원전에서의 안전-필수 시스템에 대한 소프트웨어 안전성 분석

천세우 · 이장수
한국원자력연구소

1. 서 론

지난 20년간 디지털 기술은 철도, 항공, 운송 및 통신 네트워크 등과 같은 산업 분야에서 계측제어(I&C: Instrumentation and Control) 시스템에 급속도로 적용되어 왔다. 안전을 중요시하는 원전 분야에서도 점차로 디지털 기술 도입을 하면서 외국에서는 Teleperm XS, Common Q 및 Triconex 등과 같이 PLC(Programmable Logic Controller)를 응용한 I&C 시스템 개발에 역점을 두고 있는 추세이다. [1)]

현재 국내에서도 이러한 원전의 추세에 따라서 안전-필수(SC: Safety-Critical) 소프트웨어 계측제어시스템에 대해서 품질보증(qualified)된 PLC의 국산화를 위해 KNICS(Korea Nuclear Instrumentation and Control System) 과제를 수행하고 있다. KNICS 과제에서는 안전등급 PLC의 국산화와 함께 이 PLC를 이용하여 디지털계측제어계통인 발전소보호계통(PPS: Plant Protection System)의 프로토타입 개발을 목표로 두고 있다.

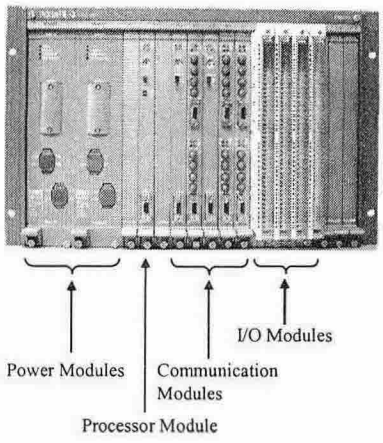
이러한 디지털계측제어계통에 대한 소프트웨어 확인 및 검증(V&V: Verification and Validation) 업무 [2)]와 함께 안전성 확보가 중요한 현안으로 부각되고 있다. 이에 따라 소프트웨어 생명주기(SLC: Software Life Cycle) 각 단계별로 안전성 분석(Safety Analysis) 수행을 인허가 기준으로 의무화하고 있다. [3)]

본 논문에서는 현재 KNICS 과제에서 수행하고 있는 안전등급 PLC의 안전-필수 소프트웨어의 안전성 분석을 위해 HAZOP(Hazard and Operability) 기법을 이용해서 소프트웨어 요구사항명세(SRS: Software Requirement Specification)의 안전성 분석에 활용할 수 있도록 지침 구문(Guide Phrases)과 체크리스트를 적용하였고 이를 이용한 SRS 안전성 분석에 대해서 기술하겠다.

2. 안전-필수 시스템 개요

현재 개발 중인 안전등급 PLC 특징은 산업체에서 검증된 기술을 사용해서 개방 구조로 구성되어 있고 Fig. 1a와 같이 크게 Power Modules, Processor Module, Communication Modules 및 I/O Modules로 구성되어 있다. 안전 소프트웨어 컴포넌트들은 Fig. 1b와 같이 PLC의 안전 기능을 위해 구현되었으며 안전-필수(SC: Safety Critical) 등급, 안전-관련(SR: Safety-Related) 등급 및 비 안전(NS: None Safty) 등급

으로 분류할 수 있다. Fig. 2는 안전등급 PLC를 기반으로 하는 전체적인 KNICS 발전소 보호계통 프로토타입 구성을 나타내고 있다. 보호계통은 크게 원자로보호계통(RPS: Reactor Protection System)과 공학적안전설비-기기제어계통(ESF-CCS: Engineered Safety Features-Component Control System)으로 구성되어 있다. [4)]



(a) 안전등급 PLC 구성

안전등급 PLC 소프트웨어	프로세서 모듈 RTOS	pCOS	커널(Scheduling, ITC, TaskManagement)	SC
			BIHS	SC
		시스템 태스크	Start Up	SC
			Shell 태스크	SC
			Diagnosis 태스크	SC
			LoaderReady 태스크	SC
			Loader_service 태스크	SC
			Communication 태스크	SC
			User_task 태스크	SC
	통신 모듈	Profibus-FDL1	FDL1-CPB 운영체제 (PNMOS4)	SC
			FDL1 Driver 운영체제 (PNDOS4)	SC
		Profibus-FDL2	FDL2-CPB 운영체제 (명칭 미확정)	SC
			FDL2 Driver 운영체제 (명칭 미확정)	SC
		Profibus-FMS	FMS-CPB 운영체제 (PNMOS1)	SR
			FMS Driver 운영체제 (PNDOS1)	SR
	I/O 모듈	Analog Input 운영체제 (PIAOS1)		SC
		Analog Output 운영체제 (POAOS1)		SC
	pSET	Interpreter, Linker		SR
		Compiler, Loader		SR
		Editor, Debugger		NS
		Simulator		NS

(b) 안전등급 PLC 소프트웨어 종류

Fig. 1. 안전등급 PLC 구성 및 소프트웨어 종류

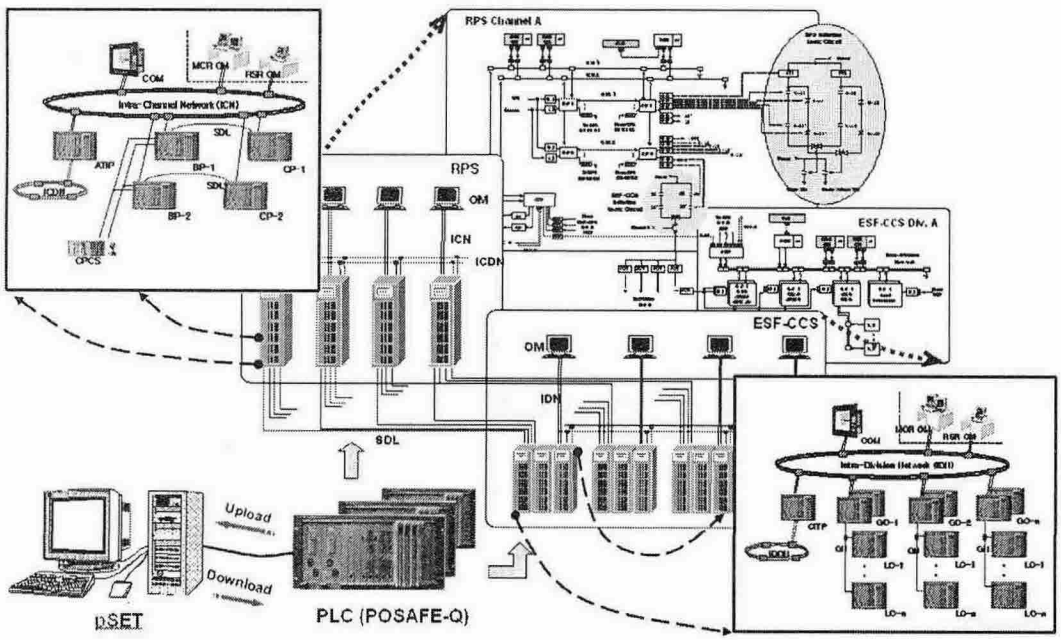


Fig. 2. KNICS 발전소 보호계통 프로토타입 구성

3. 소프트웨어 안전성 분석

3.1. 적용 기준 및 스탠다드

소프트웨어 요구사항 안전성 분석과 관련된 기준 및 기술 표준으로는 IEEE Std. 7-4.3.2-2003, [5] Reg. Guide 1.173, [6] IEEE 1228-1994 [7]와 Standard Review Plan(SRP)의 BTP HICB-14 [2]를 사용하였다. 또한 과학기술부 고시(안)의 " 원전의 안전계통에 사용되는 디지털 컴퓨터 소프트웨어에 대한 소프트웨어 요건명세서" 기준 [8]을 근거로 한다.

3.2. 소프트웨어 안전성 분석방법 및 절차

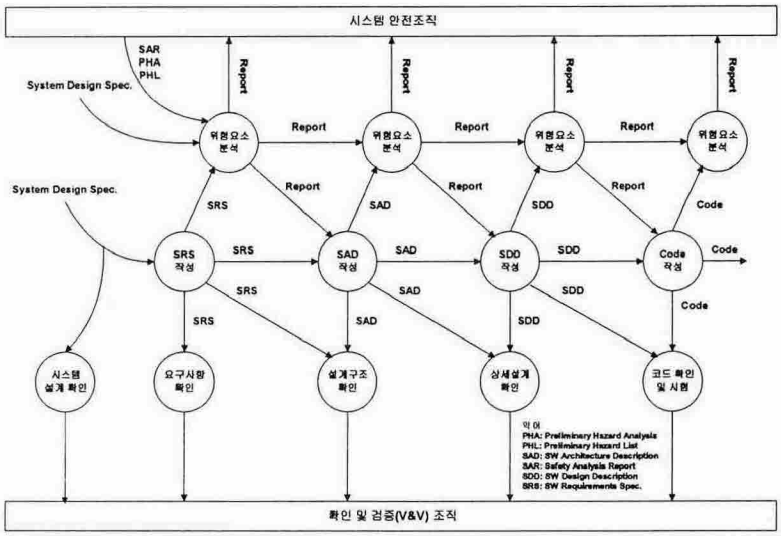


Fig. 3. 소프트웨어 개발공정 단계별 안전성 분석

KNICS 과제에서 안전성 분석은 IEEE Std 1228-1994 소프트웨어 안전성 계획 표준에서 요구하는 기준에 따라 Fig. 3과 같이 소프트웨어 개발공정 단계별로 소프트웨어 안전계획에 따라서 안전성 분석을 수행하고 있다. 소프트웨어 안전계획[9]은 시스템 안전 현안이 소프트웨어 개발 중에 적절히 고려되도록 하는 기본적인 문서로서 분석 수행조직, 안전성 분석책임, 소프트웨어 안전성 활동관리, 그리고 위험요소와 비정상조건이나 사건 등을 다루기 위해 각 단계마다 수행되어야 할 분석사항들을 기술하고 있다.

소프트웨어 요구사항명세에 대한 안전성 분석에는 화학공장과 같은 산업에서 시스템 안전성 분석을 위해 성공적으로 사용되었던 HAZOP 기법을 적용하였다. HAZOP에 의한 안전성 분석은 사고가 설계 또는 운영상에서 의도한 것에서 벗어났을 때 발생하는 것을 가정하고 설계에서 예상한 운용을 하였을 경우 일어날 수 있는 모든 가능한 이탈(deviation) 상황과 그와 관련된 모든 위해 요소를 찾으려고 하는 것이다.

소프트웨어 HAZOP 방법에 의한 안전성 분석은 Fig. 4와 같은 절차 [10,11]에 따라 시스템 또는 요구사항 명세를 구성하고 있는 각 항목에 대해 Table 1의 지침 구문(Guide Phrases)을 사용하여 의도된 동작에서 이탈이 일어났을 때 발생 가능한 모든 위해도에 대해서 전문가팀이 원인, 영향(결과), 질의 및 권고사항 등을 나열함으로써 체계적으로 수행한다.

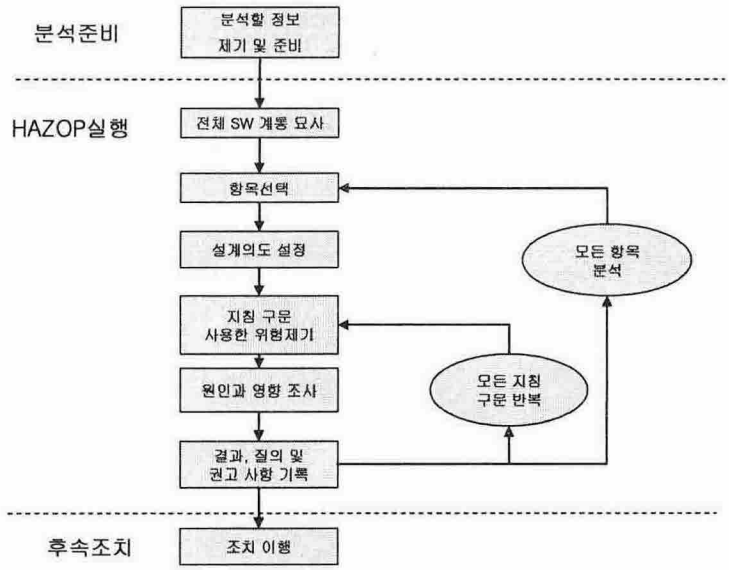


Fig. 4. HAZOP 절차

Table 1. 소프트웨어 HAZOP을 위한 Guide Phrases

품질특성	적용 대상	적용단계	Guide Phrases
정확도	태스크	RADC	Task cannot reach on the predefined states
		RADC	Task creation fail
		RADC	Task with same priority to others
	메모리	RADC	Stuck at all zeros
		RADC	Memory partition assignment fail
		RADC	Stack overflow
	WDT	RADC	WDT fail
	동기화	RADC	Supervisor task fail
		RADC	Restart application
성능	타이밍	RADC	Timer fail
	사이징	RADC	Memory chunk
기능성		RA	Function is not initialized properly before being executed
신뢰성		RA	Application task uses data structure in kernel
		RA	RTOS fails in-service test

R: Requirements, A: Architectual Design, D: Detail Design, C: Coding

4. 소프트웨어 요구사항 상세 안전성 분석

Table 2는 안전등급 PLC 프로세스 모듈에 대해서 도출된 예비 위해도 요소 및 안전 중요도 예를 나타내고 있다.

Table 2. 안전등급 PLC 프로세스모듈 예비 위해도의 안전 중요도

번호	PLC 운영체제 위해도 요소	PLC 소프트웨어 관련 여부	안전 중요도
1	PLC 에 공급되는 전원이 상실되는 경우	간접 관련	4
2	PLC 운영체제 구성요소(kernel, system tasks, bihs,...)들의 작동불가	간접 관련	4
2.1	구성요소간의interaction 실패에 의한 기능상실	직접 관련	4
3	PLC 기기의 내부 화재	간접 관련	4
4	PLC 운영체제의 작동모듈 실패	직접 관련	3
5	PLC 운영체제(kernel)의 동작실패		
5.1	태스크 생성 시스템호출(Task creation system call)	직접 관련	4

주) 안전 중요도: 4 - 매우 높음, 3 - 높음, 2 - 중간, 1 - 낮음.

안전등급 PLC 요구사항 공정특성(즉, 완전성, 일관성, 정확성, 추적성, 비모호성, 스타일 및 검증성)에 대해서 체크리스트를 이용한 종합적 안전성 검토(즉, 각 체크리스트에 대한 검토의견, 위험영향(결과) 및 설계 권고사항)를 일차적으로 실시하였다. 요구사항의 기능특성(즉, 정확도, 신뢰성, 성능(타이밍/사이징), 기능성, 강인성 및 보안성)에 대해서는 HAZOP 기법을 이용한 상세 안전성 분석을 Table 3과 같이 수행하였다. [12)]

Table 3. 기능특성에 대한 위해도 분석결과 예

품질 특성	적용 대상	Guide Phrases	Deviation Checklist	원인	공통 원인	위험영향 (결과)	위험도	권고사항	비고
성능	타이밍	Timer fail	타이머가 작동하지 않을 경우 어떠한 위험을 초래하는가?			WDT 작동불가	3		
		Interrupt latency occurs	인터럽트 지연이 발생하면 어떤 위험을 초래하는가?	스위칭 오류		Deadline 실패 가능성	4		
		Non-determ-in istic system behavior	타이밍이 비결정적일 때 어떤 위험을 초래하는가?	스케줄 에러		수행시간 예측불가	4		
	사이징	Memory chunk	메모리에서 mapping 되지 않은 ram chunk는 어떤 위험을 초래하는가?	단편화		메모리 낭비	3	static memory allocation 유도	
기능성		Function is not initialized properly before being executed	특정 기능이 각 동작 모드에 대해 명세 된 대로 수행하기 전에 적절히 초기화 되지 못할 때 어떤 위험을 초래하는가?	Reset 후 초기화 실패	연산, 변수 에러	데이터 무결성 침해	4	초기화후에만 기능이 수행될 수 있도록 함. 안전성 분석 추적 확인 필요함.	
보안성		Password system fail	비밀번호를 통한 시스템의 접근을 구현하지 못하면 어떠한 위험이 발생하는가?	어플리케 이션 에러		보안 위협	4	초기화 부분에 사용자에 대한 인증도 고려	

5. 결론 및 추후 연구

본 논문에서는 KNICS 과제를 수행하면서 안전-필수 시스템인 안전등급 PLC에 대한 요구사항 단계에서의 안전성 분석 업무에 대해서 기술하였다. 요구사항 명세의 공정 특성과 기능특성에 대한 HAZOP 안전성 분석을 수행하여 설계 권고사항들을 설계자들에게 피드백 할 수 있었다.

HAZOP 기법을 이용한 안전성 분석을 시작으로, 추후에 정형 명세(Formal Specification)화 된 요구사항에 대해서는 안전 특성을 정형화하고, 상세 모델(예를 들면 Statechart)에 대한 Model Checking 방법으로 안전성 분석을 수행 할 예정이다.

감사의 글

본 연구는 산업자원부(MOCIE) 지원으로 원전계측제어시스템개발사업(KNICS)의 "디지털계측제어 인허가확보기술 개발" 과제에서 수행되었습니다.

참고문헌

1) Proceedings of Digital Instrumentation Upgrades Workshop, Embedded Meeting of NPIC & HMIT 2004, Columbus, Ohio, Sept. 19, 2004.
2) BTP HICB-14, Branch Technical Position HICB-14, *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems*, USNRC, 1997.
3) NUREG-0800, Standard Review Plan, Chapter 7, USNRC, 1997.
4) S. W. Cheon *et al.*, "Development of a Software Configuration Management System for Software Life Cycle Management," in Proceedings of the NPIC&HMIT 2004, Columbus, Ohio, Sept. 19-22, 2004.
5) IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
6) Regulatory Guide 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Office of Nuclear Regulatory Research, USNRC, 1997.
7) IEEE Std 1228-1994, "Standard for Software Safety Plan," Institute of Electronic and Electrical Engineers.
8) 과학기술부 고시(안) 제01-X09호, 원자로시설의 계측제어계통에 관한 기준.
9) 안전등급 PLC 소프트웨어 안전계획서, KNICS-PLC-SEP109, Rev.00, 한국원자력연구소, 2004. 9.
10) 안전등급 PLC 시스템 안전성 분석 절차서, KNICS-PLC-VP101, Rev.00, 한국원자력연구소, 2005. 8.
11) NUREG/CR-6430, "Software Safety Hazard Analysis," Lawrence Livermore National Laboratory, February 1996.
12) 안전등급 PLC 프로세스모듈 운영체제 요구사항명세 안전성 분석보고서, KNICS-PLC-SVR122-01, Rev.00, 한국원자력연구소, 2005. 3.