International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies (NPIC&HMIT 2000), Washington, DC, November, 2000.

# Methodologies and Processes for the Development of Embedded System S/W for Nuclear Power Plant I&C Equipment Using CASE Tools

**Byungyun Lee, Hongju Moon, Myung-Hyun Yoon**
Korea Electrical Power Research Institue
103-16, Munji-Dong, Yusung-Ku, Daejeon, 305-380, Korea
E-mail : bylee@kepri.re.kr, hjmoon@kepri.re.kr, yoon@kepri.re.kr

**Yongkwan Lee**
Korea Electrical Power Research Institue
103-16, Munji-Dong, Yusung-Ku, Daejeon, 305-380, Korea
E-mail : leeyk@kepri.re.kr

**Keywords**: embedded system, requirement traceability management, configuration management, CASE tool

## ABSTRACT

The paper describes what is the main issues of the S/W development in the nuclear digital I&C equipment and how they can be managed efficiently, through the case study of the DCS development project. Particularly, the discussions in this paper concentrate on the analysis & design method, requirement traceability management and S/W configuration management that are closely related to the development method and processes for the embedded system S/W in digital I&C equipment. And, also in order to support the S/W development methods and processes effectively, the related CASE tools are considered and the CASE environment is presented as a real example based on the DCS project.

## 1. Introduction

The digital system has more strong points than the analog I&C system does, especially such as functionality, economical efficiency, maintainability etc. But, because most of functions in digital system depends on the S/W, the prediction and analysis of malfunction of the digital system are much more difficult than those of analog system whose malfunction usually originated from physical and environmental causes. And, the range of influence caused by the failure in analog system can be easily restricted to single mode failure, but, in the digital system a failure can affect wider range of system than that of analog system. So, in the development of digital I&C systems for nuclear power plants, the most important current issues are how to develop, verify and validate the S/W to be reliable enough and how to develop, verify and validate to avoid the common mode failure. For the successful management these obstacles, not only the design itself of structures and functions of digital I&C equipments but also the selection of the development processes, methods and their supporting tools, which are rapidly changing and have a lot of diversity, is critical.

In this paper, the development project of DCS(distributed control system), which is the state of the art digital equipment and is the composite of modern digital technology, is introduced. Through the case study of this project, the applicable methods and processes for the development of the S/W in digital I&C equipment for the nuclear power plants are considered. In order to support the processes and methods efficiently, their supporting CASE(computer aided S/W engineering) tools are also considered and CASE environment of this project is presented.

## 2. Introduction of Nuclear Power Plant DCS Development Project

### 2.1 System structure

The system structure and components are shown in Fig. 1. The DCS is composed of OIS(Operator Interface Station), EIS(Engineering Interface Station), PCU(Process Control Unit) and FCU(Field Control Unit). They are connected with three communication networks, which are Information network, Control network and Field network. And, each communication network is interconnected and isolated with respect to the information and signals through the DGW (data gateway).

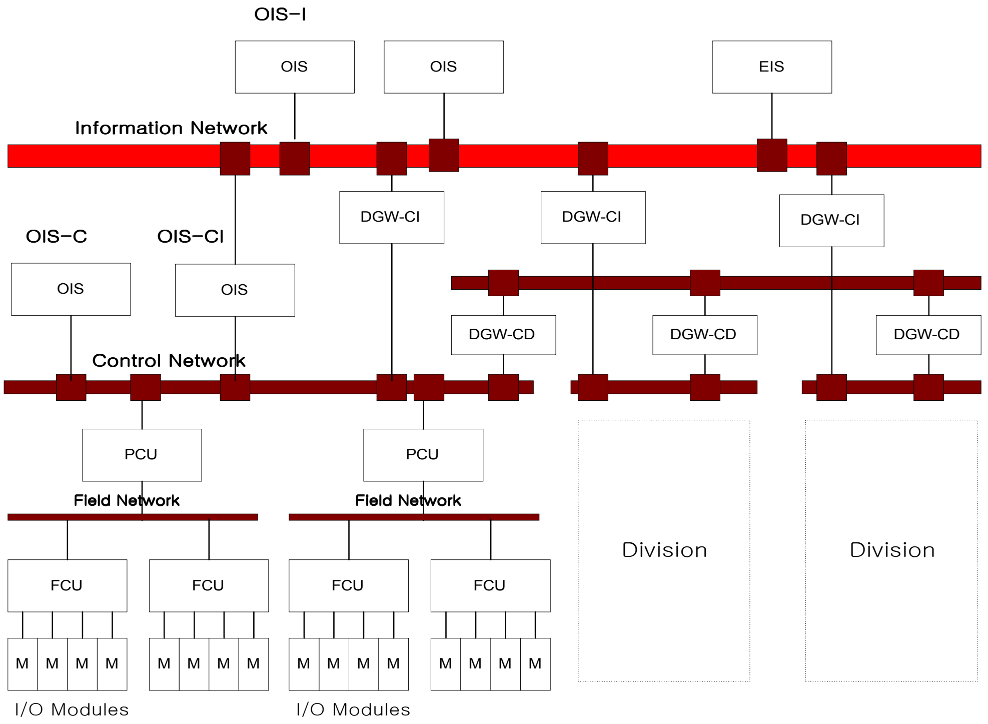

Fig. 1 The structure of DCS(distributed control system)

### 2.2 The organization of DCS development team

The DCS development is a joint development project in which three independent organizations participate. They are remotely located in long distance and composed of system development team, network development team and system V&V team. Fig. 2

shows the organization of the DCS development team. For the independent V&V, the V&V team is organized independently with the development teams.

## 3. S/W Development Issues

There can be many issues with respect to the S/W development, but in this paper, the processes and methods related issues are considered.

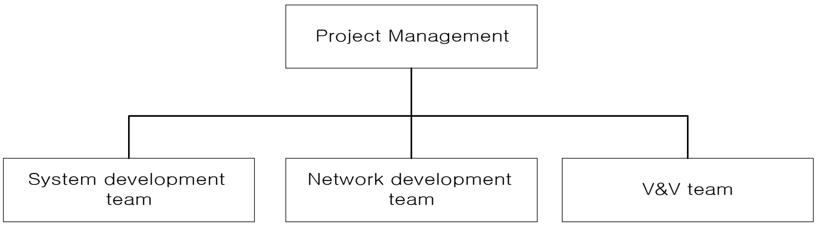

Fig. 2 The organization of DCS development team

### 3.1 S/W development life cycle

The waterfall model that is a classic life cycle is the oldest and most widely used paradigm for S/W engineering. However, over the past decade, criticism of the paradigm has caused even active supporters to question its applicability in all situations. Among the problems that are sometimes encountered when the classic life-cycle paradigm is applied are(Pressman, R.S., 1992):

- Real project rarely follow the sequential flow that the model proposes. Iteration always occurs and creates problems in the application of the paradigm.
- It is often difficult for the user to state all requirements explicitly. The classic life cycle requires this and has difficulty accommodating the natural uncertainty that exists at the beginning of many projects.

It is expected that this DCS development project will be encountered the same problems. But, the classic life cycle, a water fall model, is chosen according to following reasons:

- The iterations in the development are indispensable facts. However, one can manage and confine the iterations of development as if they occurred in the one step of waterfall model. In this case, to the point of over all project period, it can be considered as a waterfall model, but in the point of each development step it can be considered as if it is a spiral model.
- User requirements are always floating. But, in this project, the user requirements are almost originated from the system design specifications, which are already fixed. In order to take the advanced requirements that are floating to some extent according to the change in the technological circumstances, it is believed that the requirement traceability management system that is proposed later will be helpful to manage them.

### 3.2 Verification & validation

In the development of digital I&C system, the S/W V&V (verification and validation) is the very important activity. In this project, the general principles of the V&V activities are (Levy, S., 1994):

- V&V activities throughout the life cycle
- V&V should consider both process and product.
- V&V tasks should be traceable back to S/W requirements.
- A critical software product should be scrutable by independent evaluation and testing.
- V&V team members should be independent.
- V&V effort should be concentrated on area of high value and high risk
- Discrepancies should be documented.

### 3.3 S/W RTM (requirement traceability management)

The requirements are specifications that the system, which is being built, must meet. Requirements can be originated from several sources such as plant system design specifications, plant operating guideline, nuclear regulatory guide, prototypes, development meetings and more. The development of good requirements is essential to the quality product design. Requirement definition is helpful to find the contradictions, inconsistencies, redundancies and ambiguities before implementation begins. And, as mentioned above, in the V&V principles, the requirement traceability throughout the life cycle is essential principle (Levy, S., 1994).

Furthermore, in order to guarantee the requirement driven development and V&V, requirement centric communication and the share of correct requirements are essential. The requirement management is applicable not only to the S/W development but also to H/W development.

### 3.4 S/W analysis and design methods

One of the most heavily researched areas of S/W engineering over recent years concerns analysis and design methods. Two major categories of method merit particularly close examination (Morris, D., 1995). These are structured methods (War, P., Mellor, S., 1985) and object-oriented methods (Booch, G., 1994). The development environments of the OIS and EIS are naturally visual tool environment that is closely related to the OO (Object-oriented) methods. Because they have GUI functions and are operated on the commercial OS. In the FCU and PCU that are embedded systems, traditionally the structured analysis and design methods are widely used. But, today's arguments supporting OO (Object-oriented) S/W development appear in many publications (Douglass, B.P., 1999). Making a choice between the structured method and object-oriented method is not straightforward in the embedded system. The followings are mainly considered to select the methods of analysis and design for the embedded system.

### 3.4.1 Reuse of existing S/W

This project do not start from zero base and developers naturally want to reuse the existing S/W code such as libraries, which was developed in the structured methods, for the efficiency of development. Inherently, OO (Object-oriented) methods can provide highly reusable S/W module. However, in order to use the OO (Object-oriented) method, the existing S/W which have been developed using the structured method must be redesigned to OO (Object-oriented) style and the developers must change their developing paradigms into new OO (Object-oriented) paradigm. They can be strong challenge for the developers. Other proposals for dealing with reactive systems have considered the merger of the structured and OO (Object-oriented) approaches, by using SA to front end an OO (Object-oriented) result (Ward, P.T., 1989). Part of the motivation for this derives from desire to retain the best elements of a well tried and proven method (i.e. SA), but there is also a feeling that, in some applications at last, analysis of the system's functional behavior is a legitimate up-front issue. However, some workers consider the two approaches to be fundamentally incompatible, asserting that considerations of functional behavior, applied at an early stage, will seriously deform the embryonic structure of a system.

### 3.4.2 Trend of analysis and design method for embedded system

There does at least appear to be a strong consensus that an OO (Object-oriented) analysis, design & implementation is desirable more and more in the embedded system development. There are many publications to support OO (Object-oriented) method for embedded system development. Moreover, the tools supporting UML (unified modeling language) standard, which conquer several OO (Object-oriented) methods, accelerate this progress. We come to the fork of the road. There are well known advantages to support the OO (Object-oriented) method (Douglass, B.P., 1999):

- Consistency of model view
- Improved problem-domain abstraction
- Improved stability in the presence of changes
- Improved model facilities for reuse
- Improved scalability
- Better support for reliability and safety concerns
- Inherent support for concurrency

### 3.4.3 Optimization of the object code

In the embedded system such as FCU and PCU, the S/W is closely related to the H/W for the real time operation requirement, efficient use of system resources, etc. The S/W must be compact, optimized, and executed efficiently. Basically, in the OO paradigm, the S/W is executed on the basis of message passing among objects. This may require more resources and less optimal than those with structured paradigm. And also, the inheritance, encapsulation and polymorphism can be burden for the compiler to optimize the object codes.

### 3.4.4 Consistency between analysis & design

OO analysis is argued to be the most natural way to understand and model the problem domain with real-world entities prompting the choice of objects on which the abstract system model can be based. Moving from analysis to design is also considered to be simpler when using OO techniques, as it involves only incremental refinement and development rather than the creation of structurally different models. The one of the strong challenge in OO analysis and design is how to discover objects and structure their class definitions, in a way that represents the best grouping of data and function. But, in the structured methods the analysis and design model are quite different and the implementation also quite different from the model. So, the model change may cause the in consistency between the analysis and design.

For the future trend, we have to follow the OO paradigm but the ground we stand must be strongly considered. For the OO process and method, the embedded system engineer have to leave their practiced paradigm and adapt themselves to the new one. It takes a rather long period and additional cost to train them because the two paradigms have quite different approaches. This is a quite big burden to rush toward OO paradigm instantly. For the new paradigm, it is recommended that the gradual progress should be taken. As a result, in the DCS project, the structured methods are decided in the development of embedded system S/W.

### 3.5 S/W configuration management

The S/W configuration management issue contains followings (Pressman, R.S., 1992):

- Identification of objects in the S/W configuration
- Version control
- Change control
- Configuration Audit
- Status reporting

## 4. S/W Development Using CASE Tools

In order to manage efficiently the S/W development issues, the use of the CASE tools is actively considered and the CASE environment is constructed in the DCS project. The CASE (Computer aided S/W engineering) tool can be as simple as a single tool that supports a specific S/W engineering activity or as complex as environment that encompasses tools, a database, people, hardware, network, operating systems, standards, and myriad other components and there are many kinds of CASE tool such as business system modeling tools, project management tools, S/W configuration tools and more. Naturally, the fully integrated CASE environment is highly expensive and has many risks to introduce and manage them. So, some of essential CASE tools which are closely related to the S/W development issue presented above section are evaluated to construct the proper and reasonable CASE environment.

### 4.1 Evaluation and selection of the CASE tool

The evaluation and selection of CASE tools are performed according to the 'IEEE Std 1209-1992 Recommended practice for the evaluation and selection of CASE tool'. In the following sections, the decision criteria for the evaluation & selection of CASE tools in the DCS project are presented.

### 4.2 Analysis and design CASE tool

#### 4.2.1 OO analysis & design method CASE tool

Currently, the UML (unified modeling language) based tools seize the power in their OO method tool market. But, almost UML based tools support the editing the diagrams that are the UML standard and the generation of the skeleton of source code based on the class diagrams. Moreover, the UML specifications have the formalism that is good advantage for the development of the system required high reliability. But, this is not sufficient to our scope. For the requirement specification validation of some S/W modules, simulation and prototyping functions are needed. The items of main decision criteria are as follows:

- Support the UML standard
- Animation of sequence chart
- Animation of statechart
- Static/Dynamic test of model

#### 4.2.2 Structured analysis and design method CASE tool

There are also many methods for structured analysis & design of S/W. But, most of them, such as activity diagram, data flow diagram etc., which is not appropriate for the reactive embedded system, are for the general application S/W. For the reactive embedded system modeling, the statechart, which is based on the visual formalism, is one of the good considerations (Harel, D., 1987). The items of main decision criteria are as follows:

- Animation of statechart
- Functional, behavioral and structural view
- Static check of the model

### 4.3 Requirement traceability management CASE tool

Through the requirement traceability management tool, it is expected that the requirement driven development and V&V (Verification and validation), clear communication among participants in this project and shared requirement will be accomplished. Especially, because the participants are remotely located, the improvement of requirement centric communications is much more expected. For the traceable V&V activity and development, the requirement traceability management tool can be used through the entire development life cycle and not only requirements but also all the development documents are managed in the database of the requirement traceability management tool. And their linkage among items that are identified from requirement and development document will provide the traceability from requirements to the final products. And also the generation of documents from the requirement traceability tool, the configuration management of document and reduction of labor to generate the documents will be expected. The items of main decision criteria are as follows:

- Remote access through the Internet
- Linkage among the object item
- Automatic generation of document
- Support for communication tool
- Security functions
- Object item configuration management

### 4.4 Configuration management CASE tool

In the large-scale S/W development project, the S/W configuration management is the traditional issue. In addition, like this project situation of remotely located developers who must be under the same configuration management control, it is almost impossible without supporting of appropriate CASE tools. There are many S/W configuration tools and their functions are almost same. The items of main decision criteria are as follows:

- Remote access of configuration item through Internet
- User-definable change control procedure

### 4.5 Proposed CASE environment

Fig. 3 shows that the constructed physical environment of CASE tools. The NDCS-DV server contains the requirement traceability management tool, S/W analysis & design tool, S/W configuration management tool and shared disk as a repository of development results.

## 5. Conclusions

In this paper, several issues related to the methods and processes for developing the S/W in the nuclear power plant digital I&C equipment are considered and discussed. They are mainly related to the selection of the S/W life cycle, S/W V&V, requirement traceability management, S/W configuration management and the analysis and design method for the embedded system S/W. And, also in order to support the considered processes and methods efficiently, the CASE tools are considered. Especially, in the DCS project, in order to improve the communications among developers and V&V doers, the Internet based CASE environment is constructed and presented.

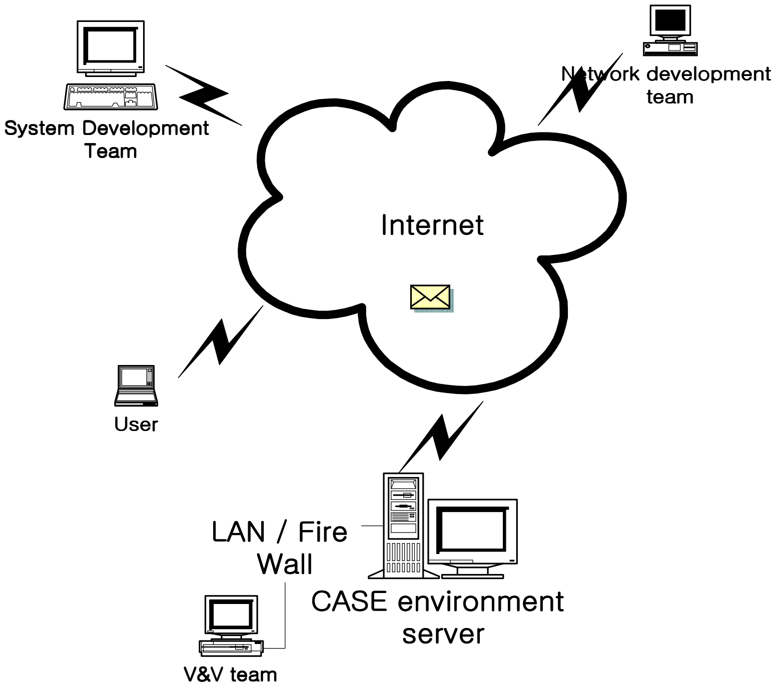

Fig. 3 The physical CASE environment

## REFERENCES

BOOCH, G., 1994. Object-oriented design with applications, Benjamin/Cummings Publishing Company, Inc., Redwood City, California, 2nd edn.

Douglass, B.P., 1999. Doing Hard Time: Developing Real Time Systems with UML, Objects, Frameworks, and Patterns, Addison-Wesley

Harel, D., 1987. STATECHARTS: a visual formalism for complex systems, Sci. Comput. Progr., pp.231~238

Levy, S., Handbook for Verification and Validation of Digital Systems, Electrical Power Research Institute EPRI TR-103291-V1, V2, December 1994.

Morris, D., Green, P., Barker, R., Nov. 1995. Engineering the Software in systems, Software Engineering Journal, pp.253~265

Pressman, R.S., 1992. Software Engineering: A Practitioner's Approach, McGraw-Hill

Ward, P., Mellor, S., 1985. Structured Development for Real-time systems, Prentice-Hall, Inc. Englewood Cliffs, New Jersey

Ward, P.T., 1989. How to integrate object-orientation with structured analysis and design, IEEE Trans. Software