설계명세서를 이용한 안전등급 PLC 운영체제 컴포넌트 시험방법

이영준[0], 성아영*, 최병주*, 손한성
한국원자력연구소, *이화여대, ㈜에네시스
yjlee426@kaeri.re.kr, aysung@ewhain.net, bjchoi@ewha.ac.kr, hsson@enesys.com

Component Testing Methodology of Operating System for Safety-Grade Programmable Logic Controller with Design Specification

Young-Jun Lee[0], Ah-Young Sung, Byoungju Choi, Han-Seong Son
Korea Atomic Energy Research Institute, EnEsys Cop.

요 약

본 논문은 안전등급 제어기기(Safety-Grade Programmable Logic Controller)에서 사용하는 프로세서모듈 운영체제에 대한 컴포넌트 시험에 대해 기술한다. 디지털 소프트웨어에 대한 NRC(Nuclear Regulatory Commission)의 지침에 따라 운영체제는 소프트웨어 생명주기에 따라 개발되고 있으며 요구사항과 설계명세, 그리고 구현코드를 가지고 다양한 시험을 수행하고 있다. 컴포넌트 시험은 구현된 코드가 테스트 커버리지를 만족하는 지 파악하는 시험이다. 이를 위해 설계명세서를 참조하여 시험대상을 구분하고 각각의 시험대상에 대한 시험항목을 세분화한 이후 시험방법과 절차, 그리고 시험환경을 구축한 후 컴포넌트 시험을 수행한다.

1. 서론

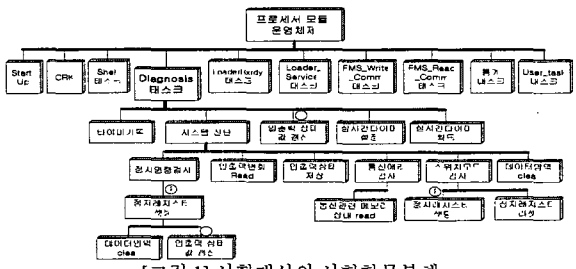
POSAFE-Q 는 원자력발전소 안전관련 계통에 적용하기 위해 모든 하드웨어 및 소프트웨어를 원전 안전등급기준에 따라 새롭게 개발하는 제어기기(Safety-Grade Programmable Logic Controller)이다. 또한 POSAFE-Q 를 운영하기 위한 프로세서모듈 운영체제가 개발되고 있다. POSAFE-Q 는 KNICS(Korea Nuclear Instrumentation and Control Systems) 과제에 의해 개발되고 있고 KNICS 는 과거 아날로그로 개발되던 계측 제어 시스템을 디지털 시스템으로 바꾸는 과제이다.

프로세서모듈 운영체제는 미국 NRC(Nuclear Regulatory Commission)의 Regulatory Guide(이하 Reg. Guide)1.173[1]에서 승인하고 있는 IEEE. Std 1074[2]를 따라 소프트웨어 공학의 폭포수 모델과 나선형 모델을 혼합하여 개발되고 있으며 운영체제에 대한 기능과 성능을 보장하기 위해서 다양한 테스트를 수행하고 있다. 요구사항을 기반으로 하는 시스템시험과 설계명세를 기반으로 하는 소프트웨어 및 하드웨어의 통합시험, 그리고 구현코드 및 설계명세 일부를 가지고 컴포넌트 단위시험 등을 수행하고 있다.

본 논문은 POSAFE-Q 프로세서모듈 운영체제의 컴포넌트 시험에 대해 기술한다. 컴포넌트 시험을 위한 시험대상 분류방법과 절차, 그리고 시험환경에 대해서 기술한다

2. 컴포넌트 시험대상

POSAFE-Q 프로세서모듈 운영체제의 시험대상을 결정하기 위해서는 프로세서모듈 운영체제 소프트웨어의 설계명세서[3]를 참조한다. 설계명세서의 모듈분해 장에서 운영체제의 커널과 시스템 태스크들의 기능을 분류해 놓았기 때문이다. 구현된 코드만을 가지고 시험대상을 분류하는 것은 거의 불가능하다. 각각의 시험 항목에 ID를 부여하고 실제 구현된 코드에서 해당하는 함수들을 찾아내어 시험의 최소단위로 결정한다.
[그림1]은 시험대상의 시험항목을 결정하기 위한 기능분해의 예이다.



[그림 1] 시험대상의 시험항목분해

2.1 커널 시험대상

커널은 운영체제의 핵심을 담당하고 있다. 시스템 태스크와 사용자 태스크를 동작시키고 필요한 자원에 대한 할당을 해주며 운영체제의 동작을 제어하게 된다. 커널의 기능을 논리적으로 분류하면 스케줄러, 시간관리, ITC및 동기화, 태스크관리, BIHS(Basic Interrupt Handler System)와 같이 구분된다. 이러한 논리적인 기능을 더욱 세분화하여 시험대상으로 삼고 각각 ID를 부여한다.

2.2 시스템 태스크 시험대상

시스템 태스크는 POSAFE-Q를 구성하고 있는 통신모듈, 입출력모듈, 개발도구, 기타 하드웨어와의 인터페이스 기능을 수행하고, 운영체제에 대한 초기화 및 특정기능을 수행하는 태스크들이다. 시스템 태스크가 수행하는 기능을 간단히 살펴보면 운영체제와 하드웨어장치에 대한 초기화, POSAFE-Q 시스템의 상태표시 및 자가진단, 응용프로그램의 작성 및 사용자 환경설정을 수행하는 통합개발도구와의 통신, 그리고 통신장치들과의 인터페이스 등이다. 이러한 태스크들 역시 그 기능을 세분화해서 시험대상으로 삼고 각각 ID를 부여한다.

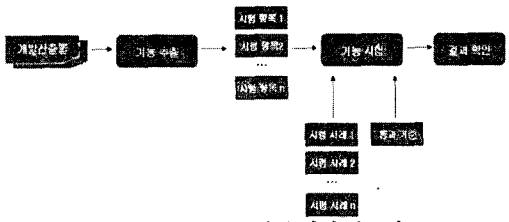
[표 1] 시험대상과 ID

S-TI-1-01	init_global_var cpu_init loader_init init_task_man force_mem_clear	시스템 초기화
중략		
S-TI-3-01	check_stop_command check_id_config check_switch	주기적으로 IO와 Profibus 통신, 스위치장치 등을 확인 및 진단
중략		
S-TI-5-13	xmit_datamonitor xmit_memory_sect_upload	pSET으로 데이터에 대한 upload
S-TI-6-01	FMS_Write_Comm()	헤더와 데이터값을 FMS 공유메모리에 저장

3. 컴포넌트 시험방법

3.1 커널 시험

POSAFE-Q 프로세서모듈 운영체제의 커널을 시험하기 위해서는 설계 명세서에 기술된 커널의 기능이 정확히 수행되는지 확인한다. [그림 2]과 같이 개발 산출물로부터 커널의 기능을 파악하고 각 기능을 시험하기 위한 시험 사례인 입력과 출력을 정의한다. 커널의 기능 및 시험 사례를 설계한 후에 실제 운영체제를 동작시키면서 명시된 기능이 만족되는지를 확인한다.



[그림 2] 커널 시험 접근법

3.2 시스템 태스크 시험

POSAFE-Q 프로세서모듈 운영체제의 시스템 태스크는 다른 장치와 인터페이스 기능을 수행하는 태스크이다. 이러한 컴포넌트는 대부분 입력 값이나 전역변수 값에 따라서 조건에 부합되는 연산을 수행한 후 그 결과를 상위 컴포넌트에 전달하는 기능을 수행한다. 따라서 이러한 특성을 갖고 있는 컴포넌트들은 화이트박스시험을 수행한다.

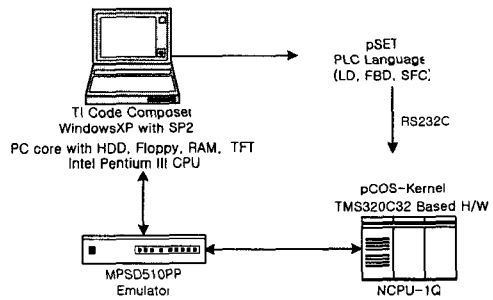
시스템 태스크에 적용한 화이트 박스 시험 기준은 Branch Coverage 이다. Branch Coverage 는 실행된 분기문의 비율을 측정하며, 측정 식은 다음과 같다.

- Branch Coverage = 실행된 분기문의 수 / 전체 분기문의 수

시스템 태스크의 시험 접근법도 [그림2]와 유사하다. 그러나 시스템 태스크를 구현하기 위해 일부 사용한 Inline Assembly 영역은 시험에 고려하지 않거나 단순히 특정변수의 값에 변화가 발생했는지 살펴본다. 시험에 사용된 사례들이 커버리지를 만족하는지 파악하기 위해서 커버리지 분석도구를 사용한다.

4. 시험 장비 구성

POSAFE-Q 프로세서모듈 운영체제의 컴포넌트 시험에 사용된 시험구성은 [그림3] 와 같다. Host와 Target 시스템 사이에 에뮬레이터를 연결하여 시험을 위한 환경을 제공한다.



[그림 3] 컴포넌트 시험구성

일반적으로 대상 시스템의 소프트웨어를 시험하기 위해서는 소프트웨어 자원과 하드웨어 자원이 필요하다. POSAFE-Q 프로세서모듈 운영체제를 시험하기 위해 필요한 소프트웨어는 Windows XP, Code Composer, MPSD510PP Driver, pSET(POSAFE-Q Software engineering Tool) 등이다. Code Composer 는 운영체제를 컴파일하고, 생성된 실행파일을 POSAFE-Q의 프로세서모듈 장치에 다운로드 한다. 또한 동작 중 변수 값을 확인할 수 있는 디버깅 기능을 제공한다.

하드웨어 자원으로는 POSAFE-Q 의 프로세서모듈이 동작할 수 있는 버스모듈, 전원장치, 에뮬레이터, 프로세서모듈, 그리고 호스트영역에서 사용되는 Host PC 등이 있다.

5. 컴포넌트 시험절차

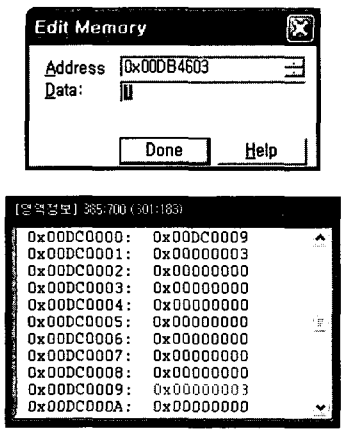
POSAFE-Q 프로세서모듈 운영체제의 컴포넌트를 시험을 위해 설계하여야 하는 시험 사례에 대한 예를 [표 2] 에서 보여준다. 시험사례를 설계하기 위해서는 입력에 대한 예상결과가 기술되어야 한다. 즉 컴포넌트의 입력

변수에 특정 값을 입력했을 때, 출력 변수들의 예상출력 값이 기술된다.

[표 2] 시험 사례 예

번호	입력변수	입력값	출력변수	예상출력값	결과값	P/F	비고
1	rx_text_ptr	7	FORCE_X_BASE (0xDC0000)	0xDA1000			
	rx_text[0]~rx_text[5]	0,0,1,0,0,0					
	force_num_x	0	FORCE_X_BASE+1 (0xDC0001)	1			
2	rx_tex_ptr	7	FORCE_Y_BASE	0xDA3000			
	rx_text[0]~rx_text[5]	0,0,3,0,0,0	FORCE_Y_BASE+1	1			
	force_num_y	0					
3	rx_text_ptr	7	0xDA5000	1			
	fc_temp	0x5000					

시험사례의 입력변수에 시험 값을 넣기 위해서 code composer 도구의 watch window 창을 이용하여 변수들의 목록을 보고 edit variable 화면을 이용하여 실제 입력 값을 입력한다. 또한 입력변수 중 실제 메모리에 값을 입력할 경우에는 memory edit 화면을 이용한다.



[그림 4] 변수 및 메모리 값 확인

시험 결과를 확인하기 위해서는 구현코드의 특정부분에서 운영체제의 동작을 일시 멈추고 확인하고자 하는 변수 값들을 살펴본다. 이러한 절차를 진행한 후 실제 결과와 예상결과를 확인하여 시험통과여부를 결정하게 된다.

6. 결론

POSAFE-Q 프로세모듈 운영체제의 컴포넌트 시험은 소스코드 수준에서 Branch Coverage를 만족할 수 있도록 수행하였다. 시험할 대상과 시험항목을 생성하기 위해서 설계명세서를 참조하였고 커버리지를 만족할 수 있는 시험사례를 추출하였다. 또한 이러한 시험사례의 입력 값과 출력 값에 대한 시험데이터를 도구를 통해 입력하고 시험환경에서 동작시킨 후 결과값을 도출하였다. 이러한 방법을 통해 POSAFE-Q 프로세서모듈 운영체제를 구성하고 있는 컴포넌트들이 정확하게 동작하고 있음을 확인할 수 있었고, 이상결과값에 대해서 구현코드를 수정하였고, 최적화를 통해 구현코드의 품질을 향상할 수 있게 되었다. 또한 예상된 결과값과 시험 결과값을 비교하여 컴포넌트들이 설계요건에 맞게 구현되어 있는 지 확인할 수 있다. 현재 통합시험을 통해 다른 장치와의 인터페이스가 정확히 이루어지고 있는 지 파악하고 있으며 그 결과를 토대로 컴포넌트 시험을 다시 수행하여 운영체제 소프트웨어의 기능을 최적화할 것이다.

참고문헌

[1] USNRC Reg. Guide 1.173, Development of Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plant, 1997

[2] IEEE Std. 1074-1997, Standard for Developing Software Life Cycle Processes

[3] POSCON, "안전등급 PLC(POSAFE-Q) 프로세서모듈 운영체제 소프트웨어 설계명세서" KNICS-PLC-SDS331-01

[4] USNRC Reg. Guide 1.152, Rev.01, Jan. 1996, "Criteria for Programmable Digital Computers System Software in Safety Related Systems of Nuclear Power Plants"

[5] IEEE Std. 7-4.3.2, 1993, "Standard Criteria for Digital Computers in Safety System of Nuclear Power Generating Stations"

[6] IEEE Std. 829-1998, "IEEE Standard for S/W Test Documentation"

[7] IEEE Std. 1008-1987, "IEEE Standard for Software Unit Testing"

[8] KAERI, "안전등급 PLC(POSAFE-Q) 프로세서모듈 운영체제 컴포넌트 시험계획서" KNICS-PLC-STG101-01

[9] KAERI, "안전등급 PLC(POSAFE-Q) 프로세서모듈 운영체제 컴포넌트 시험절차서" KNICS-PLC-STP151-01