HAZOP을 이용한 안전등급 제어기기 운영체제의 안전성분석

이영준[0] 권기춘 이장수 김장열 차경호 천세우
한국원자력연구소
{ex-yjlee426, kckwon, jslee, jykim, khcha, swcheon}@kaeri.re.kr

HAZOP-Based Safety Analysis of Operating System for Safety-Grade Programmable Logic Controller

Young-Jun Lee[0] Kee-Choon Kwon Jang-Soo Lee Jang-Yeol Kim
Kyung-Ho Cha Se-Woo Cheon, Han-Sung Son
Korea Atomic Energy Research Institute.

요 약

본 논문은 안전등급 제어기기(Programmable Logic Controller) 에서 동작하는 실시간 운영체제의 안전성을 요구사항 단계에서 평가할 수 있는 검토항목을 개발하고 HAZOP(Hazard and Operability) 을 이용하여 현재 개발중인 PLC 운영체제에 적용한 경험을 기술한다. HAZOP은 화학공장과 같은 산업에서 안전성을 평가하기 위한 방법으로 사용했던 방법론이다. 원자력발전소에 적용하기 위해 운영체제가 갖추어야 할 안전성 요건은 NUREG-0800의 BTP-14(Branch Technical Position)의 소프트웨어 기능특성 및 공정특성에 기술되어 있다. 이러한 기능적인 특성을 정확도, 신뢰성, 타이밍/사이징, 기능성, 강인성, 보안성 항목으로 나누고 세부적인 검토리스트를 만들어 HAZOP 을 적용하여 평가하였다.

1. 서론

원자력 계측제어 및 제어 시스템을 기존의 아날로그 시스템에서 디지털 시스템으로 업그레이드 하면서 내장된 소프트웨어의 안전성에 대한 확인이 필요하게 되었다[1]. 원자로 보호 계통은 원전에서도 최고 수준의 안전 필수 시스템이며, 모든 부문들이 독립적으로 기능을 수행할 수 있도록 구현된다. 원자로 보호 계통의 기능은 PLC를 기반으로 구현되어 있으며, 여기에는 독립적인 실시간 운영체제가 필요하다. 원전계측제어 시스템의 디지털화 추세에 따라 컴퓨터 소프트웨어의 안전성 확보를 인허가 기준으로 의무화하고 있다[2]. 실시간 운영체제의 안전성을 확보하기 위해서 BTP-14 에서 제공한 소프트웨어의 기능적 특성에 따라 운영체제가 갖추어야 할 특성들에 대한 검토리스트를 바탕으로 안전성 분석이 필요하다. 본 논문은 원자력 발전소에 사용하는 안전등급 제어기기(Safety-Grade Programmable Logic Controller) 운영체제의 안전성을 분석하기 위해 필요한 검토항목과 이를 바탕으로 HAZOP을 이용해 안전성 분석을 시도한 경험에 대해서 기술한다.

2. 관련연구

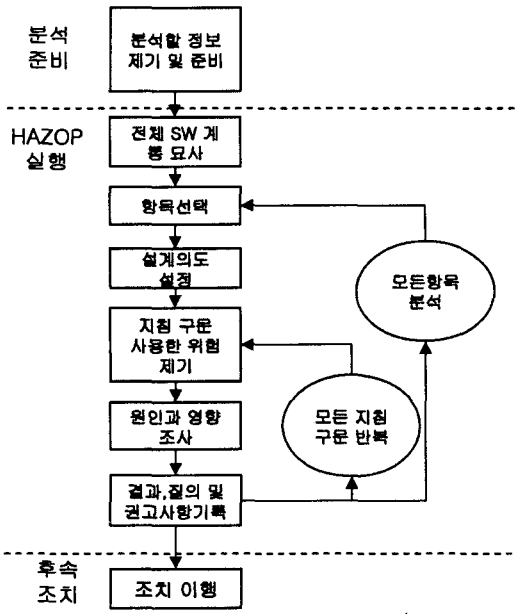
2.1 실시간 운영체제 요구사항

내장형 시스템을 동작시키는 실시간 운영체제 시스템은 기본적으로 결함 허용과 높은 가용성 특성을 제공해야 한다[3]. 이러한 특성은 운영체제 위에서 실행되는 어플리케이션의 모든 서비스를 신뢰할 수 있도록 한다. 프로세스기반의 운영체제들은 프로세스마다 서로 다른 메모리 영역을 사용하므로 프로세스간의 메모리 영역을 침범하지 않아 메모리간의 영역이 보호되었으나 일반적인 실시간 운영체제에서 사용하고 있는 태스크기반의 운영체제는 메모리를 공동으로 사용하여 운영체제와 어플리케이션을 같은 메모리공간에서 실행할 수 있도록 한다. 따라서 시스템의 안전성을 보장하기 위해서 실시간 운영체제는 하나의 주소공간에서 돌아가는 코드가 다른 공간에 접근하지 못하도록 하여야 한다.

2.2 안전성 분석 방법

소프트웨어 개발 공정 단계 중 요구사항 명세단계에서 안전성 분석을 수행하기 위한 HAZOP 방안이 있다. HAZOP은 Hazard and Operability의 약어로서 화학공장과 같은 산업에서 시스템 안전성 분석을 위해 사용하던 기법이다. 이 HAZOP 개념을 소프트웨어 요구사항 명세의 안전성 분석에 사용할 수 있고 이를 위한 분석절차가 개발되었다[4].
HAZOP에 의한 안전성 분석은 사고가 설계 또는 운용상에서 의도한 것에서 벗어났을 때 발생하는 것을 가정하고 설계에서 예상한 운용을 하였을 경우 일어날 수 있는 모든 가능한 일탈(Deviation)상황과 그와 관련된 위해 요소를 찾으려고 하는 것이다. 시스템을 구성하는 각 단위에 대하여 Guide Phrase를 사용하여 의도된 동작에서 일탈이 일어 났을 때, 발생 가능한 모든 위해도에 대하여 HAZOP 조직이

설계에 대한 의문을 제기하는 형식으로 체계적으로 수행된다



[그림1] 소프트웨어 HAZOP 절차

[표 1] HAZOP 조직

HAZOP 분석 책임자
시스템 요건 명세요원
소프트웨어 설계요원
두뇌 확인 및 검증요원
계통 안전성 분석요원
소프트웨어 안전성 분석요원
기록요원

3. PLC 운영체제의 안전성 평가항목

소프트웨어의 특성은 기능특성과 공정특성으로 분류된다. 기능특성은 소프트웨어가 실행해야만 하는 행동에 직접적으로 연관된 특성이고 공정특성은 소프트웨어가 요구된 행동을 실행하는 것을 보장하도록 하는 과정을 의미한다. 이러한 기능적인 특성들과 소프트웨어의 안전성 분석에 대한 지침인 NUREG-0800의 BTP-14 기준에 따라 검토리스트를 작성하고 각각의 특성들을 살펴볼 수 있다.

● **정확도**

운영체제의 커널이 정확하게 동작하는지를 파악하기 위해서 커널을 구성하고 있는 스케줄러, 메모리, 동기화에 대해서 평가한다. [표 2]는 정확도에 대한 검토리스트를 나타낸다. 언급한 구성요소들의 기능뿐 아니라 다른 구성요소의 기능도 역시 정확한 동작을 해야 하는 것은 사실이나 다른 구성요소들은 정확도가 아닌 다른 특성에서 다루고 있다.

[표 2] 정확도 안전성 평가항목

대상	Deviation Checklist	영향
스케줄러	태스크생성실패	시스템작동불가
	태스크우선순위동일	스케줄링불가
	태스크우선순위전도	응답시간지연
	태스크삭제실패	자원낭비
	삭제하려는 태스크가 아닌 다른 태스크가 삭제	부적당한 실행
	IDLE 태스크이상	제어기기 Halt, CPU 활용도측정불가
	태스크가 공유자원을 소유한 다른 태스크 삭제	태스크 Sequence 위반
	Deadlock 이 발생	무한대기
	Error Detection 및 핸들링을 불가	잘못된 연산수행
메모리	메모리"zero"	Overflow
	메모리파티션할당불가	TCB 생성불가능
	스택오버플로우 발생	시스템정지
동기화	기능을 상실한 태스크에 감시 태스크의 접근불가	태스크제어실패
	오류로인해 중단된 어플리케이션 재시작불가	수행데이터삭제

● **신뢰성**

신뢰성이란 어떤 소프트웨어 시스템이나 기기가 고장없이 동작하는 속성을 의미한다. 운영체제가 일관되게 사용되어 신뢰성을 달성하기 위해서는 어플리케이션과의 독립적인 운영이 필요하다.

[표 3] 신뢰성 안전성 평가항목

대상	Deviation Checklist	영향
신뢰성	어플리케이션이 커널내부 자료구조사용	Trap 에러
	어플리케이션이 위험한 결과를 가져올수 있는 모호한 포인터접근	시스템영역침범
	커널서비스도중 실패	수행자료삭제
	어플리케이션 파라미터 확인불가	

● **타이밍/사이징**

사용중인 계산시스템에 의해 부과된 타이밍 목적을 하드웨어 제약조건 내에서 달성해 내는 소프트웨어 시스템의 능력을 타이밍이라 할 수 있다. 운영체제는 자체적인 타이머를 두어 태스크들의 실행시간을 계산하고 시간 내에 종료할 수 있도록 스케줄러의 행동을 돕는 역할을 하게 된다. 타이밍이 결정적으로 동작해야 수행시간이 예측가능하여 실시간 속성을 만족할 수 있게 된다.

[표 4] 타이밍/사이징 안전성 평가항목

대상	Deviation Checklist	영향
타이밍	타이머 작동실패	시간계산불가
	인터럽트 지연발생	Deadline 실패가능
	타이밍 비결정적동작	수행시간 예측불가
사이징	할당될수 없는메모리 조각발생	메모리낭비

● 기능성

운영체제는 소프트웨어가 수행되는데 기반을 제공해 주는 것으로 특정기능의 수행여부를 가지고 그 평가를 할 수 있다. 운영체제 기능을 점검하기 위해서는 운영체제 위에 응용프로그램을 실행시키고 응용프로그램의 기능들이 동작하는 지를 확인하는 것이 더욱 용이하다.

[표 5] 기능성 안전성 평가항목

대상	Deviation Checklist	영향
기능성	특정기능이 각동작모드에 대해 수행하기전 초기화실패	데이터 무결성침해
	특정기능이 각동작모드에 대해 수행불가	운영체제가 다른프로그램제어불가
	시작조건이 만족되지 않았는데 특정기능수행	불필요한 동작수행 필요한 동작수행불가
	시작조건은 만족하였는데 특정기능수행실패	
	종료조건이 만족된후에도 특정기능이 계속수행	
	종료조건이 만족되기전에 특정기능이종료	

● 강인성

강인성은 소프트웨어 시스템이나 기기가 부정확한 입력 또는 응력의 환경조건을 받더라도 소정의 기능을 정확하게 발휘해 내는 능력을 말한다.

[표 6] 강인성 안전성 평가항목

대상	Deviation Checklist	영향
강인성	예상치않은 입력데이터에 대해 커널이 원래기능을 상실	커널예외처리
	부정확한 입력데이터에 대해 커널이 원래기능을 상실	
	특이조건발생으로 커널이원래 기능을 상실	
	커널이 요구되는 자체복구실패	커널서비스중단

● 보안성

무단적이고 불필요하고 불안전한 침투를 방지하기 위해 소프트웨어에 요구되는 능력을 말하는데 이런 침투들이 소프트웨어의 안전관련 기능에 영향을 줄 수 있는 한 보안은 안전성 현안이라고 할 수 있다. 내장형 시스템과 같이 특정한 응용프로그램만을 위한 운영체제는 메모리보호를 통해 커널이 동작하는 공간에 다른 응용프로그램이 침범하지 못하는 동작으로 보안에 관한 사항을 실천할 수 있다. 메모리 보호를 통한 보안요구사항은 정확도 사항에서 다루었고 여기서는 사용자의 확인을 통한 운영체제 접근을 인증하는 방법으로 점검한다.

[표 7] 보안성 안전성 평가항목

대상	안전성 평가 검증리스트	영향
보안성	비밀번호를 통한 시스템의 접근통제실패	임의의 사용자위협

4. 결론 및 향후 계획

안전등급 제어기기에서 사용되는 운영체제가 원자력분야에서 적용되기 위해서 가져야 할 기능들의 안전성을 위해 BTP-14 에서 제안한 정확도, 신뢰성, 타이밍/사이징, 기능성, 강인성, 보안성 특성에 따라 HAZOP을 이용하여 요구사항 단계에서의 안전성 분석을 시도하였다. 추후 운영체제가 다른 시스템에 적용되었을 경우 운영체제에 의한 위해도를 발견해 내서 그 위해도가 계통에 미치는 영향을 분석할 계획이다. 이러한 작업은 궁극적으로 운영체제 안전성분석의 목적이라고 할 수 있으며, 운영체제 안전성 분석의 완성도를 보완할 수 있게 된다.

참고문헌

[1] 이나영, "정형검증과 시험에 의한 원전 계측제어용 임베디드 소프트웨어의 개발", 정보과학회지 제22권 제6호 pp43~49, 2004.6.

[2] USNRC, "BTP-14: Guidance on Software Reviews for Digital Computer-based I&C Systems," NUREG-0800. 1997.

[3] David N. Kleidermacher, Real-time Operating System Requirements for Use in Safety Critical Systems, Green Hilis Inc.

[4] 이장수, "소프트웨어 요구명세 안전성 분석을 위한 HAZOP 방안" 2003춘계학술발표회, 한국원자력학회, 2003

[5] David Stepner, "Embedded Application Design Using a Real-time OS", IEEE, 1999

[6] Bruce Power Douglas, "Safety-Critical Embedded Systems", Embedded System Programming. Oct. 1999.