Improving the Operation of the Radiation Monitoring System (RMS) in KOMAC

*Jeong-Min Park, Yi-Sub Min
Korea Multi-purpose Accelerator Complex, Korea Atomic Energy Research Institute
**Corresponding author: jmpark027@kaeri.re.kr*

1. Introduction

Korea Multi-Purpose Accelerator Complex (KOMAC) started operating the proton accelerator in the second half of 2013. And by introducing Radiation monitoring system (RMS), the radiation/radio-activity produced in the facility and in its surrounding environment is constantly monitored. They are included the software which is integrated the information and monitors the status of each component by using a serial communication (RS485). In the existing RMS, information on the detector installed at the time of 2013 is reflected and when modifying or adding the device information, the administrator must directly access the database (DB) and make modification. In this case, the commands of the protocols for each function are complex and difficult to understand and by entering a typo or incorrect information, it can affect the entire system. Figure 1. Shown as the schematic diagram of RMS. As the operating period elapsed of the RMS and the existing detectors are discontinued and obsolete, a new model or other manufacturer's product must be installed. The existing RMS's integral software has a problem in that it is difficult to compatibility between the new detector and the RMS main server (the integral software). Because, in order to receive information such as a dose rate, alarm, or event status from the detector, predetermined communication information between the detector and the server is required, and this information may be different for each manufacturer or type of detector. However, such communication command packet is ultimately determined within the range of a specific structure. [1] Therefore, it was improved so that the new communication structure could be reflected in the RMS server by identifying the communication command packet for each detector and supplementing the data packet processing. Through this, the limitations on the introduction of detectors from other manufacturers and models were overcome, and the operational effectiveness of the RMS system was improved.

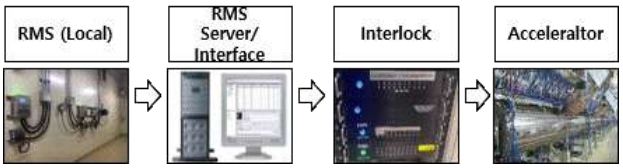

Fig. 1. Schematic diagram of RMS operation

2. Methods

The existing RMS reflects only the information on the devices installed at the time of establishment, and change to the information of the detector, the database (DB) must be modified. However, there is a disadvantage in that human errors such as typos can occur during the process of modifying the DB. In addition, the range for selecting a detector is limited due to the limitation of compatibility between the RMS's integral software and the detector. As the operating period of the detector passes, it becomes obsolete or the model is discontinued and needs to be replaced with a new model or a product from another manufacturer. Therefore, the RMS's software has been improved to overcome the limitations on the installation of new detectors. The main improvement is the communication data structure of the software, and detailed improvements include interlock setting and add/delete of monitors, data integrity assurance, other product protocol additions, and access authority setting for each user group. Figure 2. Shows the improved user interface screen.

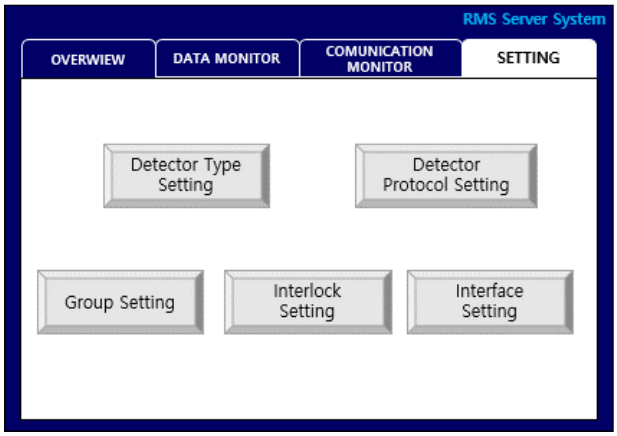

Fig. 2. User Interface Screen

2.1 Interlock Setting and Detector add/delete

In the existing RMS's program, the interlock device ID concerned about ALARM was fixedly set in the RMS server program. The improved integral software has a user interface that can change it.

Through the user interface, detectors can be added or modified and when there is a change in the detector information, it can be easily changed on the interface screen without modifying it through the database (DB). In addition, when detailed information such as detector type, name, and monitoring channel, data

communication protocol and etc. is entered and saved in the interface menu, new detector information is registered and reflected in the system UI.

2.2 Ensuring Data Integrity.

When the detector information is modified or deleted, the database (DB) should not be lost. So, if a detector is selected and deleted from the setting menu of the user interface, it is made inactive. The inactive detector disappears only from the UI, and data integrity can be secured because the detector information is all stored in the DB. Also, a detector that has disappeared from the screen can be accessed and activated in the same way.

2.3 Reflection of Other Detector Protocols

In order to receive information such as dose rate, alarm, and other events from the detector in RMS, predetermined communication protocol between the detector and the RMS's software is required. At the beginning of system operation, the detector model was not diverse, and the communication protocol was operated by inputting information only about the old model. However, as the old model was discontinued and the introduction of a new model became necessary, through system improvement, it is possible to modify and add protocol information such as data acquisition, alarm setting, and unit factor change in the user interface. Also the changed protocol is automatically saved in the DB, and necessary information can be called from the DB in the user interface. In other words, since protocols for detectors of other manufacturers or other models can be input in the user interface and reflected in the system, various types of detectors can be monitored in connection with the RMS.

2.4 Setting Access Authority for Each Group

The RMS manage detectors by grouping them according to the monitoring subject or purpose. In the existing system, the user checked the dose information or status value through the interface screen including the entire group. However, it is difficult to check the dose information for the interested area figure out the interface screen including the entire group. Therefore, the system was improved so that only the detector group in the interested area could be selected and viewed in the UI by setting the access authority for each detector group. Through this, RMS users can receive only the necessary detector information on the UI screen, so user convenience was improved such as figure 3.

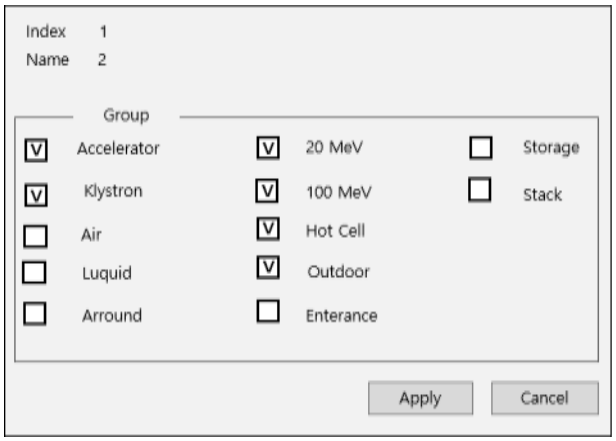

Fig. 3. Detector group selection screen

3. Conclusions

The RMS of KOAMC, established in 2013 and operating until now, reflected only the information on the detectors installed at the time. However, as the old model was discontinued and the introduction of various types of detectors became necessary, the existing system was improved. As an improvement, the existing communication structure was supplemented for compatibility with the RMS server and various types of detectors. In detail, the functions of setting interlock, adding/deleting detectors, securing data integrity, adding other detector protocols, and setting access authority for each group were added. As a result of system improvement, restrictions on introducing other types of detectors were eliminated and through this, various types of detectors could be connected to the RMS server and monitored. In addition, user convenience was improved as only monitoring information about the interested area can be checked through the UI screen.

REFERENCES

[1 Yi-Sub Min, Jeong-Min Park, C.W.Lim, The Development of the data processing device for RMS redundancy in KOMAC, Korea Multipurpose Accelerator Complex, Korea Atomic Energy Research Institute, 2021.