IFE/HR/E – 2006/011

Vision of a Framework for Design Guides for Development of Safety Critical Applications

Institute for Energy Technology

	KJELLER	HALDEN
Address	NO-2027 Kjeller	NO-1751 Halden
Telephone	+47 63 80 60 00	+47 69 21 22 00
Telefax	+47 63 81 63 56	+47 24 60

Report number	Date
IFE/HR/E-2006/011	2006-06-19

Report title and subtitle

Vision of A Framework for Design Guides for Development of Safety Critical Applications

Number of pages: 7

Project/Contract no. and name

ISSN: 0807-5514

Client/Sponsor Organisation and reference

ISBN: 82-7017-573-0

Abstract

Safety critical systems are strictly controlled and monitored along their whole life cycle from requirements elicitation and system development to utilization, modernizations and decommissioning. Often such systems need also to be licensed to suit their intended purpose, which is a demanding and complicated task. This paper first introduces the most important concepts and principles of designing safety critical I&C systems, especially for the nuclear industry. The importance of the research topic is justified and validation and licensing processes are discussed. General design requirements and other types of requirements related mainly on system modernizations are introduced as well. The paper presents an idea of a framework for design guides and provides a preliminary example to illustrate the concept. Finally, there is an outlook on the future plans and becoming work.

Keywords:

	Name	Date	Signature
Author(s)	Janne Valkonen	2006-06-19	Sign
Reviewed by	Atoosa P-J Thunem	2006-06-19	Sign
Approved by	Ø. Berg	2006-06-19	Sign

Vision of a Framework for Design Guides for Development of Safety Critical Applications

Janne Valkonen, MSc; Software Engineering laboratory (SElab), Halden Reactor Project; Institute for Energy Technology, Halden, Norway

Keywords: design, life cycle, requirements elicitation, licensing, nuclear automation

Abstract

Safety critical systems are strictly controlled and monitored along their whole life cycle from requirements elicitation and system development to utilization, modernizations and decommissioning. Often such systems need also to be licensed to suit their intended purpose, which is a demanding and complicated task. This paper first introduces the most important concepts and principles of designing safety critical I&C systems, especially for the nuclear industry. The importance of the research topic is justified and validation and licensing processes are discussed. General design requirements and other types of requirements related mainly on system modernizations are introduced as well. The paper presents an idea of a framework for design guides and provides a preliminary example to illustrate the concept. Finally, there is an outlook on the future plans and becoming work.

Introduction

The digital I&C (instrumentation and control) systems have been developing fast during the past few decades. Among other branches of industry, also nuclear power generation has shown carefully growing interest towards new technology. The carefulness comes mainly from the stringent safety requirements in the nuclear area and from the fact that there have to be enough operational experiences from other industries before new type of technology can be taken to safety critical applications.

In many nuclear power plants, the ageing of current I&C systems is becoming a problem because of growing economical and technical obsolescence. At many plants, the original I&C systems cannot be maintained until the end of the plant life cycle. Due to that, the interest towards implementing new digital I&C systems in nuclear power plants has been growing.

When adopting something new to a safety critical area, there is always lots of work related to the verification that the new types of systems could be used in nuclear power plant applications. It is because the authorities and regulators require that the systems and equipment in safety critical applications, especially at nuclear power plants, have to be validated so that they are suitable for their purpose along their whole life cycle. It means that the utility has to prove, show and report that systems are functioning safely in all conditions and situations. The same authoritative and regulatory requirements apply for both old and new technology. In the I&C modernizations, there is often need to interpret the old requirements from the viewpoint of the new system. It may also be necessary to create interfaces and establish communication between parts of the old and new systems.

The field of developing and licensing safety critical systems is very complicated and has many points to take into account. There are several parties and several development phases that have to communicate and fit together in order to reach successful results. The purpose of this paper is to make a vision of a framework for design guides for facilitating the design and safety demonstration of safety critical systems in nuclear power plants. The topic is relevant because of growing number of modernizations in nuclear power plants and it will also be easily implemented to other branches with safety critical applications.

To provide the reader with some background information about the area under consideration and give justification for the research, the following section describes shortly the concepts and principles of designing safety critical I&C systems. The section after that introduces validation and licensing processes and describes general design requirements and other types of requirements related mainly on system modernizations. The section number four presents the idea and example of the framework of design guides. Finally, the last section summarizes the presented ideas and provides an outlook on the future work and activities.

Design of Safety Critical I&C Systems

Nuclear power plant's I&C systems are designed to operate the plant during design basis and design extension conditions. The design basis conditions include normal operation (power operation, zero power operation, hot shutdown and cold shutdown modes), incident conditions (infrequent with limited damage) and accident conditions (design basis conditions). The design extension conditions include severe accidents.

I&C systems have a crucial role in the operation of a nuclear power plant. The most important tasks of I&C systems are to control and supervise processes in the power plant and the interfaces with the outside world. The control and supervising tasks are performed with human interactions or automatically according to predetermined rules.

The main objectives of I&C systems are safety, availability and performance of the plant. The requirements for I&C systems are derived from the main objectives and they are presented as functional and technical requirements. The functional requirements are implemented by the I&C systems. The protections prevent systems and process components from damages, the interlocking functions prevent unwanted operational conditions of process, the closed loop controls keep process parameters within predefined limits, the automatics start and shutdown processes and the measurement functions acquire process values and present them in the control room. The technical requirements influence mostly on the selection, design and implementation of equipment.

The I&C system needs lots of information from the process itself and also from control commands. This information is provided by different kinds of measurements or measuring systems. The HMI (human-machine interaction) is realized through different types of indicators, push buttons and computer workstations in control rooms.

Defense in Depth Principle: Defense in depth means several levels of protection, ensuring that if a failure were to occur, it would be detected and the release of radioactive material to the environment would be prevented (ref. 3). The concept is applied to all safety activities: organizational, behavioral and design related. It sets requirements for the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material) and helps to preserve them as well as protecting people and environment from radioactive materials.

Safety Classification: The safety classification is one of the most important requirement sources in designing the systems of a nuclear power plant. The classification follows usually the principle of defense in depth. All mechanical and electrical equipment in a nuclear power plant shall be categorized with respect to safety requirements. The categorization is needed for ensuring that the design, manufacturing, installation and operation actions are qualified according to the safety importance of each component. Safety classes determine quality requirements of nuclear power plant's systems, structures and components and their quality assurance.

Following Safety Glossary, Terminology used in nuclear, radiation, radioactive waste and transport safety (ref. 4), IAEA (International Atomic Energy Agency) makes a distinction between safety systems and safety-related systems, which together form the systems important to safety. Item important to safety is an item whose malfunction or failure could lead to a radiation exposure of the site personnel or members of the public. Safety related item is an item important to safety, which is not part of a safety system. Safety system is a system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

I&C System Architecture: The I&C system architecture means the organizational structure of an I&C system. The design of the I&C architecture provides a top-level definition of the I&C systems of the NPP, of the communication between these systems, and of the tools necessary to ensure a consistent interface between these systems (ref. 5).

The design of the architecture is based on the functional and technical requirements. Following Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems (ref. 5), the design of the I&C architecture shall decompose the entire I&C into sufficient systems and equipment to meet the requirements on:

- Independence of the functions in different lines of defense.
- Adequate separation of the systems of different classes.
- Fulfillment of the constraints on the physical separation and electrical isolation arising from the environmental and layout constraints, hazard analysis, and maintenance during operation.

The architecture of I&C in a nuclear power plant can be divided into three levels: Man-machine level, control system level and sensor/actuator level. The man-machine level includes emergency and main control rooms, and plant information system consisting of workstations, desks and panels. The control system consists of computer systems taking care of control functions. It is divided into safety systems, safety related systems and non-safety systems, according to safety classification. Sensor/actuator level comprises the individual sensors, transducers and switchgears providing information to and performing tasks provided by computer systems.

1 Validation and Licensing

Safety critical systems have to be validated so that they are suitable for their purpose along their whole life cycle. It means that the utility has to prove, show and report that systems are functioning safely in all conditions and situations. Licensing is a demanding and complicated task, where the regulatory body issues a legal document to the licensee granting authorization to perform specified activities related to a facility or activity.

Following and interpreting (ref. 1 & ref. 12), safety goals and requirements originate from legislation comprising of acts and regulations. Requirements for the design, functions, systems and equipment are described in the Safety Analysis Report (SAR) of the plant. Laws, regulations and SAR together dictate the safety importance of a specific safety function and its associated systems and equipment. The safety importance is expressed by safety classes, which were discussed in previous section.

The licensing process is formed by interrelated activities for collecting and assessing the acceptability evidence. It is often called a safety case, and it consists of safety claims, evidence supporting the claims, and the arguments and inference mechanisms supporting the evidence. The SHIP Safety Case Approach (ref. 2) defines safety case as: “A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.” The safety case should be constructed along with the system development life cycle and maintained as the system is changed. The system acceptance criteria finally define the necessary procedures and their application level both for the system development process and also for its assessment process (licensing process, safety case).

General Design Requirements: There are several general safety requirements that must be taken into account when designing safety critical systems. Majority of them come from standards and authoritative regulations. For example: The duplication of critical parts in a system with the intention of increasing reliability is called redundancy. In many safety-critical systems, like in reactor protection system, some parts of the control system may be triplicated or quadrupled. An error in one component may then be outvoted by the other similar components. Because components are expected to fail independently, the probability of all of them failing is extremely small. Because the purpose of this paper is to describe a vision of a framework of design guides and not to describe all the general design requirements, some of them are just listed in the following: redundancy, diversity, independence, separation, power supply demand, fail safe principle. Explanations and further information can be found from the relevant guides and standards (ref. 5, 6).

Other Requirements: In addition to general design requirements, there are some other types of requirements affecting on the design and implementation. Because of high reliability requirements, simple solutions can be considered better than complicated ones. Simple solutions and implementations are easier to maintain and control and there are less parts susceptible to failures. Also robustness may be important. It means that small disturbances or changes in the environment or in the system (e.g. related systems) do not affect on performance or reliability.

The requirement of minimizing the number of cables may come from e.g. the requirement of minimizing the cost, or from the requirement of robustness. Cables may be required to be distributed into different fire compartments, which also implement the diversity requirement. Also maintainability of systems or components may affect on design decisions and implementation.

At some stages the importance of low cost drives over the well known ALARA principle of risk (As Low As Reasonably Achievable). That is why there is the word ‘reasonably’. Budgets are not limitless. Because the nuclear field is not that big and the safety requirements are very stringent, the lack of variety of available technologies (e.g. application platforms) may restrict options and set requirements from that viewpoint as well.

Vision of the Framework

The previous sections described the area under consideration and current practices related to it. This section will now make a vision of the opportunities that could improve the efficiency of actions related to designing and licensing safety critical systems. The suggested framework for design guides could have a positive affection on demonstrating the safety and it would help both the system developers and also regulators in their tasks and enable better communication between them when applying and granting licenses.

The main idea is to create a framework for design guides that take safety and dependability issues into account and deals with testing, quality management, fault-tolerance, and formal qualification / licensing of such applications. The aim is to characterize and typify existing nuclear automation solutions and look for repeating patterns and formalisms from requirements, problem definitions, design solutions, implementations, and testing and licensing activities. The starting point and initial assumption is that there are similarities between the development phases of different safety critical systems and functions.

As Raheja & Moriarty state in Design for Safety (ref. 7), safety should be treated like a product, which is a deliverable item and the customer can tell if it is delivered or not. Then the building blocks of a product called safety are proven methods, structures and solutions listed in design guides. In case of nuclear power plants and related applications, the customer is the regulator, who tells if sufficient safety is delivered or not.

The first step in the development of these design guides is to search for repeating characteristics in the problem definition and requirements specification phases and secondly in design phases and further in implementation and testing phases. Examples of development life cycles from real applications play key role in this. Figure 1 illustrates the main idea. By taking several examples from different systems, and by comparing them with each other, the purpose is to typify repeating types of problems and repeating ways of solving them.

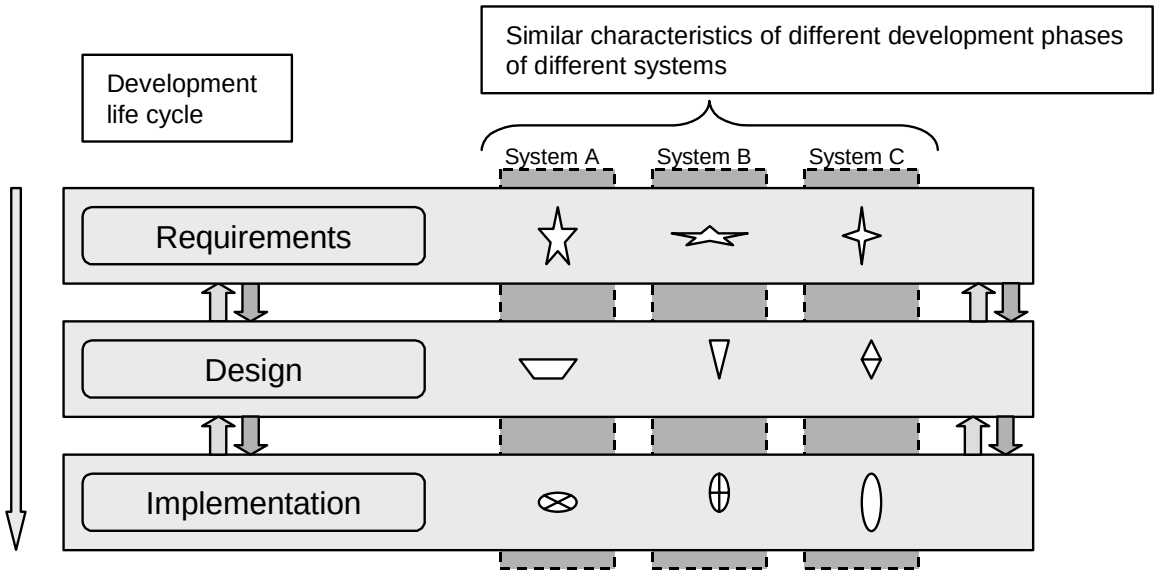

Figure 1 — Simplified Life Cycle and Visualization of Similar Characteristics in Example Systems.

There is a simplified view of the development life cycle on the left hand side of Figure 1. The cycle is simplified because these three phases - requirements, design, and implementation - are the phases where the partial results of development activities are seen most easily. The importance of other typical phases is not underestimated, but they are more or less only supporting the development and making sure that the partial results can be accepted for the next development phases.

On the right hand side of the figure, there are three example systems: A, B, and C. They are different systems, but they all have high safety significance and they have to be approved by authorities before they can be taken into use. They have similar types of requirements (as described in the chapter above), which have to be validated and possibly checked by authorities before they can be taken to the next development phase. That is typical for systems in nuclear power plants.

These three systems (A, B, C) seen in the figure, have similar types of requirements, which are described by different forms of star figure. When going from the requirements phase down to the design phase, it can be seen that the designs of systems (or at least parts of them) have common features as well, and they can be categorized in a similar way as was done with the requirements. The same principle applies also for the implementation, which is described by different forms of ellipses with or without a cross inside.

Example from a Reactor Protection System: Let's take a simple example from a reactor protection system (RPS), which has a very high safety importance. The system's main purpose is to guarantee the safe shutdown of the reactor and ensure the heat removal from the reactor core to the final heat sink. Another important task of the RPS is limiting the consequences of anticipated operational occurrences and accident conditions. At this stage of the research, the example is only demonstrating the idea and what will be done, meaning that the example is not complete or finished

As an example, one of the requirements set to the RPS is independence from other systems. Independence prevents propagation of failures from system to system and propagation of failures between redundant parts within systems, and common cause failures due to common internal plant hazards (ref. 6). That is the requirement part and the next step is to find how the requirement should be transferred to design efficiently and without loosing any information or changing the meaning of the actual requirement.

In this case, we can say that independence can be achieved at least by means of physical separation and electrical isolation, and by independence of communication methods and the implementation of communication between different systems. This sets the starting point for designers. There are also other systems having similar requirements and they can be put into the same category. Further on, the implementation will get the input from design and there are new problems and solutions, which may belong e.g. to the group listed earlier under heading "Other requirements".

Above the requirements, designs, and implementation solutions lies always the need for licensing and demonstrating safety, which should make a continuous chain between the different phases in the vertical direction in Figure 1. The purpose of the framework is not only to help on that vertical level, but also to find and connect the similarities of life cycle phases on the horizontal level.

Notation: It is not wise to start inventing a new notation for this kind of framework for design guides, because there are already several approved notations available, just to mention object-oriented modeling (ref. 11) and IDEF (integrated definition language) (ref. 8). The vision is to choose one approved notation and describe developed design guides as a combination of graphical notation and written instructions. The written parts of guidelines are intended to follow similar type of format as used in describing design patterns (ref. 9) and also safety case patterns (ref. 10) which have adopted their notation from design pattern world.

Summary and Outlook

This paper describes a vision of a framework for design guides for facilitating the design and safety demonstration of safety critical systems in nuclear power plants. The idea has been discussed with several professionals working in the field, but it needs, of course, further refinement and hard work to get from the ideas to real utilizable results.

The desirable result is a ‘hand book’ or a ‘recipe book’ of design guides for different needs in the fields of safety critical automation design, software development, quality procedures and analysis and system licensing. Having such a framework of guides, engineers could easily utilize it in development activities and for safety demonstration purposes. By knowing for what kind of purposes each guide is suitable for, it would be easy to use them as guidelines and references along with the development. For example, by following a certain type of approved guide, the developer could be quite confident that the system under development meets the required regulations and standards. That would also make licensing of systems easier, as the regulator would see that the system development has followed a certain already proven pattern. That would naturally make the licensing activities and the safety case justification a lot simpler and improve the quality of outcome.

One future benefit of successful research results in this area can be seen as public, open, and critical discussion and consensus about which solution or procedure is good and which is not so good. That might lead to similar development evolution phenomenon as with design patterns in the area of software engineering, where good solutions have evolved and developed further, while the evolution has eliminated the weaker solutions by itself. To achieve this kind of open discussion, the atmosphere and the attitudes towards open information sharing have to be changed.

References

1. P. Haapanen, J. Korhonen, and U. Pulkkinen, Licensing process for safety-critical software-based systems, STUK-YTO-TR 171, Oy Edita Ab, Helsinki, December 2000

2. P. Bishop, and R. Bloomfield, The SHIP Safety Case Approach, SafeComp95, Springer, Belgirate, Italy 11-13 October 1995, (Ed. Gerd Rabe), pp. 437-451

3. IAEA (International Atomic Energy Agency), Safety of Nuclear power plants: Design, Safety requirements, Safety standards series no. Ns-r-1, Vienna, 2000

4. IAEA (International Atomic Energy Agency), Safety Glossary, Terminology used in nuclear, radiation, radioactive waste and transport safety, Version 1.0, April 2000

5. IEC 61513, (International Electrotechnical Commission), Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems, 2001

6. IAEA (International Atomic Energy Agency), Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Guide No. NS-G-1.3, Vienna, 2002

7. Raheja, D., and Moriarty, B., Design for Safety, Journal of System Safety, Volume 41, No. 4, July - August 2005 Washington DC

8. IDEF webpages, http://www.idef.com, accessed 21st Feb, 2006

9. Gamma, E., Helm, R., Johnson, R., and Vlissides, J., Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley, 1995

10. Kelly, T.P., Arguing Safety - A Systematic Approach to Safety Case Management, DPhil Thesis, University of York, Department of Computer Science, September 1998

11. Rumbaugh, J., Blaha, M., Premerlani, W., Eddy, F., and Lorensen, W., Object-Oriented Modeling and Design, Prentice-Hall, 1991

12. T. Sivertsen, R. Fredriksen, A. P-J Thunem, J-E. Holmberg, J. Valkonen, O. Ventä, J-O Andersson. Traceability and Communication of Requirements in Digital I&C Systems Development. Final Report, NKS-115, ISBN 87-7893-176-2. Nordic nuclear safety research (NKS, 2005)

Biography

Janne Valkonen, MSc, Software Engineering laboratory (SElab), Computerised Operation Support Systems Division, Institute for Energy Technology, OECD Halden Reactor Project, P.O. Box 173, NO-1751, Halden, Norway, telephone +358-50-3240118, e-mail - janne.valkonen@hrp.no

Currently Valkonen works as a visiting researcher for the Institute for Energy Technology in Halden, Norway. He also works part time for his home organization, VTT Technical research centre of Finland. He is also a PhD student at the Helsinki University of Technology. His experience is in requirements engineering, simulation of batch processes, distributed energy systems and innovation management.