7.2 Effectiveness of the reading technique

The reviewer estimated that the perspective-based reading technique was more effective in finding defects than the traditionally used review technique. The reviewer made nine findings in the document. The findings were classified into categories as described in section 6. A single finding could belong in several categories at the same time. Four of the findings were marked as omissions (something significant information was missing from the document). Five

findings were marked as ambiguous (the information in the document was unclear, or the document is inconsistent).

7.3 Suggested improvements

The reviewer had some difficulties in following the reading scenario. Namely, some of the given instructions were too detailed, and the task could not be fully performed based on the conceptual design plan. The reading scenario directs the reviewer to draw the physical routes of required signals in the layout picture. This task was too demanding, and could not be done based on the conceptual design plan within the given time. As the given task was not fully feasible, the reviewer instead performed an improvised task, and created a table that listed all the relevant hardware subsystems. For every subsystem the reviewer then checked whether the relevant aspects such as redundancy, separation, placement, environmental conditions, alarms, and electrical distribution were addressed in the conceptual design plan. The reviewer stated that it is more important to check that all these aspects are somehow covered in a conceptual design plan.

The reviewer also said that it is important that the reviews are kept as concise as possible. Defects can be found when the documents are rigorously scrutinized but this takes a lot of resources, especially when there are so many documents. Apparently, the conceptual design plan is suitable for short reviews because it does not go too much into detail, and the review can be performed within a few hours.

8 Conclusions

We have applied the PBR reading technique for reviewing nuclear domain conceptual design plans. The technique is based on perspective-based reading, where the idea is to examine a software artefact from the perspectives of the artefact's stakeholders in order to identify defects. A scenario (review instructions) is written for each perspective. The intention of the scenarios is to make the reviewer to create some work products in order to force the reviewer to analyse whether the examined document is suitable for its intended purpose.

We used the ideas of perspective-based reading and created five scenarios for reviewing conceptual design plans: an automation designer scenario, a control room designer scenario, an electrical designer scenario, a safety designer scenario, and a regulator scenario. The main novelty of the developed technique is that the reviewer can try to simulate the future work phases, and try to anticipate what kind of practical issues may not have been considered in the conceptual design phase. The review technique may be more effective in finding more complex defects that the check-list based review methods does not consider, and that would normally be found during the following detailed design phase.

It seems that the scenarios created for the regulator perspective, and the safety designer perspective are not as compatible with the PBR principles as the other design scenarios. The regulator and safety designer roles are not typical engineering roles in which some input is used to produce some output as part of the development life-cycle. These roles are more like observers that simply

evaluate the work done by others and analyse it. It was very challenging to try to create reading scenarios for these perspectives. These roles by their nature seem to be more suitable with reviews using check-lists.

We performed a brief test review in which the developed method was tried out for its intended purpose in a real case. Only one of the created reading scenarios (automation designer) was used. The developed method was considered to be effective, and the reviewer found several omissions and ambiguities in the reviewed document. The used scenario was not fully feasible, and the reviewer had to alter some of the tasks in the scenario.

The testing of the developed technique was limited to a single test review. The main reason for such conciseness was the limited resources available for performing additional experimental reviews. If the aim of our research would have been to find out whether some quantitative difference exists between the traditional review methods and the developed technique, we should have done an experiment in which two groups of reviewers used the different techniques and the groups' efficiency for finding defects could be compared against each other. This kind of research was impossible because of limited resources. With respect to the objectives of this work, simply trying out the developed technique is an appropriate way to find out whether it is usable and effective. We rely on the opinion of the reviewer to evaluate whether the developed technique is suitable for its intended purpose.

Rigorous review techniques can find more defects. However, it is also necessary that the reviews do not take an excessive amount of resources. Traditionally used check-lists are more concise do not take a long time to perform. In the nuclear domain, the documents are often based on standards, and are quite schematic. Because of the documents' standard structure many document defects can be found by following a simple check-list based on that standard.

The more rigorous perspective-based review methods cannot completely replace the more traditional check-list based methods. However, the perspective-based reviews can be used to complement the existing review techniques where necessary.

References

- [Basili et al., 2011] Basili, V. R., Green, S., Laitenberger, O., Lanubile, F., Shull, F., Sørumgård, S., and Zelkowitz, M. 2011. Lab package for the empirical investigation of perspective-based reading. http://www.cs.umd.edu/projects/SoftEng/ESEG/manual/pbr_package/manual.html (accessed: 15 March, 2012).
- [Basili et al., 1996] Basili, V. R., Green, S., Laitenberger, O., Shull, F., Sørumgård, S. and Zelkowitz, M. V. 1996. The empirical investigation of perspective-based reading. *Empir Softw Eng-Int J.*, Vol. 1, pp. 133–164.

- [Christenson et al., 1990] Christenson, D.A., Huang, S.T. and Lamperez, A.J. 1990. Statistical quality control applied to code inspections. *IEEE Journal of Selected Areas of Communication*, Vol. 8, Issue 2, pp. 196–200.
- [Fagan, 1976] Fagan, M. E. 1976. Design and code inspections to reduce errors in program development. *IBM Sys. J.* Vol. 15, No. 3, pp. 182–211.
- [Fagan, 1986] Fagan, M. E. 1986. Advances in software inspections. *IEEE Transactions on Software Engineering*, Vol. 12, Issue 7, pp. 744–751.
- [Grady and Slack, 1994] Grady, R. B. and van Slack, T. 1994. Key lessons in achieving widespread inspection use. *IEEE Software*, Vol. 11, Issue 4, pp. 46–57.
- [IEEE, 2008] IEEE Standard 2008. IEEE Standard for Software Reviews and Audits, 1028-2008.
- [Kan, 1995] Kan, S. H. 1995. Metrics and models in software quality engineering. Addison-Wesley Publishing Company.
- [Kaner, 1998] Kaner, C. 1998. The performance of the n-fold requirement inspection method. *Requirements Engineering Journal*, Vol. 2, No. 2, pp. 114–116.
- [Lahtinen, 2011] Lahtinen, J. 2011. Application of the Perspective Based Reading technique in the nuclear I&C context, CORSICA work report 2011. VTT Technology 9. Espoo, Finland.
- [Laitenberger and DeBaud, 1997] Laitenberger, O. and DeBaud, J.-M. 1997. Perspective-based reading of code documents at Robert Bosch gmbhGmbH, Tech. Rep. ISERN-97-14.
- [Laitenberger and Atkinson, 1999] Laitenberger, O. and Atkinson, C. 1999. Generalizing perspective-based inspection to handle object-oriented development artifacts. In: *Proceedings of the 1999 International Conference on Software Engineering*, 1999. Los Angeles, CA, USA, pp. 494–503.
- [Laitenberger et al., 2000] Laitenberger, O., El Emam, K. and Harbich, T. 2000. An internally replicated quasi-experimental comparison of checklist and perspective-based reading of code documents. *IEEE Transactions on Software Engineering*.
- [Laitenberger, 2002a] Laitenberger, O. 2002. A survey of software inspection technologies. In: *Handbook on Software Engineering and Knowledge Engineering*. Vol. 2: Emerging Technologies, River Edge: World Scientific, pp. 517–555.

- [Laitenberger et al., 2002b] Laitenberger, O., Beil, T. and Schwinn, T. 2002. An industrial case study to examine a non-traditional inspection implementation for requirements specifications. *Empirical Software Engineering*, Vol. 7, Issue 4, pp. 345–374.
- [Porter and Johnson, 1997a] Porter, A. A., Johnson, P. M. 1997. Assessing software review meetings: Results of a comparative analysis of two experimental studies. *IEEE Transactions on Software Engineering*, Vol. 23, Issue 3, pp. 129–144.
- [Porter and Votta, 1997b] Porter, A. A., Votta, L. G. 1997. What makes inspections work? *IEEE Software*, Vol. 14, Issue 6, pp. 99–102.
- [Remus, 1984] Remus, H. 1984. Integrated software validation in the view of inspections/reviews. In: *Proc. of a symposium on Software validation: inspection-testing-verification-alternatives*. Elsevier North-Holland, Inc. New York, NY, USA ISBN 0-444-87593-X, *Software Validation*, pagespp. 57–6564.
- [Rifkin and Deimel, 1994] Rifkin, S. and Deimel, L. 1994. Applying program comprehension techniques to improve software inspection. In: *Proceedings of the 19th Annual NASA Software Eng. Laboratory Workshop*. NASA.
- [Shull et al., 2000] Shull, F., Rus, I. and Basili, V. 2000. How perspective-based reading can improve requirements inspections. *Computer*, Vol. 33, Issue 7, pp. 73–79.
- [Weller, 1993] Weller, E. F. 1993. Lessons from three years of inspection data. *IEEE Software*, Vol. 10, Issue 5, pp. 38–45.

Appendix A – Review scenarios

Automation Designer scenario for conceptual design plan reviews

Introduction

Assume you are reading the design document from an automation designer's perspective. You are interested in knowing whether the conceptual level design is sufficient so that it has all necessary information to produce a more detailed design for automation. In particular, you are interested in:

- whether the design supports the requirements for system separation, and redundancy
- whether it is possible to transfer the necessary signals to the control room

Concentrate on the comprehensiveness of the document. Document all your work, all your thoughts and drawings, and the conclusions and findings (both positive and negative) you make.

Instructions

Create a rough preliminary design for transferring the necessary signals to the control room. Based on the conceptual design, interpret its general requirements where needed, and based on those requirements, create a plan to provide the necessary signals to the system. Draw a picture of the control room layout, and outline in it the current systems/interfaces, and the new/changed system. In your picture, draw the physical routes for the required signals. Try to think about the practical matters such as the required voltage levels. If possible, select the type of equipment used to provide the required signals to the system.

Task-related questions:

1. Are you able to create an automation design based on available information?
2. Does the physical routing of signals highlight any practical problems that should also be taken into account?
3. Can the separation requirements and redundancy requirements be met?
4. What cable length is required? Are signal amplifiers needed?

Document-related questions:

5. Are there any unclear parts in the reviewed document?
6. Are all aspects covered in the reviewed document? (Comprehensiveness)
7. Does the document answer to the issues it attempts to answer?
8. What kinds of assumptions are made in the design that might influence automation design?

Maintenance questions:

9. What is the purpose of the designed systems? Why are they designed in this way? Are reasons for various design solutions, and the purpose of the system described in the document?
10. Are future modifications / repairs considered? Is there room for more cables? Should there be? What kind of repairs or other maintenance is probable in the future? Any practicalities related to this that should be written in the document?

Outputs

1. Signal transfer design drawing
2. Review notes (Found defects, remarks, positive findings)

Control Room Designer scenario for conceptual design plan reviews

Introduction

Assume you are reading the design document from the point of view of a control room designer. You are interested in finding out whether the conceptual design plan is such that it serves as a good basis for designing the more detailed control room layout. In particular, focus on:

- whether the document describes all required controls
- whether the document describes all the constraints related to the positioning of the controls

Document all your work, all your thoughts and drawings, and the conclusions and findings (both positive and negative) you make.

Instructions

Create a list of constraints that exist related to positioning of the control room controls (separation requirements, space limitations, what panels are available, other constraints,). Based on these constraints, create a rough drawing of the control room, and design how the needed controls are positioned in the room. Sketch the layout of the control panels. Try to think of practical matters that need to be considered. Think in terms of actual hardware as well. If possible, select the equipment used to implement the control room. Make preliminary device selection decisions when needed, and document these decisions. As you design the control room layout, think whether there are issues that should be addressed in the conceptual design plan / have not been previously thought of. Document these issues.

Task-related questions:

1. Can you design the control room based on the information in the conceptual design plan?
2. Do the operators see the necessary screens from their seats? Are there any visual obstructions?
3. Can the cables be brought to the room so that necessary separation requirements are met?
4. Are there other ergonomic requirements for the operators to be considered?

Document-related questions:

5. Are there any unclear parts in the document?
6. Does the document mention all assumed operator tasks?
7. Does the document state all necessary design constraints related to the control room design?

Maintenance questions:

8. What is the purpose of the designed systems? Why are they designed in this way? Are reasons for various design solutions, and the purpose of the system described in the document?
9. Are future modifications / repairs considered? Is there room for more cables? Should there be? What kind of repairs or other maintenance is probable in the future? Any practicalities related to this that should be written in the document?

Outputs

1. Review notes (Found defects, remarks, positive findings)
2. Control room layout design draft

Safety Designer scenario for conceptual design plan reviews

Introduction

Assume you are reading the design document from the point of view of a safety designer. The safety designer focuses on plant safety and reliability from the process point of view, even though all aspects of safety are covered. A lot of the safety requirements have been set by the regulator, and the safety designer translates these requirements to specific requirements more related to the various design tasks. In particular, you are interested in knowing

- whether all relevant regulator / safety requirements are addressed in the conceptual design plan
- whether the safety requirements are feasible in detailed design

Document all your work, all your thoughts and drawings, and the conclusions and findings (both positive and negative) you make.

Instructions

First, write down the operating conditions of the system that are mentioned in the conceptual design plan. In addition, write down the design areas relevant to the detailed design of the system.

Make a list of the main safety requirements of the system, and the source of these requirements. Below each requirement, write down how the requirement is expressed in the system. Think how that requirement affects each of the design areas relevant to the system. Translate the requirement to a design area specific requirement, and write down all the translated requirements. To each translation, add a statement explaining the purpose of this requirement. Do the different operating conditions influence these requirements?

Finally, check whether the conceptual design plan covers every aspect brought up in the previous paragraph. Document your findings.

Task-related questions:

1. Are the requirements in the conceptual design plan written so that the designers can implement them?
2. Have the appropriate regulatory requirements been used as reference?
3. Are the requirements the design is based on correct and sufficient?

Document-related questions:

4. Are there any unclear parts in the document?
5. Are all safety aspects covered in the conceptual design plan? (Comprehensiveness)
6. Is the list of anticipated events / accidents complete?

Maintenance questions:

7. Is the reasoning behind the detailed safety requirements clear? If the system is later modified, are the reasons behind different design solutions documented?

Outputs

1. List of requirements, and the translations of these requirements to requirements used by various designers.
2. Review notes

Electrical designer scenario for conceptual design plan reviews

Introduction

Assume you are reading the design document from the point of view of an electrical designer. You are interested in knowing:

- how electricity can be distributed to the equipment,
- how different safety classes can remain separate,
- how single failure tolerance can be achieved in the electrical systems.

Document all your work, all your thoughts and drawings, and the conclusions and findings (both positive and negative) you make. If problems arise during the tasks below, are these problems caused by missing information in the conceptual design plan?

Instructions

First, write down the equipment that needs power, and the type of electricity needed. Write down the safety classifications of the equipment. Also, figure out relevant constraints: separation requirements, redundancy requirements etc.

Create a preliminary plan for electrical distribution. Select and document the equipment (hardware, cables) used, and sketch the positioning of the central electric units and how the cables are run. Draw a picture. Think of practical matters. Make preliminary device selection decisions when needed, and document these decisions. Try to calculate whether there will be any power requirements for the diesels.

Task-related questions:

1. What kind of interfaces the selected equipment have?
2. What kind of connections are between equipment?
3. Is the required level for voltage / power feasible?

Document-related questions:

4. Are there any unclear parts in the document?
5. Is the conceptual design plan detailed enough so that the necessary electrical equipment can be selected?
6. Are the requirements in the conceptual design plan for separation and redundancy feasible?

Maintenance questions:

7. Are reasons for various design solutions, and the purpose of the system described in the document?
8. Are future modifications / repairs considered? What kind of repairs or other maintenance is probable in the future? Any practicalities related to this that should be written in the document?

Outputs:

1. Plan for electrical distribution
2. Review notes

Regulator scenario for conceptual design plan reviews

Introduction

Assume you are reading the design document from the point of view of a regulator. You are interested in knowing what standards and other guidance are being followed in the development of the system. You are also interested whether proper quality assurance exists.

Document all your work, all your thoughts and drawings, and the conclusions and findings (both positive and negative) you make.

Instructions

Create a list of standards and other relevant documents that are referred to in the conceptual design plan. If internal guides are referred to, check also whether these documents reference standards. Based on the conceptual design plan, create a list of licensing documents that the conceptual design plan mentions.

Questions:

1. What standards are followed?
2. What standards are followed in quality assurance?
3. Are all relevant licensing documents referenced in the conceptual design plan?
4. Are there deficiencies in the references in the document? Are all relevant standards and guides stated?
5. Are there any unclear references? Are there any inconsistencies in the references of the document?
6. Are all relevant topics related to the system addressed in the conceptual design plan?

Outputs

1. List of standards and other relevant documents.
2. List of licensing documents mentioned in the conceptual design plan.
3. Review notes

Appendix B – Interview questions to the reviewers

1. Describe your review role. What is your review area? What does that area comprehend? What does not belong to that review area?
2. What kind of information is important to you in a typical conceptual design plan / other design phase document? Why is this information important? When reviewing design documentation, what are the questions that you are trying to answer?
3. There exists some background information related to your review role (e.g. YVL guides, basics of electrical engineering, plant operation). Describe how you evaluate the reviewed document against this background information.
4. Which one of your future work phases uses the information in a conceptual design plan? How is this information used? What is the output document of this future work phase? (E.g. the information is used in the design of function block diagrams)
5. Describe your current review practices. Do you have some specific technique?
6. What else would you tell about the review process to a new employee?