Journal of The Institute of Electronics and Information Engineers Vol.53, NO.8, August 2016 http://dx.doi.org/10.5573/ieie.2016.53.8.107
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2016-53-8-12

원전 계측제어 시스템 보안성환경을 위한 진단기능 평가

(Evaluation of Software Diagnostics for Secure Operational Environment in Nuclear I&C systems)

유 성 구*, 설 남 오*

(Sung Goo Yoo and Namo Seul©)

요 약

원자력발전소의 안전필수 기능을 수행하는 계측제어 시스템은 원자로의 예상되는 과도상태가 발생되거나 설계기준사고의 결과를 완화하기 위해 원자로 및 주요 기기의 상태를 감시한다. 만일 원자로출력, 냉각재 온도, 또는 증기발생기 수위 등의 상태가 기 정해진 설정치에 도달하게 되면 정확하고 신속하게 원자로를 정지시키는 기능을 수행한다. 이러한 안전필수 시스템은 예상 가능한 사고로부터 인간과 자연을 보호하기 위한 중요 기능을 수행하는 디지털 제어시스템으로써, 비인가 된, 의도되지 않은 변경 등의 취약점으로 인해 신뢰성 있는 운영이 영향을 받지 않도록 보안성환경이 구축되어야 한다. 이러한 보안성환경은 관리적 조치와 기술적 조치를 통해 구현될 수 있다. 본 논문에서는 안전필수 기능을 수행하는 원전 계측제어 시스템의 제어용 소프트웨어 진단기능이 보안성환경을 구축하는 데 효과적인 설계방안인지를 평가하였다. 이를 위해, 제어용 소프트웨어의 무결성을 확인하는 순환잉여검사(CRC) 진단기능에 대한 모의실험을 수행하였다. 본 논문에서의 효과성 평가는 향후 안전필수 기능을 수행하는 원전 계측제어 시스템의 설계 및 안전성 분석에 활용될 수 있을 것으로 기대된다.

Abstract

Safety Critical Instrumentation and Control Systems perform those functions to maintain nuclear power plants' parameters within acceptable limits established for a design basis events and anticipated operating occurrence to ensure safety function. Those digitalized systems shall protect inadvertent and non-malicious behavior to ensure the reliable operation of systems, known as a Secure Development and Operational Environment(SDOE). SDOE would be established through managerial and technical controls. The objective of this paper is to evaluate the effectiveness of Cyclic Redundancy Checksum diagnostic, which is one of technical controls for SDOE, that can confirm the integrity of software of I&C systems to establish the secure environment. The results of this assessment would be the practical implementation of design and safety review of nuclear I&C systems.

Keywords : Nuclear Instrumentation & Control Systems, Plant Protection Systems, Safety-Critical Systems, Secore Development and Operational Environment(SDOE), Software Integrity

Ⅰ. 서 론

원자력발전소의 계측제어 시스템은 원자로 및 주요 기기의 다양한 변수를 연속적으로 감시하여, 기 설정된 운전범위 이내로 이들 변수와 기기를 안전하게 운전하는 기능을 수행한다. 특히, 원전의 예상되는 운전사건으로 인해 핵연료제한치가 기 설정된 값을 초과하지 않도록 핵증기공급계통(NSSS, Nuclear Steam Supply System) 및 구동기(펌프, 밸브 등)를 자동 제어하는 안전필수 기능을 수행한다. 원전 안전필수 기능의 대표적인 시스템인 발전소보호계통(Plant Protection Systems)은 원전의 예상되는 과도상태가 발생되거나 설계기준사고의 결과를 완화하기 위해 원자로 및 주요 기기의 상태를 감시한다. 만일 원자로출력, 냉각재 온도, 또는 증기발생기 수위 등의 상태가 기존의 정해진 설정치에 도달하게 되면 정확하고 신속하게 원자로를 정지시키는 기능을 수행한다[1~2].

최근 원전의 계측제어 시스템은 디지털 기술을 적용한 프로그래머블 논리 제어기(PLC) 또는 분산제어시스템(DCS) 기술을 기반으로 설계되고 있다. 특히 개방된

* 정회원, 서남대학교 (Seonam University)
© Corresponding Author (E-mail : selnamo@nate.com)
Received ; June 9, 2016 Revised ; July 13, 2016
Accepted ; July 27, 2016

자원(하드웨어, 소프트웨어, 펌웨어)을 통해 설계 및 운영되는 추세이며, 그에 따라 정보기술 분야에서와 동일 또는 유사한 취약점이 발생될 수 있는 가능성이 증대되고 있다. 즉, 디지털 기반의 안전필수 계측제어 시스템은 물리적인 접근이 없더라도 대상 시스템을 제어하고 감시할 수 있는 능력을 가지고 있으며, 이는 성능이나 운영 측면의 장점으로 부각될 수 있는 반면, 부주의한 변경을 통해 대상 시스템에 양향을 미칠 수 있는 취약성도 가지고 있다. 이에 따라, 디지털 기술이 적용된 원전 계측제어 시스템은 연결된 계통의 부주의한 행위나 접근에 의해 개시된 사건이 동 계통의 신뢰성 있는 운영을 저해하지 않음을 보증할 수 있을 정도로 적절한 관리적 및 기술적 통제를 갖추어야 하며, 이는 보안성환경(SDOE, Secure Development and Operational Environment)로 정의된다[3~4]. 보안성환경은 안전성 확보를 위한 계측제어 시스템의 설계기준과 속성을 통해, 부주의하거나 의도하지 않은 비 악의적 침해행위를 탐지하고 차단하여 대응할 수 있는 일련의 능력을 의미한다.

원전 계측제어 시스템의 보안성환경을 위한 설계는 다중화, 독립성, 그리고 심층방어 및 다양성 등의 개념을 포함한다. 특히, 제어기의 건전성을 지속적으로 확인하는 여러 진단기능은 보안성환경의 구축을 위한 매우 중요한 속성으로 대두되고 있다[5]. 이러한 진단기능에는 안전필수 소프트웨어(시스템 소프트웨어 및 응용 소프트웨어 포함)의 부주의한 변경 발생 시, 이를 탐지하는 기능도 포함된다.

본 논문에서는 원전 계측제어 시스템의 무결성 확보를 위한 소프트웨어 진단기능의 특성을 분석하고, 이러한 진단기능이 계측제어 시스템의 보안성환경을 구축하는 데 충분한 능력을 보유하고 있는지 시뮬레이션을 통해 확인하고자 한다.

Ⅱ. 원전 계측 시스템의 보안성 환경

1. 보안성환경의 개념

원전 계측제어 시스템은 설계기준사건의 결과를 방지하거나 그 영향을 완화시켜, 방사선의 재해로부터 안전성을 확보하는 목적으로 설계된다. 이를 위해 원자력안전법 등 법령에서 규정하는 높은 신뢰성과 다양한 설계 요건을 만족시켜야 한다. 이를 위해 원전의 계측제어 시스템은 법령 및 산업 표준에 부합하기 위해, 여러 설계기준을 통해 설계된다. 예를 들어, 동일한 기능을 수행하는 4개 채널의 동일 제어기를 통해 제어논리를 수행하는 다중성 설계나, 공통원인고장(Common Cause Failure)을 대비하여 속성이 다른 하드웨어 및 소프트웨어를 적용한 다양성(diversity) 설계 등이 적용되고 있다. 이러한 원전 계측제어 시스템에 대한 보안성환경의 개념은 크게 원전 계측제어 시스템의 개발환경과 운영환경으로 구분한다. 보안성 개발환경(SDE, Secure Development Environment)은 디지털 안전계통에 불필요하거나 문서화되지 않은 기능(예, 잉여 코드)이 포함되지 않음을 보장할 수 있을 정도로 동 계통의 개발단계(즉, 개념, 요건, 설계, 구현, 시험) 중 적절한 물리적, 논리적, 계획적 통제를 갖춘 상태를 말한다. 또한, 보안성 운영환경(SOE, Secure Operational Environment)은 연결된 계통의 바람직하지 않은 행위나 부주의한 접근에 의해 개시된 사건이 디지털 안전계통의 신뢰성 있는 운영을 저해하지 않음을 보증할 수 있을 정도로 적절한 기술적, 운영적 및 관리적 통제를 갖춘 상태를 말한다[6~8]. 아래 그림 1은 보안성환경에 대한 개념을 간략히 나타낸 것이다.

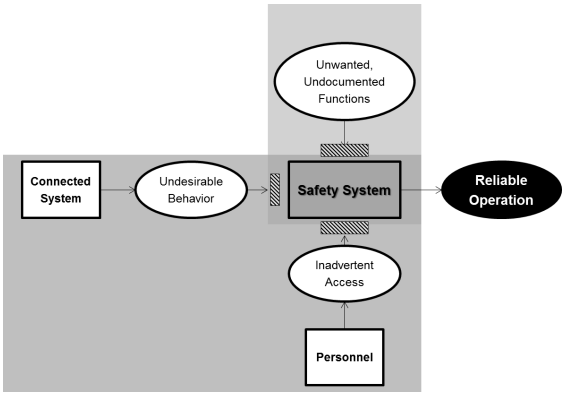

그림 1. 보안성 활동 및 기능
Fig. 1. Secure development activities and features.

원전에서의 보안성환경은 사이버보안과 구별된다. 원전에서의 사이버보안은 사보타주 및 핵물질 불법이전을 위한 사이버 공격을 효과적으로 예방·탐지·대응하는 체계를 구축하는 개념으로서, 악의적(malicious) 사이버 공격에 대응하는 전반적 체계를 의미한다. 이에 비해, 보안성환경은 불필요하거나 문서화되지 않은 기능이 포함되지 않고, 부주의한 접근 등에 의해 개시된 사건이 안전계통의 신뢰성 있는 운영을 저해하지 않도록 보증하는 개념으로서, 비 악의적(non-malicious) 행위에 대응하는 설계 및 운영 특성을 의미한다.

특히, 안전필수 기능을 수행하는 제어용 소프트웨어의 무결성을 확보하는 등 다양한 진단기능이 설계되고

있다. 이러한 진단기능은 소프트웨어의 부주의한 변경을 탐지하고 대응할 수 있도록 설계되는 등 계측제어 시스템의 보안성환경의 구축을 위한 중요 속성으로 인식되고 있다.

원전에서의 사이버보안과 보안성환경에 대한 개념 비교는 아래 표와 같다.

표 1. 사이버 보안과 보안성환경의 비교
Table1. Comparison of Cyber Security and SDOE.

	사이버보안	보안성환경
개념	· 사보타주 및 핵물질 불법 이전을 위한 사이버 공격을 예방·탐지·대응 · 사이버 공격 영향 최소화	· 불필요하거나 문서화되지 않은 기능이 포함되지 않고, · 부주의한 접근으로 인해 제어 시스템의 운영성 저해를 방지
취약성 예시	· 악성코드에 의한 컴퓨터 손상 · 의도적인 데이터 폭주 · 전송 데이터의 변조 등	· 포함되지 않아야 할 코드로 인해 제어기의 고장 발생 · 오류데이터로 인한 기능상실 · 부주의한 변경 등
방법	· 사이버보안 체계의 수립 · 기술적, 운영적, 관리적 사이버보안 통제	· 생명주기 단계별 평가 및 검증 · 보안성 환경 설계 특성 적용 · 의도되지 않은 코드 비 포함
통제 예시	· 제어기의 바이러스 탐지 S/W · 주기적 보안 패치 · 이동형 저장장치의 통제 · 사이버보안 조직 구성 · 인적 보안 등	· S/W 확인 및 검증 · 문서화되지 않은 코드를 제거 · 제어용 S/W에 대한 진단기능 설계

2. 보안성환경을 위한 진단기능 특성

원전 계측제어 시스템의 하드웨어는 높은 신뢰성을 갖는 부품의 사용, 소프트웨어의 품질 및 신뢰도 확보, 그리고 결정론적 처리 등 성능요구사항을 충족해야 한다. 또한, 계측제어 시스템의 고장 및 오작동을 사전에 감지하여, 원전의 안전성에 지장을 초래할 가능성을 제거하기 위한 진단기능이 구현되어야 한다. 이를 위해 계측제어 시스템의 고장 유형이 설계에 고려되어야 한다.

그림 2는 원전의 계측제어 시스템에 적용되는 PLC의 CPU 모듈에 대한 진단기능을 개략적으로 나타낸 것이다.

이러한 진단기능은 프로세서의 정지, 운영체제 및 응용 프로그램의 오류, 메모리 오류, 통신 입·출력 오류, 형상 오류, 스캔타임 초과 등 다양한 고장상태의 감지를 포함한다. 특히, 제어기의 운영체제 소프트웨어와 응용 프로그램에 비정상적인 변경이 발생할 경우, 이를 탐지하기 위한 설계를 위해 순환잉여검사(CRC, Cyclic Redundancy Checksum) 방식도 적용된다[9~10].

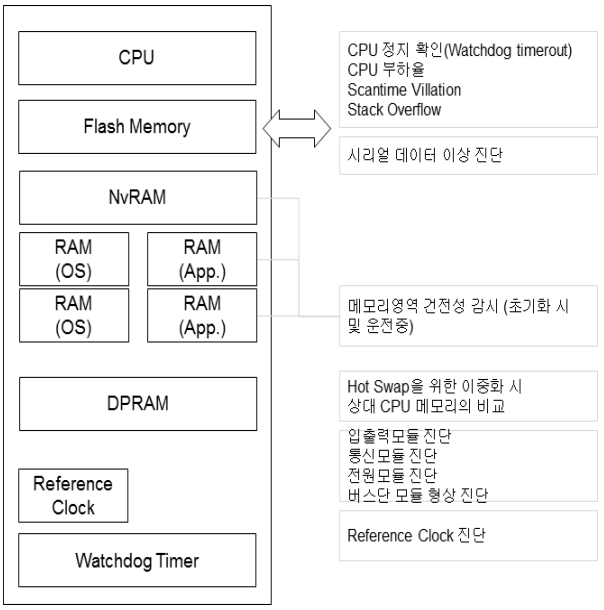

그림 2. 프로세서 모듈의 진단 기능
Fig. 2. Diagnostic Function of Processor Module.

Ⅲ. 무결성 진단 및 모의실험

1. 제어용 소프트웨어의 무결성 진단

원전의 계측제어 시스템은 운전 중 부주의한 제어용 소프트웨어의 변경으로 인해 동 계통의 신뢰성 있는 운영이 영향을 받지 않도록 보안성환경이 구축되어야 한다. 이를 위해, 동 계통은 실시간 운전 중에도 다양한 방식을 통해 제어용 소프트웨어가 무결성을 유지하고 있는지 확인한다. 이러한 방식에는 동일한 기능을 수행하는 다중 제어채널간의 주기적인 운전상태 비교 등 관리적인 사항, 그리고 실시간 소프트웨어 무결성 진단기능 등 기술적인 사항을 포함한다.

통상 CRC 진단기능은 네트워크 전송시 미리 계산된 다항식의 결과값을 원 데이터와 함께 전송하고, 수신단에서는 이를 역변환하여 원 데이터가 정상적으로 도달하는지를 진단하는 기능으로 통상 활용되어 왔다. 이와 같이, 통상적으로 네트워크의 송수신 데이터에 대한 진단기능에 적용되는 CRC 방식은 오프라인 형태의 시스템 내부에서 발생하는 소프트웨어의 부주의한 변경을 탐지하는 데에도 활용될 수 있다[11].

표 2에 일반적으로 사용하는 CRC방식들을 나타내었다.

표 2. CRC 다항식과 비트크기
Table2. CRC Polynomial and bit size.

CRC 방식	다항식 형태	비트 크기
CRC-4	$x^4+x^3+x^2+x+1$	4
CRC-8	$x^8+x^7+x^6+x^4+x^2+1$	8
CRC-16	$x^{16}+x^{15}+x^2+1$	16
역 CRC-16	$x^{16}+x^{14}+x+1$	16
CRC-24	$x^{24}+x^{23}+x^{14}+x^{12}+x^8+1$	24

원전 계측제어 시스템은 통상적으로 네트워크의 송수신 데이터에 대한 진단기능에 적용되는 CRC 진단 방식과 유사한 방식으로 제어용 소프트웨어의 무결성을 진단하도록 설계되어 있다.

원전 계측제어 시스템은 firmware와 RAM의 모든 stack domain, 그리고 사용자 flash PROM에 대해 CRC 점검을 수행한다. 이는 앞서 기술한 CRC의 연산 방식과 유사하며, 운영체제 및 응용 프로그램은 기본 4k bytes단위의 블록마다 CRC를 계산하도록 설계된다. 계측제어 시스템이 초기화되는 경우, 프로그램을 Flash ROM에서 RAM으로 복사되며, CRC도 동시에 복사되어 RAM 영역의 firmware data area에 고정값으로 저장된다. 원전 계측제어 시스템의 정상운전 중 RAM에 저장된 프로그램은 주기적으로 CRC 계산을 수행하고, Firmware Data Area에 저장된 CRC와 비교한다. 만일 RAM에 저장된 설정치 등이 운전 중 부주의하게 변경되거나, 연결된 계통의 영향으로 인해 메모리 영역이 변경된다면, 주기적으로 계산되는 CRC값은 고정값으로 저장된 CRC값과 일치하지 않게 되며, 이를 감지하게 되면 응용 프로그램은 단일 프로세서의 기능을 정지시키고 운전원에게 경보를 제공하도록 설계되어 있다. 원전 계측제어 시스템의 제어용 소프트웨어 무결성 진단을 위한 CRC는 16bit 연산을 수행하며, 만일 탐지율을 높이기 위해 보다 강화된 CRC 연산을 수행할 경우, 전체 계통의 응답시간 등이 영향을 미칠 수 있다. 이러한 CRC 진단기능은 운영체제 및 응용 프로그램의 부주의한 변경을 탐지할 수 있는 설계 기법으로 활용되고 있다.

2. CRC 진단기능에 대한 모의실험

본 논문에서는 원전 계측제어 시스템의 제어용 소프트웨어가 부주의한 변경 등으로 영향을 받지 않도록 설계된 CRC 진단기능이 보안성환경을 구축하는 데 효과적인 설계방식인지를 평가하기 위해, 그림3과 같은 모의실험 환경을 설정하였다.

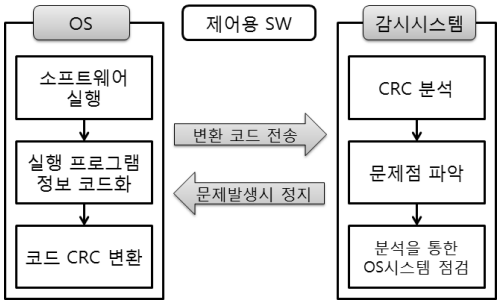

그림 3. 건전성 직단 방식 구성도
Fig. 3. Simulation Environments for Diagnostics to ensure Secure Operational Environment.

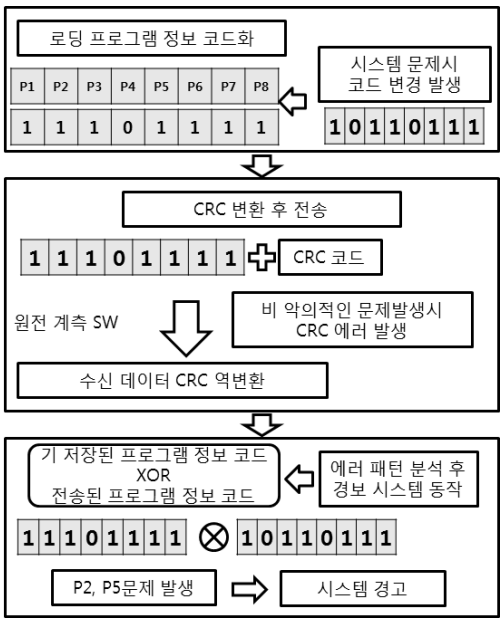

그림 4. 시뮬레이션 진행순서
Fig. 4. Simulation Flow.

본 논문에서는 모의실험을 위해, 대상 시스템의 운영체제 메모리영역 안에서 로드된 프로그램을 코드화하고, 이를 일정 블록단위로 CRC 연산을 수행하여 그 결과를 타 시스템에서 감시하도록 설정하였다. 프로그램 정보 코드는 8bit 단위로 구성하였으며, 특정 메모리 공간은 원치 않는 또는 부주의한 프로그램 변경이 발생할 수 있도록 할당하였다. 계측제어 시스템에 로드된 소프트웨어는 고정적으로 운영이 되므로, 만일 소프트웨어에 부주의한 변경이나 악영향이 발생하지 않는다면 소프트웨어 코드정보는 항상 일정한 CRC 값을 출력하게 된다. 만일 부주의한 변경이 발생하여 특정 메모리 공간이 변경되었다면, 지속적으로 동일한 CRC값이 아닌

다른 결과값이 나타나게 될 것이다.

표 3. 에러 패턴
Table3. Error pattern.

오류패턴	시간	P1	P2	P3	P4	P5	P6	P7	P8
EP1	10분	0	1	1	0	1	1	1	1
EP2	20분	1	0	1	0	1	1	1	1
EP3	30분	1	1	0	0	1	1	1	1
EP4	40분	1	1	1	1	1	1	1	1
EP5	50분	1	1	1	0	0	1	1	1
EP6	60분	1	1	1	0	1	0	1	1
EP7	70분	1	1	1	0	1	1	0	1
EP8	80분	1	1	1	0	1	1	1	0
EP9	90분	1	0	1	0	1	0	1	1
EP10	100분	1	1	1	0	1	0	0	1
EP11	110분	1	0	1	0	1	1	0	0
EP12	120분	1	1	1	1	0	0	0	1
EP13	130분	1	0	0	1	1	0	0	1
EP14	140분	1	0	0	0	1	0	0	0
EP15	150분	0	0	0	1	0	0	0	0

표 4. 표3을 적용한 에러 코드
Table4. Error code according to Table 3.

	CRC 코드 (CRC-16)				에러 체크 코드 (0 : 정상, 1 : 에러 발생)							
					P1	P2	P3	P4	P5	P6	P7	P8
정상값	0	C	C	1	0	0	0	0	0	0	0	0
EP1	9	D	4	9	1	0	0	0	0	0	0	0
EP2	4	4	0	5	0	1	0	0	0	0	0	0
EP3	2	8	A	3	0	0	1	0	0	0	0	0
EP4	1	E	F	0	0	0	0	1	0	0	0	0
EP5	8	D	C	9	0	0	0	0	1	0	0	0
EP6	4	C	4	5	0	0	0	0	0	1	0	0
EP7	2	C	8	3	0	0	0	0	0	0	1	0
EP8	1	C	E	0	0	0	0	0	0	0	0	1
EP9	0	4	8	1	0	1	0	0	0	1	0	0
EP10	6	C	0	7	0	0	0	0	0	1	1	0
EP11	7	4	6	6	0	1	0	0	0	0	1	1
EP12	F	F	3	E	0	0	0	1	1	1	1	0
EP13	1	2	8	0	0	1	1	1	0	1	1	0
EP14	1	0	8	0	0	1	1	0	0	1	1	1
EP15	1	2	3	1	1	1	1	1	1	1	1	1

8bit코드로 가정된 운영체제에 로드된 소프트웨어 정보는 기본값 [11101111]을 적용하였다. 또한, 네트워크시스템은 일반적인 시간지연을 가지는 형태로 특수한 경우(peer to peer 링크, RS-232, 광통신 등)로 한정하지는 않았다. 네트워크상의 오류는 랜덤노이즈 형태를 적용하여 실험을 진행하였다. 그림 4에 시뮬레이션 실험과정의 예시를 나타내었다. CRC코드변환 방식은 CRC-16을 적용하였다. 상위 방식의 경우 8bit코드 변환용으로는 덧붙이는 코드가 많아 프로세서 과정상 불필요한 내용이 많아진다.

그리고 부주의한 소프트웨어의 변경이 발생하였음을 모의실험하기 위해 표 3과 같이 각 영역에 오류 패턴을 10분 주기로 입력하여 실험을 진행하였다.

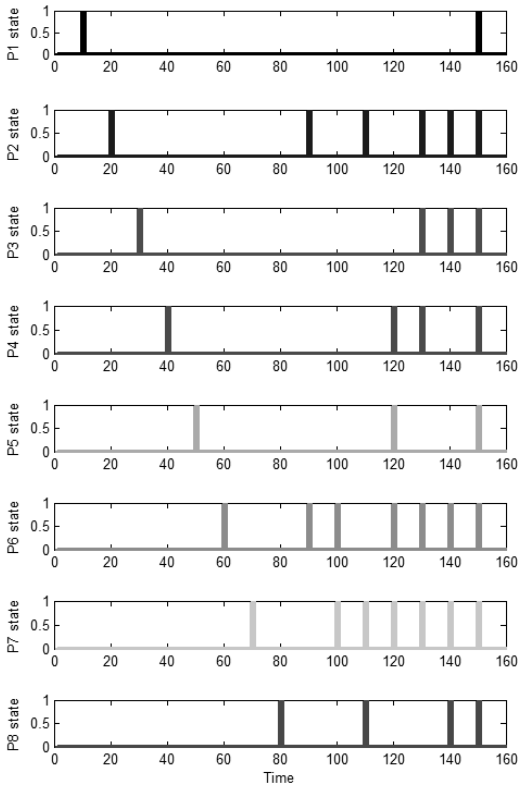

그림 5. 모의실험 결과
Fig. 5. Simulation Results.

이와 같은 시험환경을 통해 원전 계측제어 시스템의 제어용 소프트웨어가 부주의한 변경이 발생하여도 이를 감지할 수 있는지 모의실험을 수행한 결과는 표 4와 그림 5와 같다. 정상상태에서의 CRC 코드와 프로그램 코드 상에 문제가 발생할 경우의 CRC코드가 변경되어 이를 감지할 수 있음을 확인할 수 있다. 그리고 그림 5에서 각 프로그램 정보 코드의 상태 y축의 값은 0인 경우 오류가 없음을 의미하고, 1인 경우는 문제가 감지된 경우를 뜻한다.

모의실험을 통해 제어용 소프트웨어의 특정 메모리가 주기적으로 변경되어도 CRC 진단기능은 이를 정확히 탐지할 수 있음을 확인하였다. 이러한 소프트웨어 무결성 진단기능은 부주의한 소프트웨어의 변경을 미리 탐지하고, 기 설계된 프로세서의 정지 등 조치를 가능하게 함으로써, 원전 계측제어 시스템의 보안성환경을 구축하는 데 효과적인 방법이 될 수 있음을 확인하였다.

Ⅳ. 결 론

안전필수 기능을 수행하는 원전 계측제어 시스템은 연결된 계통의 부주의한 행위나 접근에 의해 개시된 사건이 동 계통의 신뢰성 있는 운영을 저해하지 않음을 보증할 수 있을 정도로 적절한 관리적 및 기술적 통제를 갖추어야 한다. 본 논문에서는 원전 계측제어 시스템의 제어용 소프트웨어에 대한 CRC 진단기능이 부주의한 변경 등을 탐지할 수 있는지 모의실험을 통해 평가하였으며, 제어용 소프트웨어의 특정 메모리가 주기적으로 변경되어도 이를 정확히 탐지할 수 있음을 확인하였다. 이를 통해 소프트웨어의 무결성에 대한 진단기능은 원전 계측제어 시스템의 보안성환경을 구축하는데 효과적인 설계방식임을 확인하였다.

본 논문에서 제시된 평가 방법 및 사례는 안전필수 기능을 수행하는 산업분야의 보안성환경에 대한 분석에 활용될 수 있을 것으로 기대된다. 또한, 원자력발전소 등 안전필수 기능의 제어 시스템 개발에 활용 가능한 기술기준 또는 지침의 개발에 활용될 수 있을 것으로 기대된다.

REFERENCES

[1] Y. Kang, K. T. Chong, “Safety Evaluation on Real Time Operating Systems for Safety-Critical Systems”, Journal of Korea Academia-Industrial Cooperation Society, Vol. 11, No. 10, pp. 3885-3892, Oct, 2010.

[2] K. S. Son, “Conceptual Design of Emergency Communication System to Cope with Severe Accident in Nuclear Power Plants”, Journal of The Institute of Electronics and Information Engineers, Vol. 51, No. 5, pp. 58-69, May 2014.

[3] KINS Regulatory Guide 8.13, Utilization for Digital Computers of Safety Systems, 2014.

[4] NRC Regulatory Guide 1.152, Rev.3, Criteria for use of computers in safety systems of nuclear power plants, July 2011.

[5] SH.Ye, J. Lyou, “Fault Tolerant Design of Universal Soft Controller for Advanced Power Reactor”, Journal of The Institute of Electronics and Information Engineers, Vol. 49, No. 9, pp. 279-286, September 2012.

[6] Y. Kang, et al., “Perspective on Secure Development Activities and Features of Safety I&C Systems,” Transactions of the Korean Nuclear Society Spring Meeting, 2015.

[7] J. S. Yun, Y. S. Kim, D. S. Kim, “Redundancy Method for Industrial Real-time Ethernet for NPPs,” Journal of The Institute of Electronics and Information Engineers, Vol. 48, SC. No. 4, pp. 71-79, July 2011.

[8] K. S. Son, “Performance Analysis of Emergency Communication System of Nuclear Power Plant using Markov Model”, Journal of The Institute of Electronics and Information Engineers, Vol. 51, No. 3, pp. 10-21, March 2014.

[9] H. Youm, J. Kwon, S. Yang, M. Rhee, “Performance Analysis of CRC Error Detecting Codes”, The Journal of Korean Institute of Communications and Information Sciences, Vol. 14, No. 6, pp. 590-603, 1989.

[10] J. Moon, J. Park, J. Lee, “Cyclic Redundancy Check Code Based High-Rate Error-Dettection Code for Perpendicular Recording”, IEEE transactions on magnetics, Vol. 42, No. 5, pp. 1626-1628, 2006.

[11] J. A. Davis, M. Mowbray, S. Crouch, “Finding Cyclic Redundancy Check Polynomials for Multilevel systems”, IEEE transactions on communications, Vol. 46, No. 10, pp. 1250-1253, 1998.

저 자 소 개

유 성 구(정회원)

2003년 전북대학교 제어계측공학과 학사 졸업.

2005년 전북대학교 제어계측공학과 석사 졸업.

2010년 전북대학교 제어계측공학과 박사 졸업.

2011년～현재 서남대학교 전기전자공학과 조교수

<주관심분야 : 인공지능, 제어시스템, 로보틱스>

설 남 오(정회원)

1991년 전북대학교 전기공학과 석사 졸업.

1998년 전북대학교 전기공학과 박사 졸업.

1997년～현재 서남대학교 전기전자공학과 교수

2006년～현재 서남대학교 산학협력단 단장

<주관심분야 : 제어계측, 원격제어, 원전시스템>