*Transactions of the Korean Nuclear Society Virtual Autumn Meeting*
*October 21-22, 2021*

# Framework of Safety Display System Design in Nuclear Power Plant

Su Ho Kim, Ji Hyeon Kim, Ki Hoon Jung
I&C System Engineering Department, KEPCO-E&C, Daejeon, Korea

## INTRODUCTION

Application software for a digital safety I&C system for the Nuclear Power Plant consists of two major parts, safety functional logic and Human Machine Interface(HMI). Up to now, there has been applying different safety level for these two parts, i.e., SIL 4 (Safety Integrity Level 4)[3] for functional logic and SIL 3 for HMI. However, there is a possibility that safety requirements for the I&C systems will become stricter.

Recent regulatory positions require to apply the SIL 4 to Type A variable display based on RG 1.94 (rev.4). For now, SIL 4 requirements are just for Type A variable but based on the movements of regulation authority so far, there is a chance to applying strict requirements on whole HMI system becomes mandatory in the near future. As a result, it is necessary to prepare meeting the SIL 4 requirement for both functional logic and HMI, by developing a safety critical grade display system [1].

As an effort to improve the safety of nuclear power plants (NPPs) and to respond to the recent regulatory positions, KEPCO-E&C has been developing the safety display system, which is named, Nuclear Safety display(NUSAY). NUSAY is developed to meet two requirements to satisfy the SIL 4 grade. First, both SIL 4 certified hardware platform and system software should be available. Second, the developed application software needs to be verified and validated in accordance with the SIL 4 requirements.

Two sequential phases of research have been performed to develop the NUSAY. In the first phase, two(2) methodologies of using/unusing Open GL were considered. Among them, a method without Open GL was selected and confirmed the applicability for NUSAY. It is now in the second phase to perform detail design which includes developing the graphic library and user interface with the safety features. This paper presents the design of the developed prototype NUSAY that applies a polling method for display, as well as its capability and limitation.

## DESCRIPTION ON NUSAY

NUSAY is a nuclear safety display system. Study for developing a safety grade display system has been made [1]. Various methodologies have been proposed and a first prototype of NUSAY has been developed by adopting a methodology of using power PC. The developed prototype NUSAY is configured in four layers; Hardware, Operating System(OS), Graphic Library and Application. Hardware and OS are distinguished as hardware design and the others, Graphic Library and Application, are Software Design. This structure is illustrated in Fig. 1.

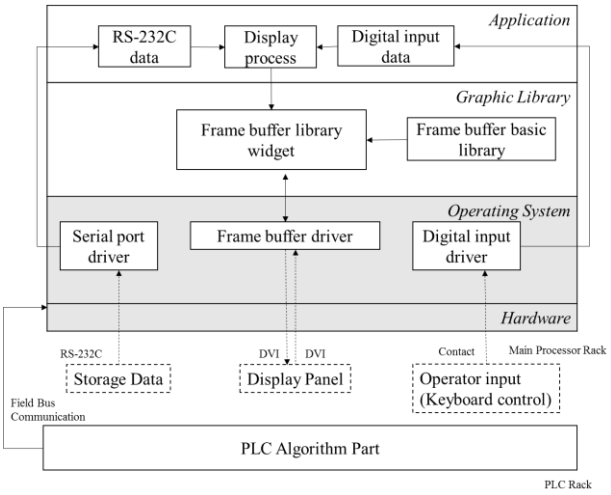


*Fig. 1 NUSAY structure*

### Hardware and System Software

NUSAY is designed based on MEN's D602 board power personal computer. The D602 board uses a triple CPU and triple main memory to ensure the safety and reliability of the processor board. The tripled CPU supports lockstep with triple modular redundancy. This makes system fault-tolerant and gives system high ability to monitor and correct errors. The P505 board is used as a graphic support card for graphic display, and Compact PCI is used as a backplane bus. The system software applied to NUSAY is based on the real time operating system that is certified as DO178B Level A for aerospace industry.

### Graphic Library

NUSAY has an independently established graphics library which is based on frame buffer concept, and the frame buffer mentioned here refers to the memory map function for display. It is simpler than the graphics library used in general embedded systems such as OpenGL. The frame buffer library has functions such as graphic operation, screen processing

system, resource management, image loading, and font rendering. Such functions will eliminate using of GPU resource to make ease of getting SIL 4 safety grade.

Conceptually, the graphic library has three layers: Low level, Middle level, High Level. Each layer is designed to support the higher level.

Low level is a Frame buffer driver which controls the visual display. Low level is the most basic step, which corresponds with the Frame buffer. The Frame buffer driver directly controls hardware management information and hardware frame buffers. The frame buffer is mapped to a memory area on the system and stores the desired value in the memory, and the graphic controller outputs the information to the connected display panel. Though display driver is a part of graphic library, it is physically located in OS (as described in Fig. 1) to do its job.

Middle level is a Frame buffer basic library which supports drawing line, filling, polygon, circle and etc. It is able to set the color property of the specified pixel or check the current setting value as the basic library. Vertical lines (x, y, y, color), horizontal lines (x, y, x, color), polygon, and circle are provided to display. In addition, it can provide functions such as filling, line thickness, font rendering, image processing, and the like.

High level is an application software widget package which includes various API. An extended widget for processing user input and display of buttons, input boxes, group border boxes and the like is provided. Font processing for character display on the screen is also included.

## Application software

Display software can be divided into RS232C communication module, display processing module and digital input processing module. The display processing module draws the display picture so that the operator input and the stored data are displayed on the screen. Operator input comes from digital input processing module and the stored data input comes from RS232C. Fig. 2 illustrates the flow chart of the NUSAY display processing. Initially, display processing performs initialization. The next step is to read the stored data. The stored data are constant values used in PLC algorithms or display processing. Next, it reads the digital input and executes the display process and decides whether the command from the digital input needs to read storage data. If it needs to read the data, it goes to second step to read storage data. Otherwise, the display data is made in frame buffer to send the display data to the display panel through DVI cable. While the display panel displays the data and in the same time it gives display process module a frame buffer feedback which has been received through the DVI cable. The display panel compares the sent and received frame buffers and alerts fail by blinking when they are different; otherwise, it moves to read digital input step and continues to run the display processing. These series of processes will ensure the integrity of display panel.

The application software executes Man Machine Interface functions for the safety functional logics. It also controls the overall layout display by updating and processing the data. NUSAY can provide GUI based framework to make display design easily. Application software for NUSAY will be coded under strict coding rules which come from variety of industry standard especially of Europe, United States and Korea. These rules are listed up from IEC 61508 [4], NUREG/CR-6463, and RS-015 Cyber Security.

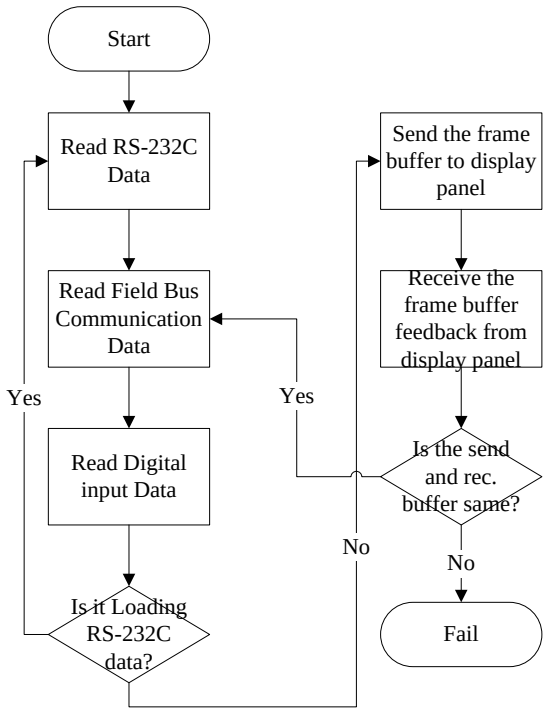


*Fig. 2 NUSAY displaying flow chart*

## Limitation

NUSAY has limitations in using hardware input/output devices such as keyboards and touch screens. SIL-4 level development and verification is difficult for I/O hardware drivers such as keyboards and touchscreens. These drivers run by interrupting the operating system. Safety critical (i.e., SIL-4) does not permit external interrupts in CPU board except the timer interrupt [2], therefore, these cannot be used as SIL-4 software. To compensate for these limitations, hardware inputs are deterministically received using a digital input module. Controls for page movement and data entry are made through a digital input module. However, when a keyboard input is received as a digital input signal, various

combinations of inputs must be considered. The keyboard input can be complicated by numerous combinations. Conversely, if you limit it to a simple input combination, operator control becomes complicated and difficult. The problem is finding the appropriate control interface configuration. This limit should be eliminated by improving or fixing OS and to do this, frequent communication with OS vendor is critical.

**Applicability**

Plants in Korea which are in operation, has a possibility of equipment replacement due to the obsolescence or discontinuance of equipment or component of it. In this case, licensing authority could require high safety features to make public credit the safety of nuclear power plant. At this point, NUSAY can be applied to satisfy requirements and expectations of the authority. Furthermore, nuclear plants with NUSAY can get more competitiveness than other nations' plant when exporting to overseas.

## CONCLUSION

Primary goal of the KEPCO E&C's NUSAY project is to provide a safety grade operator information display system. This paper presents and analyzes the NUSAY; hardware, new operation system (i.e., RTNOS), graphics library using frame buffers and an application program for display processing. Also, I/O handling and frame buffer graphic library problems have been identified while developing NUSAY. It is also suggested that NUSAY platform can be used for safety functional logics instead of safety grade PLC.

This paper introduces the improved design based on several facts that have been derived from implementing the prototype. Nevertheless, there are still a few engineering obstacles and efforts is being made to overcome them.

## REFERENCES

1. J.H.Kim and et al., *Development Methodologies for a Nuclear Safety Display System*, 36th Annual Conference of the Canadian Nuclear Society and 40th Annual CNS/CNA Student Conference, Toronto, ON, Canada (2016).
2. IEC 60880, *Nuclear power plants - Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions* (2009).
3. IEEE 1012, *IEEE Standard for Software Verification and Validation* (1998).
4. IEC 61508, *Functional Safety of electrical/electronic/programmable electronic safety-related systems (2010)*.