A Study on Evaluation Issues of Real-Time Operating System in Nuclear Power Plants

Y. M. Kim, C. H. Jeong, J. S. Koh
Regulatory Research Division, Korea Institute of Nuclear Safety
ymkim@kins.re.kr

1. Introduction

Control applications such as aircraft, robotics and nuclear power plant have to maintain a very high level of safety, typically defined as the avoidance of unplanned events resulting in hazard. These applications usually operate with hard real-time operating system (RTOS). In this case, hard RTOS software should be reliable and safe. RTOS used in safety-critical I&C system is the base software for the purpose of satisfying the real-time constraints. So, careful evaluation of its safety and functionality is very important.

In this paper, we present the case study for RTOSs used in real nuclear power plants (NPP), and suggest the evaluation approach for the RTOS.

2. Hard Real-time Operating System

Hard RTOS must achieve a timely execution of hard real-time tasks. Hard RTOS must have several characteristics for correctness action such as timing constraints, resource constraints, precedence constraints, concurrency constraints, communication requirements, placement constraint, and criticalness. In order to support these constraints, hard RTOS must have high performance, predictability, reliability and adaptability [1].

There are several commercial hard RTOSs such as VRTX, QNX, REAL/IX and LynxOS. An RTOS named pCOS is now being developed for Korea Nuclear I&C System (KNICS) under the control of the government.

3. RTOS in Nuclear Power Plants

From Ulchin 5&6 nuclear power plant, PLC based digital systems have been adapted for safety I&C system. The PLC consists of various I&C logics in software including real-time operating system (RTOS). In this chapter, we review RTOSs which have been using or will be used in Korea NPP.

3.1. VRTX

For DPPS, DESFAS-AC, CPCS of Ulchin 5&6, Shin Kori 1&2, Shin Wolsong 1&2, Advant Controller 160(AC160) Common Qualified Platform was adapted. The AC160 software consists of a real-time operating system VRTX, task scheduler, diagnostic functions, communication interfaces, and user application programs, all of which reside on flash PROM in the PM646A processor module. The VRTX operating system executes the control units of the application program, diagnostics routines and communication interfaces. Westinghouse submitted commercial grade dedication report which contains the methods, requirements and results for the commercial grade dedication of the base system software which contains VRTX that is supplied for use in the AC160 PM646A processor, for use in nuclear plant protection systems [2]. Figure 1 shows the AC160 Software Configuration Block Diagram [4].

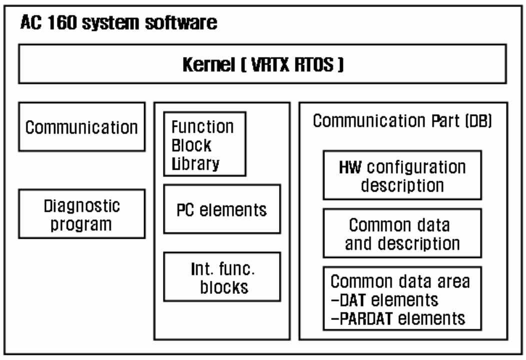

Figure 1 AC160 Software Configuration Block Diagram

3.2. QNX

The operating system for CPCS MTP (Maintenance and Test Panel) of Shin Kori 1&2 is QNX. There is one MTP in each CPC/CEAC channel, implemented using a Flat Panel Display System identical to that of the Operator's Module. The MTP is local to the CPC processors and is the primary man-machine interface for routine maintenance and surveillance testing by plant technicians. In Shin Kori 1&2, MTP software was designed with ITS (Important To Safety) grade software. Westinghouse executed QNX commercial grade dedication process according to EPRI-TR 106439[3].

The core of the QNX operating system consists of several critical modules: the kernel and a group of cooperating processes, one of which is the Process Manager. The kernel is responsible for message passing among processes and scheduling (whenever a process changes state as a result of a message or interrupt). A typical QNX operating system configuration would include additional modules such as a network manager;

file system manager and/or serial device manager as Figure 2.

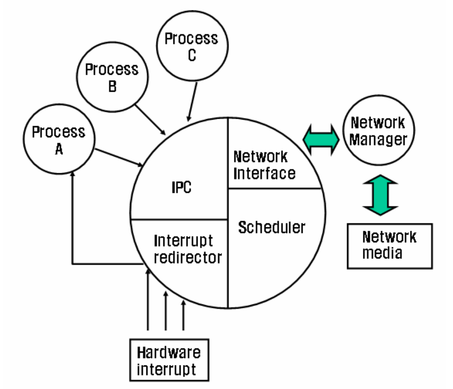

Figure 2 QNX Operating System Overview

3.3. RTOS in KNICS (Korea Nuclear I&C System)

RTOS embedded in safety grade PLC has been developed by KNICS project. Figure 3 shows the design objects of RTOS for process module. The operating system of process module consists of Kernel, other external devices and system tasks [5].

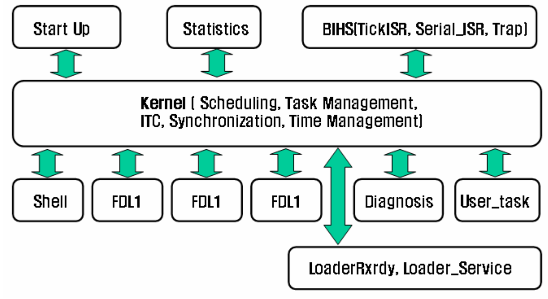
Start Up
Statistics
BIHS(TickISR, Serial_ISR, Trap)
Kernel (Scheduling, Task Management, ITC, Synchronization, Time Management)
Shell
FDL1
FDL1
FDL1
Diagnosis
User_task
LoaderRxrdy, Loader_Service

Figure 3 Design Objects of RTOS for Process Module

4. Evaluation Issues of RTOS

For the evaluation of Commercial off-the-shelf RTOSs and other specific RTOS developed for specific PLC like pCOS for nuclear I&C system, the research about assessment guidelines is now under study.

We classified evaluation items into scheduling, memory management, timing and security. The RTOS must support multi-tasking and task synchronization. And resolution methods about the priority inversion and deadlock problem must be presented very clearly. Also, the timing must be deterministic and correct memory management policy must be implemented and counter measures against the virus intrusion must be existed.

The Following results are some of the evaluation items from our study.

Classification	Evaluation Items
Scheduling	Is supporting the multi-tasking and task synchronization? Is providing the execution of processes based on priority? Is there the preemption function?
	How is the priority inversion prevented and/or resolved? How is the deadlock prevented and/or resolved?
Memory Management	What is happened when a memory partition assignment fails? Can it be prevented?
	Is there any method about the stack overflow prevention and resolution?
Timing	Are there any critical timing sections? If so, how is the timing ensured? What happens if the timing is off?
	Is the timing deterministic and predictable?
	What is happen when the WDT fails?
	What is happen when the kernel fails in the presence of built-in heart beat?
Security	Can an unauthorized person access to OS kernel?
	Can unauthorized changes be made to software?
	Is there any plan about virus intrusion?

5. Conclusion

A hard RTOS used in safety-critical I&C systems must guarantee deadlines of tasks in a worst case scenario. Also, a hard RTOS used in the nuclear power plant must satisfy severe performance requirements even in a worst case scenario. In this paper, we surveyed commercial RTOS which was embedded in PLC of Nuclear I&C systems and RTOS which is under development with the object of using nuclear I&C system. Also, we suggested the evaluation issues of the RTOS for nuclear power plant. Future, we will develop more detailed assessment guidelines in order to review various ROTS effectively.

REFERENCES

[1] A Study on the Hard Real-Time Operating System Kernel, J. H. Park, H. G. Lee, KISS, 1994
[2] Commercial Grade Dedication Report the ABB ADVANT PM646A Firmware/Base System Software Version 1.3/4 for COMMON Q Applications, 00000-ICE-37618, Rev0, 2003
[3] Commercial Dedication Report for QNX 4.25G for Common Q Applications, WNA-CD-00018-GEN, Rev.00, 2004
[4] COMMON QUALIFIED PLATFORM TOPICAL REPORT, CENPD-396-P, Rev. 01, 2000.
[5] KNICS-PLC-SDS331-01, Rev0