Safety benefit evaluation of data communication between IFPD and ESCM

Yun Goo Kim[*], Eung-se Oh

Korea Hydro and Nuclear Power Co., ltd, Central Research Institute, Daejeon, Korea
[*]*Corresponding author: ygkim.stpn@khnp.co.kr*

1. Introduction

The independence between safety system and non-safety system is one of the important design requirements in the nuclear power plant's instrumentation and control (I&C) system. The non-safety system shall not prevent the safety system from performing its intended safety functions [1].

If there exists any connection between safety system and non-safety system, the connection may challenges the independence. The connection may have the potential safety loss which interference the safety function of safety system. Therefore, connections between safety system and non-safety system must be deemed and the benefit of the connection should be obvious despite of the potential independence degradation. In the APR1400 human system interface (HSI) design, each operator console is designed as a sit down workstation type with four information flat panel displays (IFPDs) and four soft control module (ESCMs) to control individual safety components in the engineered safety features component control system. All IFPDs are designed as non-safety system and ESCMs are designed as safety system. There are data communication links between IFPDs and ESCMs. The safety benefit of these communication links has been evaluated in this paper.

2. HSI design for safety component control

The IFPD provide various operator supporting functions such as system mimic display, computerized procedure system (CPS) and alarm system. Operator uses IFPD as primary operational means during normal, abnormal, and emergency operation. When operator control safety component, operator uses IFPD and ESCM.

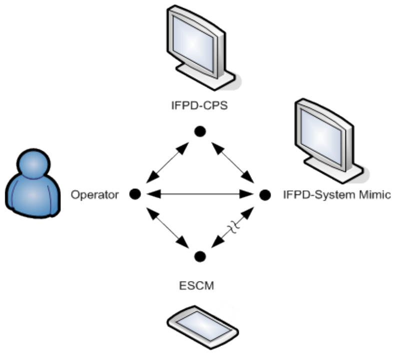

Fig. 1. The interaction between operator and HSI

Fig. 1 shows the interaction between operator and HSI. When operator selects a safety component in a IFPD, the identification signal for the safety component (Component ID) is delivered from IFPD to corresponding ESCM. Then the ESCM provide the soft control page for the component. This data communication link from IFPD to ESCM helps operator to call soft control page in ESCM. If there is no link between IFPD and ESCM, operator should call the soft control page in ESCM by using ESCM display navigation menu. It means that the operator should navigate the ESCM display from starting page to selected soft control page according to the display hierarchy in ESCM. The safety benefit of the data communication from IFPD to ESCM has been evaluated with comparing operation without the data communication from IFPD to ESCM.

3. Sequence of operation for safety component control

For the safety benefit evaluation, sequence of operation is modeled with sequence diagram in united modeling language (UML). The sequence diagram is one of interaction diagram which focuses on the message interchange between a numbers of lifeline [2]. Each lifeline represents the operator and HSI system events.

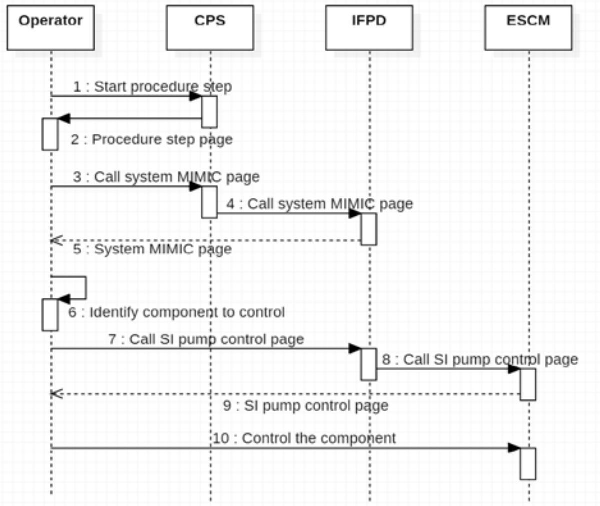
Operator
CPS
IFPD
ESCM
1 : Start procedure step
2 : Procedure step page
3 : Call system MIMIC page
4 : Call system MIMIC page
5 : System MIMIC page
6 : Identify component to control
7 : Call SI pump control page
8 : Call SI pump control page
9 : SI pump control page
10 : Control the component

Fig. 2. Sequence diagram of a component control with link between IFPD and ESCM

Fig. 2 shows the sequence diagram of a component control with link between IFPD and ESCM. Operator uses CPS for the procedure execution. During the step execution in the procedure, operator needs to control a component. Each step displayed in CPS provides link to the system mimic page. Operator calls the system mimic for the component by using the links in the CPS page. and system mimic page is provided at an adjacent IFPD. When operator selects the component in system mimic page, then IFPD send signal to ESCM, and ESCM provides soft control page. Fig. 3 shows the sequence diagram of component control without link between IFPD and ESCM. The sequence for the CPS is same with Fig. 2 but operator do not use IFPD to call soft control page. Operator need to memorize the Component ID in his/her short term memory and navigate ESCM display according to his/her long term memory of ESCM display hierarchy. This increase operator mental workload and there is potential of error to select wrong component.

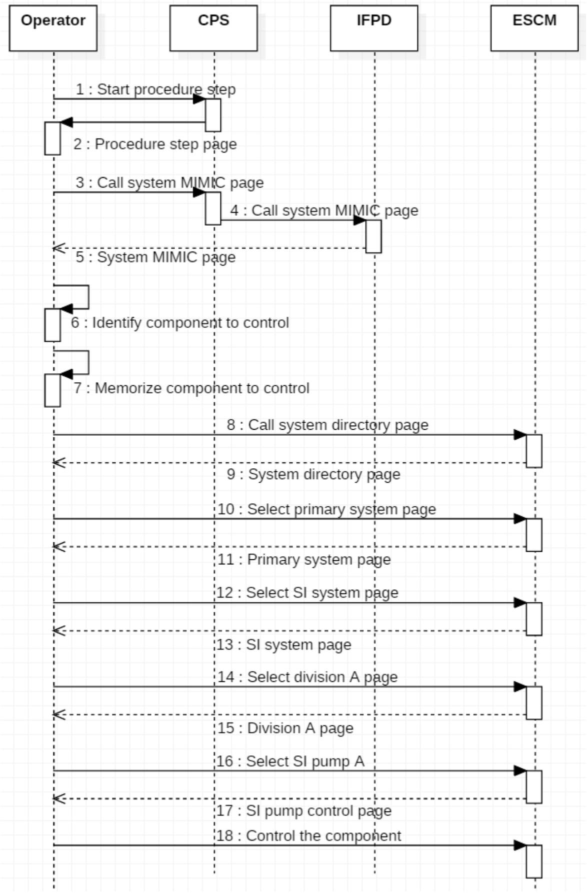
Operator
CPS
IFPD
ESCM
1 : Start procedure step
2 : Procedure step page
3 : Call system MIMIC page
4 : Call system MIMIC page
5 : System MIMIC page
6 : Identify component to control
7 : Memorize component to control
8 : Call system directory page
9 : System directory page
10 : Select primary system page
11 : Primary system page
12 : Select SI system page
13 : SI system page
14 : Select division A page
15 : Division A page
16 : Select SI pump A
17 : SI pump control page
18 : Control the component

Fig. 3. Sequence diagram of a component control without link between IFPD and ESCM

4. Evaluation of safety benefits of communication between IFPD and ESCM

Table 1 shows the numbers of operator action and ESCM processing for the modeling. When there is link between IFPD and ESCM, only one operator action is needed to call soft control page. If there is no link between IFPD and ESCM, then maximum six operator actions are required for the navigation. One other noticeable benefit of IFPD-ESCM link is reduced ESCM processing times to display a page. Therefore, required time for operator control action is reduced and it allows more time margin for operator actions. Also operator's mental workload will increase to memorize the component identification and to use the knowledge of ESCM navigation menu hierarchy.

Table1. Time based workload analysis result for the sample scenario

Number of	Without link between IFPD and ESCM (from identification to control page)	With link between IFPD and ESCM (from identification to control page)
Operator actions	6	1
ESCM processing	5	1

5. Evaluation of safety loss of communication between IFPD and ESCM

For the evaluation of safety loss of communication link, the requirements of DI&C-ISG-04 are reviewed, which is interim staff guideline for highly-integrated control rooms-communications issues by U.S. NRC [4]. DI&C-ISG-04 requires that the communication faults should not adversely affect the performance of required safety functions in any way. Also it provides examples of credible communication faults caused by such as message corruption, repeat, lost, delay, high rate and so on. ESCM only receives the Component ID from IFPD for the soft control page display, therefore the worst communication fault of ESCM may 1) display wrong soft control page or 2) out-of-service of ESCM by such as data storming.

For the first failure case, ESCM does not generate any control command before operator generates the command action. If operator fails to notice about wrong component selection display, he may take one commission error. But immediate feedback check by a procedure or co-worker will rend him to take a subsequent recovery or repair action.

For the second failure case, ESCM will be stuck and operator notices that ESCM does not working. Operator will stop any command trial for this failure case.

From these failure analyses, there is no significant affect to the safety functions in both cases.

6. Summary

The safety benefits evaluation of data communication link between IFPD and ESCM are provided. The evaluation shows that the safety loss is considered as small enough to trade off the safety benefit of the operator supporting.

REFERENCES

[1] IEEE Std 603-1991, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

[2] OMG Unified Modeling Language Specification Version 2.5

[3] NUREG-0711, Revision 3, "Human Factors Engineering Program Review Model," US NRC, November 2012.

[4] ISG -04 Rev 1, Highly –Integrated Control Rooms – Communication Issues, US. NRC, March 2009.