Development Strategies of an Information Minimalism Prototype for a Monitoring System of Korean NPPs

Gwi-sook Jang [a*], Jae-hwan Kim[b], Gee-yong Park[a]
[a]I&C and HFE Research Division, Korea Atomic Energy Research Institute, 989-111, Daedeok-daero, Yuseong-gu, Daejeon 305-353, Republic of Korea
[b]Maritime Reactor Development Center, Korea Atomic Energy Research Institute, 989-111, Daedeok-daero, Yuseong-gu, Daejeon 305-353, Republic of Korea

1. Introduction

Currently, the information display of the digital based control room of Korean NPPs (Nuclear Power Plant) is operated with hierarchy structure of the system-oriented, component-oriented and function-oriented based on existing P&IDs. The operator obtains the monitoring and the controller information necessary for operation through the information navigation by hierarchically distributed information over five or more display pages to perform a particular operation mode. As a result of the intervention of these additional tasks, the reaction time is delayed and it is difficult to maintain the cognitive context, and it can cause the cognitive error in the emergency situation.

Therefore, it is necessary that an information structure and visualization shall be designed to minimize the cognitive burden of recognition, memory, and judgment on the relationship between complex systems when an unexpected event occurs. The information structure and visualization design is based on careful analysis and understanding of the work domain of the operator.

In order to solve the above problem, the designer has to decide how to reduce the amount of information to be displayed on the screen so that the user can work easily. Also, it is important to provide a means for the operator to easily move in the information display space and naturally make a cognitive transition in the display design with a large amount of information networks.

We proposed a monitoring and controller display method for each operation mode based on log analyses of operator actions to overcome the above problems last year [1]. This method minimizes the existing information navigation by providing monitoring and control means necessary for the operator to perform a specific operation mode on one or two display pages. The method provides the monitoring and controller information for each operation mode of NPP to operator based on the understanding of the work domain of the operator. And the method complements the monitoring information and the control means for each operation mode through analysis of the operation behavior logs obtained during operation to improve the efficiency of the display for each operation mode (See Fig.1).

This paper proposes detailed design ideas and additional issues of information minimalism in Korea NPP (See Fig.2). Also, this paper proposes development strategies of an information minimalism prototype for a monitoring system of Korean NPPs.

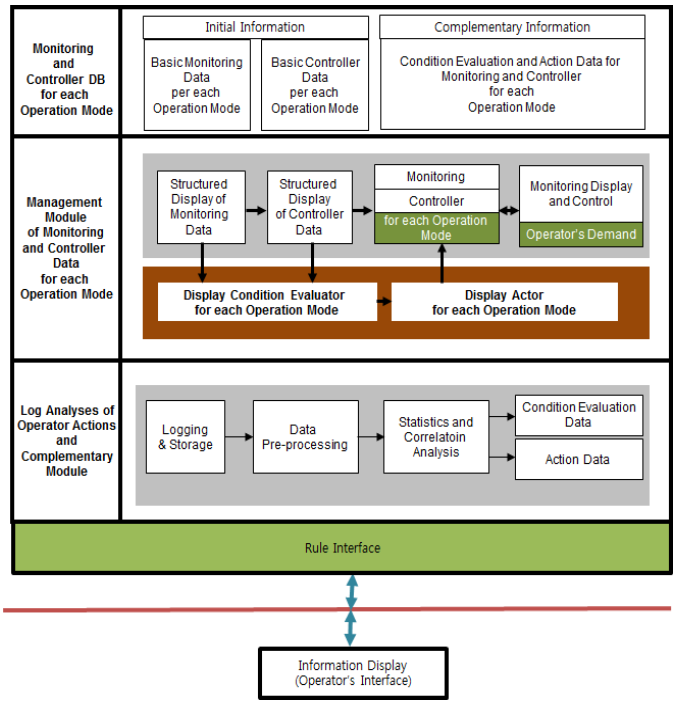

Fig. 1. A Monitoring and Controller Display Method for each Operation Mode based on Log Analyses of Operator Actions

Design Ideas and Issues	Description
Information Minimalism	▪ Minimize unnecessary screen components to reduce screen complexity ▪ Visualization scheme to reduce display transition than commercial NPP ▪ Easy display page navigation
Information Structuring and Visualization for Information Minimalism	▪ Operator task-oriented information display structure ▪ Monitoring and control display by operation mode ▪ Reflecting experience information analyzing operator activity log ▪ Go to the desired screen with information site map ▪ Display bookmarks are provided to collect only the operator selection display
Additional Issue	▪ Preparing the database security in information log ▪ Display sharing scheme for information display device failure

Fig. 2. Design Ideas and Issues of an Information Minimalism

2. Development Strategies of Prototype

The development principles of prototype to confirm the information minimalism concept is as follows:

- Standardization and modularization the development process by improving a development productivity and reuses
- Establishment of prototype product sharing systems
- Establishment of prioritized development items and step-by-step development
- Identification of common risk factors and design security for safe software development
- Performing objective risk analysis and testing on all prototyping outputs

In order to satisfy the development principles described above, the following prototype development strategies are set up.

2.1 Component Based Development (CBD)

The development process of S/W components and component-based systems differs in many significant ways from the "classical" development process of software systems. The main difference is in the separation of the development process of components from the development process of systems. The primary idea of the component-based approach is the (re)use the existing components instead of implementing them whenever possible. Fig. 3 shows a detailed V-shape development process for CBD. The main idea of the component-based approach is building systems from already existing components.

Fig. 4 shows one example of components and a component diagram for this prototype.

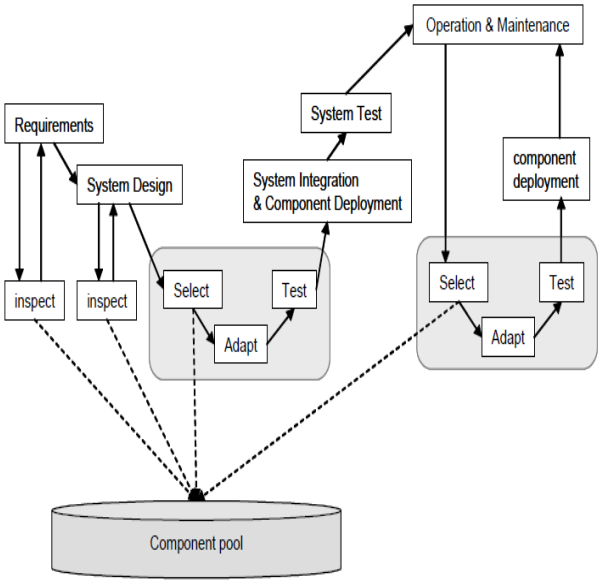

Fig. 3. A Detailed V-shape Development Process for CBD

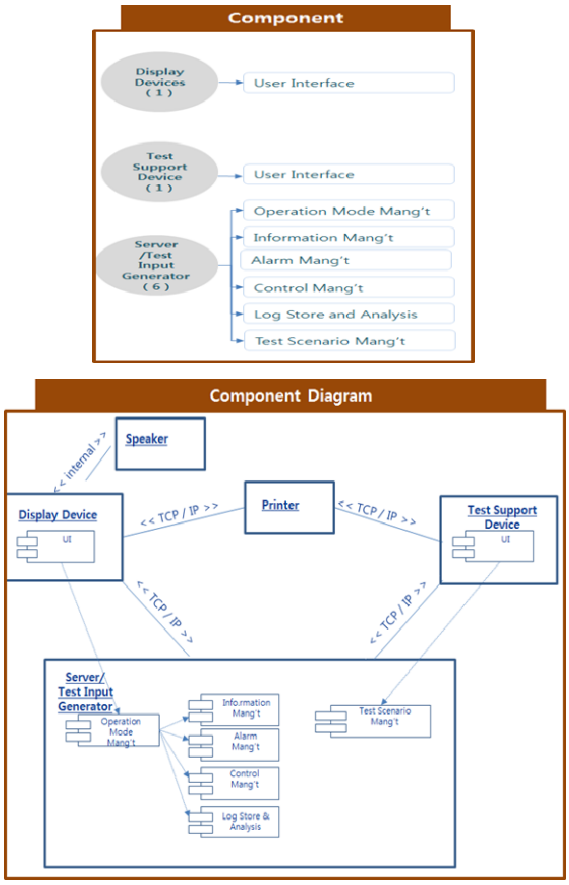

Fig. 4. Component and Component Diagram for Prototype

2.2 Secure SDLC

Secure SDLC (Software Development Life Cycle) process ensures that security assurance activities such as penetration testing, code review and architectural analysis are an integral part pf the development effort.

Software security touchpoints are based on good software engineering practice and involve explicitly pondering security throughout the software lifecycle [3]. Table I shows a secure SDLC plan for this prototype.

Table I: A Secure SDLC Plan for the Prototype

SDLC	Description	Result
Requirements and use cases	• Converting both overt functional security(e.g., use of applied cryptography) and emergent security propertied (as reveals by the abuse cased and attack patterns) • Describe the system's behavior when under attack to clarify what areas and components of the software-based system need to be protected, from which threats, and for how long	S/W Req'ts Spec.

Architecture and Design	• Includes documenting assumption and identifying possible attacks, and uncovering and ranking architectural flaws for mitigation. Recurrent risk tracking, monitoring, and analysis should be ongoing throughout the life cycle	S/W Design Spec.
Test Plans	• Includes testing of security functionality using standard functional testing techniques, and risk-based security of the software as a whole, with test scenario based on attack patterns	Test Plan & Procedure
Code	• entails use of static analysis tools to detect common vulnerabilities	
Test and Test Results	• With the architectural risk analysis results driving the selection and implementation of "canned" black-box tests offered by automated application security and penetration testing tools	Test Report
Feedback from the Field	• After Development, this includes monitoring the behavior of the fielded software system for indications of attacks and exploits against the software. Knowledge gained through monitoring attacks and exploits should be cycled back into the other touchpoints	S/W Req'ts Spec.

3. Results and Future Plans

Traditional HMI design approach of NPPs was heavily based on P&IDs. A current trend in Korea NPP is to modernize control rooms with moving from panel-based traditional control rooms to computerized solutions. A significant amount of work was been done on process control HMI design using ecological interface design and the operator centered interface. These designs were applied to a limited set of screens and did not differ largely from the traditional HMI design in that the layout the information is somewhere similar to P&IDs [4].

This paper proposes detailed design ideas and additional issues of information minimalism in Korean NPPs. Also, this paper proposes development principles and strategies of an information minimalism prototype for a monitoring system of Korea NPP.

These concepts provide the monitoring information and control means necessary for the operator to perform a specific operation according to operation mode. This method can reduce the information searching process time and the transition between the display pages. So, this method can be provided as an alternative to overcome the problems of P&ID based hierarchical information provision. And this concept is added to the concept of operator support with the existing display configuration and navigation as it is, and it is anticipated that it extends its application range while actually utilizing it.

REFERENCES

[1] G.S.Jang, S.M.Lee, G.Y.Park, A Monitoring and Controller Display Method for each Operation Mode based on Log Analyses of Operator Actions, Transactions of the Korean Nuclear Society Spring Meeting Jeju, Korea, May 18-19, 2017.
[2] I.Crnkovic, S.Larsson, Component-based Development Process and Component Lufecycle, Malardalen University, Sweden.
[3] Goertzel, "Software Security Assurance: A State-of-the-Art Report", IATAC, July 2007.
[4] S.Y Kim, J.V.Wormer, Human-Machine Interface Design for Power Generation Plant Operators.