원전 안전통신망을 위한 TDMA 기반의 프로토콜 개발

論 文
55D-7-1

Development of TDMA-Based Protocol for Safety Networks in Nuclear Power Plants

金 東 勳† · 朴 聖 宇* · 金 政 憲**
(Dong-Hoon Kim · Sung-Woo Park · Jung-Hun Kim)

Abstract - This paper proposes the architecture and protocol of a data communication network for the safety system in nuclear power plants. First, we establish four design criteria with respect to determinability, reliability, separation and isolation, and verification/validation. Next, we construct the architecture of the safety network for the following systems: PPS (Plant Protection System), ESF-CCS (Engineered Safety Features-Component Control System) and CPCS (Core Protection Calculator System). The safety network consists of 12 sub-networks and takes the form of a hierarchical star. Among 163 communication nodes are about 1600 origin-destination (OD) pairs created on their traffic demands. The OD pairs are allowed to exchange data only during the pre-assigned time slots. Finally, the communication protocol is designed in consideration of design factors for the safety network. The design factors include a network topology of star, fiber-optic transmission media, synchronous data transfer mode, point-to-point link configuration, and a periodic transmission schedule etc. The resulting protocol is the modification of IEEE 802.15.4 (LR-WPAN) MAC combined with IEEE 802.3 (Fast Ethernet) PHY. The MAC layer of IEEE 802.15.4 is simplified by eliminating some unnecessary functions. Most importantly, the optional TDMA-like scheme called the guaranteed time slot (GTS) is changed to be mandatory to guarantee the periodic data transfer. The proposed protocol is formally specified using the SDL. By performing simulations and validations using Telelogic Tau SDL Suite, we find that the proposed safety protocol fits well with the characteristics and the requirements of the safety system in nuclear power plants.

Key Words : 안전통신망, 결정론성, 프로토콜, GTS, SDL, Validation

1. 서 론

현재 상용/산업 분야에서 적용되고 있는 데이터 통신 시스템들은 안전성에 기반을 두고 개발된 시스템이 거의 없는 실정이며, 무엇보다도 개발과정 또는 제작과정의 안전성 보장을 위한 검증에 취약점을 갖고 있다. 원전 시스템의 경우에는 안전 및 검증 특성 때문에 정보처리계통과 같은 비안전계통에 제한하여 통신망 개념을 적용해 왔으며 최근에야 보호계통과 같은 안전계통 적용을 위한 통신망이 도입되고 있다. 국외에서 적용된 안전 통신망의 경우 대부분 데이터링크 방식이나 필드버스 수준의 데이터 통신이 적용되고 있다. SIEMENS의 Teleperm XS는 정보망은 이더넷을 수정한 SINEC H1을, 안전망으로는 프로피버스 근간의 L2망을 적용하고 있으며 웨스팅하우스의 COMMON-Q는 안전 상태망으로는 토큰패싱 방식의 AF100을 사용하고 안전필수 데이터는 고속데이터링크인 HSL을 적용하고 있다. 이밖에도 프랑스의 N4 원전에 사용된 NERVIA는 토큰패싱 방식을 사용하여 안전망에 적용하고 있다. 이들 통신망은 대부분 안전필수 데이터 전송수단으로는 일대일의 데이터링크 방식을 사용하고, 안전 상태망은 기존 상용 또는 산업용 통신망을 일부 수정한 전용 프로토콜을 개발하여 원전에 공급함으로써 전송용량이 한정적이고 원전 고유의 특성을 만족하지 못하고 있으며 무엇보다도 검증성 문제를 포함하고 있다. 국내 원전의 경우 2005년에 상용 운전을 시작한 울진 5호기와 6호기 원전에 최초로 안전계통인 보호계통에 웨스팅하우스의 AF-100 통신망이 도입되었다. AF-100은 상용 토큰패싱 프로토콜의 일부 기능을 수정한 방식이나 전송용량이 1.5 Mbps에 불과하여 높은 전송용량이 요구되는 안전 제어계통에는 적용이 어렵다. 무엇보다도 AF-100은 안전성에 대한 검증 부족으로 안전필수 기능을 위한 데이터 전송 수단으로는 부적합하고 그 보다 낮은 등급의 안전관련 상태 데이터 전송에 국한하여 사용되고 있다 [1]. 이러한 점들을 고려할 때 원전에서 안전필수 기능을 위한 데이터 통신망의 개발이 요구되고 있으며 이를 위해서는 결정론적이며 명확하고 검증 가능한 데이터 통신 프로토콜의 개발이 선행되어야 한다.

기존의 원전 안전통신 구조의 경우, 안전필수 기능은 일대일 데이터링크를, 안전상태 기능은 다대다 버스구조를 갖고 있다. 본 논문에서는 안전필수와 안전상태 기능을 통합한 다대다 통신 구조를 제안하였다. 안전필수 기능의 고장-

† 교신저자, 正會員 : 韓國原子力研究所 責任研究員
E-mail : dhkim4@kaeri.re.kr
* 正 會 員 : 韓南大 情報通信工學科 教授
** 正 會 員 : 韓國原子力研究所 專門研究員
接受日字 : 2006年 4月 17日
最終完了 : 2006年 5月 30日

안전 (fail-safe) 요건에 가장 적합한 중앙 제어방식의 성형 구조를 설정하고, 기존에는 고려하지 않았던 다중 채널간 분리 및 격리를 위한 별도의 연계 노드를 포함한 구조를 제안하였다. 프로토콜의 경우, 기존의 안전상태 기능에 사용된 토큰패싱 방식은 안전필수 통신에서 요구되는 결정론성에 부적합한 특성을 갖고 있다. 즉, 전송권한을 전체노드가 분산 관리함으로 인하여 어느 한 노드의 고장에 대한 영향 확률이 높으며 무엇보다도 토큰의 분실이나 중복 시에는 비결정론적 특성을 보유한다. 본 논문에서는 전송권한의 제어를 결정론적 특성에 유리한 중앙 관리형으로 하고 시분할에 의한 고정적 할당 방식인 IEEE802.15.4의 GTS 방식을 채택함으로써 전송 구조가 확정적인 프로토콜을 제안하였다.

본 논문에서 제안한 프로토콜은 IEEE 802.15.4를 기반으로 하지만 세부 기능과 구조는 안전통신망에 적합하도록 모두 수정되었다. 주요 변경사항은, IEEE 802.15.4의 선택사항인 GTS 전송을 안전통신망의 주기적 공정 데이터 전송을 위한 기본방식으로 변경하였으며 개별 노드별로 할당하던 GTS를 전송 단계에 따른 그룹 노드에 대한 할당으로 변경하였다. 전송 지연시간의 불확실성을 지닌 간접 전송 방식은 삭제되고 모든 전송은 직접 전송으로 변경되었다. 또한 안전통신망의 기능적, 물리적 배치구조에 적합하도록 중간 교환기가 추가됨에 따라 이들 교환기의 MAC 스위칭을 위한 관리 기능이 새로 추가되었다. 기타, 결정론적 특성 또는 검증성에 위배되는 제반 기능은 모두 삭제하여 단순화 하였다. 무엇보다도, 본 논문에서 제시한 프로토콜은 정형 명세화에 의한 도달성 검증에 의하여 원전의 검증 요건을 만족하는 특성을 보유한다.

본 논문의 이하 구성은 다음과 같다. 2장에서는 안전통신망 구조 설계를 위하여 전체적인 통신망 설계 기준을 설정하고 노드 및 전송 트래픽 분석과 통신망 구성 요소 분석을 통하여 안전통신망 구조를 설계하고 설계요소를 확정하였다. 3장에서는 안전통신망의 토폴로지와 전송 구조를 설정하고 상용 및 산업용 통신 프로토콜의 원전 적용성 분석을 통하여 프로토콜에 대한 기본 구조를 결정하고 세부 프로토콜 사양과 특성을 제시하였다. 4장에서는 개발된 안전통신망 프로토콜 규격을 정형기법을 이용하여 명세화하고 명세 오류의 제거, 주요기능에 대한 시뮬레이션을 통한 교착상태, 차폐성 등에 대한 검증을 거쳐 최종적으로 validation을 통한 프로토콜 도달성 검증에 대한 결과를 제시하였다. 마지막으로 5절에서는 본 논문의 결론을 맺고 있다.

2. 원전 안전통신망 구조설계

원전 안전통신망은 그 특성상 데이터량과 구성 모듈의 수가 거의 고정적이며, 짧고 주기적인 데이터에 대한 단순 전송기능이 요구된다. 반면에 사고시 신속하게 정해진 응답시간이내에 작동해야 하는 안전계통 기능을 위하여, 전송 지연제한 시간을 엄격하게 준수해야 하는 경성 실시간 (hard real-time) 특성의 고속 전송이 요구된다 [2]. 안전통신망은 이러한 특성을 잘 만족할 수 있어야 할 뿐만 아니라 원전 안전계통의 필수 요건인 안전성과 검증성을 만족해야 한다. 안전성은 계통이나 기기의 신뢰성뿐만 아니라 구조적 결정론성과 고장 격리성을 포함한다. 따라서 안전통신망은 결정론적 통신구조, 명확한 분리 및 격리구조, 고 신뢰도 및 검증성의 4가지 설계기준을 만족할 수 있어야 한다.

2.1 안전통신망 구성

원전 안전통신망은 발전소보호계통 (PPS: Plant Protection System), 노심보호연산기계통 (CPCS: Core Protection Calculator System) 및 공학적안전설비-기기제어계통 (ESF-CCS: Engineered Safety Features-Component Control System)의 3개의 시스템에 대한 모든 데이터 전송 기능을 제공해야 한다. 안전통신망 전체는 발전소보호계통 24개, 노심보호연산기계통 33개, 공학적안전설비-기기제어계통 106개 등 모두 163개의 프로세서 모듈로 구성된다. 전송연계 분석 결과에 의하면 안전통신망은 각 주기마다 전체적으로 1600여개의 전송 연계를 수행해야 하는데, 이들 전송 연계는 안전망 내부와 외부 연계로 구성되며 내부 연계는 채널 내부, 계통 내부 및 채널간 연계로 구성된다. 데이터 전송주기는 50 msec와 500 msec의 두 가지 종류로 구성되며 안전성 요건에 따른 전송 데이터의 품질 요건은 SC (Safety-Critical)와 ITS (Important to Safety)로 나뉜다.

안전통신망은 안전계통의 다중 채널간 분리요건에 따라 채널 A, B, C, D 및 공통 채널을 분리해야 하며, 안전계통의 품질 등급 요건에 따라 SC와 ITS 데이터를 분리하고, 안전 정지를 위한 제어반 설비의 다양성 요건에 따라 주제어실과 원격정지실 통신망을 분리해야 한다 [3]. 또한, 가능하면 기능적 밀접성과 위치에 따른 연계를 고려하여 분할해야 한다. 이들 분할 기준에 따라 안전통신망은 품질 등급 SC의 안전필수망과 ITS의 안전상태망으로 분류되고 각각의 망은 개별 채널망 4개와 공통 채널망 2개로 구성된다. 표 1은 분할된 안전통신망의 구성을 정리한 것이다.

표 1 안전통신망 구성
Table 1 Composition of Safety Network

안전 / 채널	안전필수 통신망	안전상태 통신망
개별 채널망	안전필수 채널 A망 (SC-A)	안전상태 채널 A망 (SS-A)
	안전필수 채널 B망 (SC-B)	안전상태 채널 B망 (SS-B)
	안전필수 채널 C망 (SC-C)	안전상태 채널 C망 (SS-C)
	안전필수 채널 D망 (SC-D)	안전상태 채널 D망 (SS-D)
공통 채널망	주제어실 안전필수 공통 채널망 (SC-M)	주제어실 안전상태 공통 채널망 (SS-M)
	원격정지실 안전필수 공통 채널망 (SC-R)	원격정지실 안전상태 공통 채널망 (SS-R)

안전통신망은 표1과 같이 12개로 분할되어 구성되는데, 안전필수망과 안전상태망을 구성하는 각각의 채널망은 동일한 전송 연계사양을 갖는다. 또한, 주제어실과 원격정지실의 안전필수망과 안전상태망은 구성모듈 수나 전송 연계가 채널망 보다는 작다. 따라서 안전통신망을 위한 전송 연계사

양 분석은 안전필수와 안전상태에 대한 채널 A망을 분석하여 표2에 제시하였다.

표 2 안전상태 채널 A망(SS-A)과 안전필수 채널 A망(SC-A)의 전송사양

Table 2 Transmission Specification for SS-A and SC-A

전송사양		SS-A망	SC-A망
내부 통신노드 수량		33	24
외부 연계노드 수량	송신	9	4
	수신	3	7
총 전송 연계 수량		195	198
연계 데이터량 (비트)	최소	1	1
	최대	19,758	2401
	평균	1,419	219
	합계	286,536	43,417
전송 주기 (msec)		500	50
Raw 데이터 전송용량 (BPS)		572,872	869,340

2.2 안전통신망 설계요소 설정

표 3 원전 안전통신망 설계요소 설정

Table 3 Design Elements for Safety Network

설계요소			선정	선정기준
전송매체			광케이블	o 전기적 격리성 o EMI 검증성
토폴로지			성형	o 분리 및 격리성 o 고장 격리 및 진단성
프로토콜	물리계층	인코딩	광케이블 인코딩 방식	o 속도, 간섭, 잡음, 동기
		동기화	동기전송	o 전송속도
		멀티플렉싱	시간분할	o 결정론성
	데이터링크계층	링크구성	일대일	o 분리 및 격리성, 결정론성
		흐름제어	적용하지 않음	o 결정론성
		에러제어	CRC, 재전송 없음	o 결정론성, 신뢰성
		접근제어	고정할당	o 결정론성, 검증성

통신망 기본 설계요소인 전송매체, 토폴로지 및 프로토콜에 대하여 2.1절에서 기술한 설계기준에 따라 평가하고 설정하였다. 전송매체의 경우, 광케이블은 다른 전송매체에 비해 전기적인 격리성이 확실하며 환경 검증성 중 가장 민감한 EMI 영향이 없다는 결정적인 장점을 갖는다 [4]. 토폴로지는 분리 및 격리, 신뢰도 기준에 따라 성형을 선정하였다. 분리 및 격리성은 토폴로지 구조가 송신과 수신간의 물리적 분리와 전기적 격리가 용이한 구조를 갖추어야 하는 요건으로서, 중앙 장치에 의한 물리적인 분리 또는 격리가 가능한 성형이 유리하다. 신뢰도는 고장의 감지 및 격리성이 중요시 되며 중앙 스위칭 장치의 신뢰성이 보장된다면, 데이터가 집중됨으로 인하여 진단이 유리하고 고장시 해당 링크를 격리할 수 있는 성형이 강점을 갖는다 [5]. 따라서 원전 안전통신망의 토폴로지는 고 신뢰도를 갖는 중앙의 제어장치에 의한 성형이 적합하다. 프로토콜의 경우, 안전통신망은 계산 및 예측된 데이터량에 따른 고정적 전송특성을 보유하므로 흐름제어 기능은 요구되지 않으며, 전송지연시간의 불확실성 배제를 위하여 재전송 기능을 제외하였다. 전송 권한의 획득을 위한 접근 제어는 충돌 가능성을 갖는 랜덤할당이나 복잡한 알고리듬과 오류시의 비결정론성을 특성을 갖는 요구할당 방식보다는 결정론성과 검증성 기준에 명확하게 부합될 수 있는 고정할당 방식을 설정하였다 (표 3 참조).

3. 안전통신망 프로토콜 설계

2장의 분석 결과에 의하여 안전통신망은 성형의 토폴로지를 갖고, 각각의 링크가 일대일 접속인 구조가 적합하다. 안전통신망은 규모상 단일 성형 망으로는 부적합하므로 그림 1과 같이, 중앙교환기 (CSW, Central Switch)를 중심으로 기능과 현장구조에 따라 그룹교환기 (GSW, Group Switch)와 로컬교환기 (Local Switch)를 배치한 계층적 성형의 토폴로지를 갖도록 하였다.

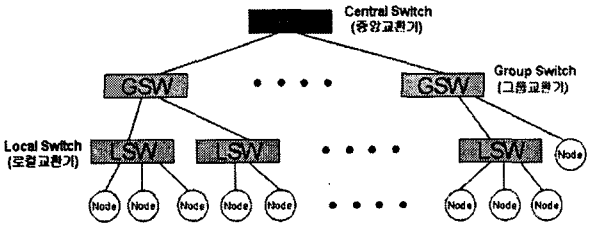


그림 1 안전통신망 토폴로지

Fig. 1 Safety Network Topology

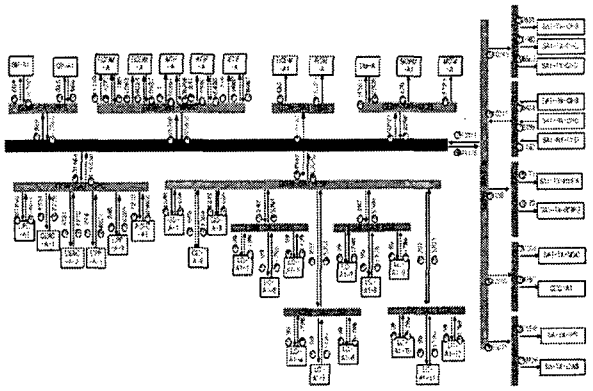


그림 2 안전상태 채널-A망(SS-A) 구성 및 전송구조

Fig. 2 Configuration & Transmission Architecture of SS-A

모든 통신노드는 자신의 계층에 맞게 할당된 교환기와 일대일 링크를 갖고, 데이터 송수신은 교환기의 중계방식에 의하여 주기적으로 수행된다. 설정된 구조에 따른 안전상태

채널 A망(SS-A)의 교환기 및 통신노드의 구성은 그림 2와 같다. 각 노드의 전송은 계층에 따른 교환기의 중계에 의해 한 주기 내에서 순차적으로 수행된다. SS-A망의 경우에는 그림 2에 표시된 바와 같이, ① 로컬교환기 노드의 전송, ② 로컬교환기, 그룹교환기 노드의 전송, ③ 그룹교환기의 전송, ④ 중앙교환기의 전송, ⑤ 그룹교환기의 전송, ⑥ 로컬교환기의 전송의 6단계로 한 주기의 전송이 완료된다.

모든 통신 링크는 전이중 (full-duplex) 방식이다. 따라서 각 전송 단계별로 각 노드 또는 교환기에 송신 권한을 부여함으로써 모든 데이터 교환을 수행한다. 그림 2의 링크 상에 나타난 숫자는 노드-교환기 또는 교환기-교환기간 데이터 연계로서 통신단계에 따른 데이터 전송 요구량이다. 그림 2에서 보면, SS-A망은 1개의 중앙교환기, 7개의 그룹교환기, 9개의 로컬교환기 및 45개의 통신노드로 구성된다. 그룹교환기는 계통 및 기능, 위치에 따라 분리 배치되고 로컬교환기는 현장위치와 연계에 따라 분리되어 배치된다.

현재, 상용 또는 산업용으로 적용되고 있는 프로토콜은 수백 종류가 넘으며 이중 국제 표준과 산업 표준으로 사용되는 것도 수십 종류가 존재한다. 이들 표준 프로토콜 중 원전 안전통신망의 프로토콜 계층 구조를 1, 2계층으로 한정하고 개방성이나 기술적인 완성도 또는 원전 특성과의 부합성을 고려할 때, 원전 적용이 가능한 대상은 이더넷, 각종 산업망에서 적용하고 있는 토큰 링과 토큰 버스 및 폴링 방식, 그리고 최근 무선망 적용 국제 표준으로 개발된 IEEE 802 계열 등이 존재한다. 원전 안전통신망에 적용될 프로토콜의 필수 요건은 안전성이다. 또한 안전통신망은 제어망, 경보망, 정보망 등과 연계되어야 하므로 호환성도 중요한 요소이다. 따라서 원전 안전통신망에 대한 적용성 분석은 안전성 요건의 핵심인 결정론성과 검증성, 그리고 호환성을 고려하여 평가되어야 한다. 표 4에 적용대상 프로토콜에 대한 분석 사항을 정리하여 제시하였다.

프로토콜 적용성 분석에 의하면, 현재 상용 또는 산업에서 이용되고 있는 방식을 원전 안전통신망에 직접 적용하기에는 부적합하다. 프로토콜 대상 중 필수 요건인 결정론성과 검증성을 고려할 때 폴링 방식과 IEEE 802.15.4의 보장형 방식이 안전통신망에 가장 적합하다. 폴링 방식은 중앙 마스터(master)에 의한 결정론적인 전송 특성을 보유하고 비교적 단순한 알고리듬에 의하여 검증성도 무난하나 전송 용량의 한계를 갖고 있다. 중앙 마스터에 의하여 모든 전송 핸드쉐이킹(handshaking)을 수행함으로 인하여 대역폭의 낭비가 심하고 이로 인하여 현장의 단순 기능 장치에 주로 이용되고 있는데, 근본적으로 고 전송량의 통신망으로는 한계를 갖는다. 또한, 모든 노드의 데이터 전송을 마스터의 능동적 제어에 의하여 수행함으로써 마스터의 성능과 신뢰성에 절대적으로 의지해야 하는 단점을 갖고 있다[12]. IEEE 802.15.4의 보장형 방식은 시분할방식에 의하여 고정적 전송 권한을 부여하기 때문에 결정론적 특성이 매우 우수하며 전송 알고리듬도 단순하여 검증성도 문제가 없을 것으로 보인다. 802.15.4의 단점은 무선망 적용 목적 때문에 물리계층이 안전통신망으로 부적합하고 전송용량도 매우 적다는 것이다. 그러나 물리계층을 개정하고 MAC 계층의 무선망 특성을 수정 보완 할 경우에는 안전통신망에 가장 최적화한 방식이 될 수 있다.

표 4 원전 프로토콜 적용 대상 분석

Table 4 Analysis of Applicable Protocols for NPP

종류	표준화	응용망	전송권한 부여 방식	결정론성	검증성	호환성
이더넷 [6]	IEEE 802.3	이더넷	경쟁할당 (CSMA/CD)	비결정론적	보통	우수
토큰링 [7]	IEEE 802.5	IBM 토큰 링, FDDI	요구할당 (Token)	토큰 분실시 비결정론적	어려움	어려움
토큰 버스 [8]	IEEE 802.4	MAP, ArcNet, Profibus	요구할당 (Token)	토큰 분실시 비결정론적	어려움	보통
폴링 [8,12]	산업 표준	마스터 -슬레이브	요구할당 (Polling)	결정론적	보통	보통
IEEE 802 무선망 [9]-[11]	802.11	무선 데이터 전송망	DCF :경쟁할당 (CSMA -CA) PCF :요구할당 (Polling)	DCF :비결정론적 PCF :결정론적	어려움	어려움
	802 .15.4	무선 센서망	비보장형 :경쟁할당 (CSMA -CA) 보장형 :고정할당 (GTS)	비보장형 :비결정론적 보장형 :결정론적	우수	어려움
	802 .15.3	무선 멀티 미디어 전송망			어려움	어려움

3.1 원전 안전통신망 프로토콜 구조

원전 안전통신망 프로토콜 구조는 IEEE 802.15.4의 MAC 계층의 보장형 시분할 (GTS) 방식을 기본 사양으로 선택하고 물리계층을 100 Mbps 이더넷 사양으로 교체한 구조로 설정하였다. 15.4는 전송 권한을 수퍼프레임 구조를 통해 설정하고 이를 비콘을 통하여 각 주기마다 통보 하는데, 각 노드의 전송은 기본 사양인 CAP (Contention Access Period) 구간에서는 CSMA-CA에 의한 경쟁할당 방식과 선택 사양인 CFP (Contention Free Period)에서는 GTS (Guranteed Time Slot) 방식을 이용하고 있다[11]. 원전 안전통신망은 GTS 전송을 기본사양으로 하여 주기적인 시스템 요구 데이터를 수용하며 이를 제외한 안전통신망 유지나 관리를 위한 명령 데이터 등의 이벤트 데이터는 15.4의 CAP 구간에 랜덤할당 방식을 적용하도록 수정한 구조를 갖는다. 또한, 15.4의 무선망 관련 및 비 결정론적 기능 특성은 모두 삭제 또는 수정하였다. 물리계층은 원전 타계통과의 호환성을 고려하고 기술적으로 이미 검증된 이더넷 100 Mbps의 사양을 채택하였다. 설정된 안전통신망 프로토콜 계층구조는 그림 3과 같이 물리계층, MAC 계층 및 상위 계층으로 구성된다. MAC 계층 중 management 기능은 교환 장치에 적용되는 선택 사항으로서 스위칭 관리와 중앙 교환장치의 비콘 관리 기능이 포함된다. 상위 계층은 전체 통신망의 구성과 관리 기능 또는 시스템 요구에 의한 응용 기능으로 구성된다. 본

논문에서는 계통 요구에 따른 상위 계층과 이더넷 표준 사양 [6]을 적용하는 물리계층에 대해서는 프로토콜 개발에서 제외하고 MAC 계층을 상세 개발 범위로 하였다.

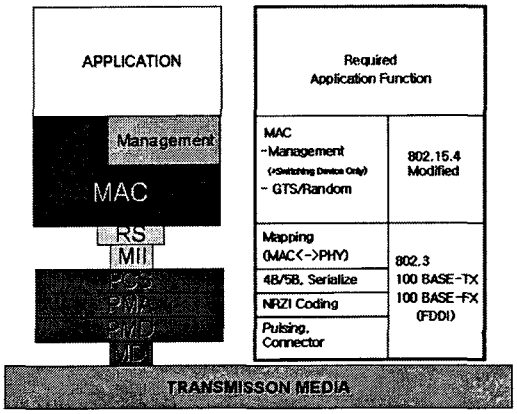


그림 3 안전통신망 프로토콜 계층 구조
Fig. 3 Protocol Stacks of Safety Network

3.2 안전통신망 프로토콜 사양

안전통신망의 프로토콜 사양은 IEEE 802.15.4의 MAC 프로토콜을 분석하고 이를 원전 안전망의 요건에 따라 삭제 또는 수정하여 설정되었다. IEEE 802.15.4는 CSMA-CA를 기본 전송 방식으로 하여 GTS를 선택 사양으로 하고 있으나 안전통신망은 모든 공정 관련 안전등급 데이터의 전송을 보장형 전송 방식인 GTS로 하고 기타 통신망 운영 관련 또는 비 안전성 이벤트 데이터는 랜덤할당 방식을 채용함으로써 결정론적 구조를 개선하였다. 이에 따라 수퍼프레임 구조와 관련 변수, GTS 할당 및 관리 기능과 관련 변수 등이 변경되었다. IEEE 802.15.4의 무선망 적용 물리계층 사양이 안전통신망은 유선망인 이더넷 100 Mbps 사양으로 변경함에 따라 IEEE 802.15.4의 MAC 기능 중 무선망 특성을 지원하는 기능은 모두 삭제 또는 수정 되었다. 이들 변경 사항에는 CSMA-CA 알고리듬의 삭제, IFS (Inter Frame Space) 변경, 채널 스캔 관련 기능 삭제 및 변경, PAN ID 충돌 관련 기능 삭제, 동기화 상실 관련 기능 변경 등이 포함된다. 안전통신망의 검증성을 위하여, 전이중 (Full-Duplex) 방식을 채택하고 전송 단계에 따라 그룹 GTS 할당 방식을 이용하고 IEEE 802.15.4의 기능 중 복잡하거나 투명하지 못한 기능들을 단순화 하였다. 이들 관련 사항에는 각종 송수신기 변경 관련 기능, GTS 할당과 관리, 망가입과 탈퇴, ACK 사용의 축소, 명령 프레임의 통 폐합 등이 포함된다. 안전통신망은 이들 개선 또는 변경사항에 따라 IEEE 802.15.4에서 제공하던 23개의 서비스 기능을 10개로 단순화하였으며 9개의 관리명령은 3개로 축소하였다. 또한 주소체계는 short address를 채택하고 안전통신망 특성에 따라 등급, 채널, 계통, 장치 및 프로세서로 분류하여 설정하였으며 비콘 프레임의 망 운전모드 식별 정보, 가입 명령 프레임의 GTS 할당 정보 등 세부 기능이 추가되었다. 안전통신망을 위한 변경 또는 개선 사항을 포함한 안전통신망 프로토콜의 기능사양을 정리하면 다음과 같다.

안전통신망은 수퍼프레임 구조를 이용하여 노드와 교환기의 전송권한 시간을 규정한다. 수퍼프레임은 중앙교환기(CSW)의 비콘 프레임 전송에 의하여 규정된다. 비콘의 주기와 수퍼프레임의 길이는 동일하며 1 msec ~ 1000 msec의 범위를 갖는다. 수퍼프레임은 3개의 부분으로 구성된다 : 비콘, FDTP (Fixed Data Transmission Period), VDTP (Varaible Data Transmission Period). 수퍼프레임은 비콘의 전송과 함께 시작하며, 비콘 구간은 모든 통신 노드의 비콘 수신 및 해석을 위한 시간을 보장할 수 있도록 한다. FDTP 구간에서는 안전망의 주기적인 공정 데이터를 할당된 GTS별로 전송한다. VDTP는 FDTP 이후에 곧바로 시작하여 수퍼프레임 종료기간까지 수행된다. VDTP 구간에서는 모든 통신 노드가 랜덤하게 접근 및 전송한다. VDTP 구간에 전송이 요구되는 데이터에는 서비스 기능에 요구되는 명령 프레임 및 응답 데이터 전송, 망 관리 및 진단용 데이터 전송 등이 포함된다. 수퍼프레임 구조에 대한 예를 그림 4에 제시하였다.

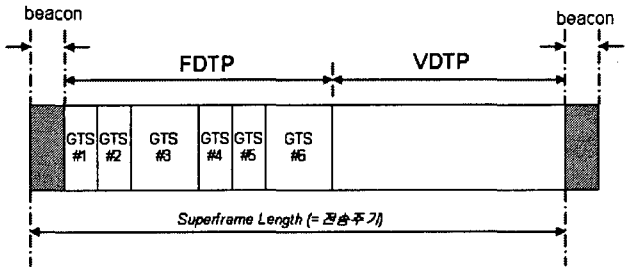


그림 4 수퍼프레임 구조 (예)
Fig. 4 Superframe Structure (Example)

안전통신망의 중앙교환기는 초기화 후 미리 설정된 정보에 따라 수퍼프레임을 구성하며, 망 운전모드를 비운전 모드로 설정하고 비콘을 전송한다. 각 노드 및 중간 교환기는 초기화 후 가입요청을 한다. 중앙교환기는 가입요청 노드의 목록을 확인하고 응답하며 각 노드는 응답 정보를 받아 통신 설정을 수행하고 대기한다. 중앙교환기는 가입 및 구성 정보에 따라 수퍼프레임을 새로 구성하며 운전모드를 운전 중 모드로 설정하고 비콘을 전송한다. 노드는 운전 중 모드가 설정된 비콘을 수신하면 비콘에 포함된 수퍼프레임의 정보에 따라 데이터 전송을 시작한다. 이후 중앙교환기는 설정된 비콘 주기에 따라 매 주기마다 비콘을 전송하며 모든 노드는 비콘에 포함된 수퍼프레임 정보에 따라 전송 동기화를 수행한다.

통신 노드는 초기화 후 대기모드에서 비콘을 수신하면 비콘에 표시된 가입 가능 여부를 확인하고 비콘에 표시된 VDTP 구간에서 중앙교환기에 가입요청명령을 전송하고 대기한다. 가입요청명령에는 자신의 주소 및 GTS 요청정보가 포함된다. 중앙교환기는 가능 자원을 확인하고 가입 허락여부를 결정한 후 가입응답명령을 전송한다. 가입응답명령에는 가입허락 여부와 거절 이유 및 GTS 할당 번호 등이 포함된다. 노드는 가입응답명령의 정보를 확인하고 대기한다. 운전 중 모드가 설정된 비콘을 받으면 곧바로 비콘의 수퍼프레임 구조에 따른 전송을 시작한다. 노드의 탈퇴는 두가지 경우가 존재한다. 하나는 중앙교환기가 탈퇴시키는 것이고 다른 하나는 노드 자신이 탈퇴를 원하는 것이다. 중앙교

환기가 탈퇴시킬 경우에는 VDTP 구간에서 노드에 탈퇴통지명령을 전송하고 ACK 없이 중앙교환기는 탈퇴된 것으로 간주한다. 노드가 탈퇴를 원하는 경우에는, 중앙교환기에 탈퇴통지명령을 보내고 중앙교환기는 ACK로 확인한다. ACK를 받지 못하면 재시도 해야 한다. 노드는 모든 망 관련 정보를 삭제함으로써 스스로 탈퇴하며, 중앙교환기는 노드에 대한 정보를 삭제함으로써 해당 통신 노드를 탈퇴시킨다. 탈퇴통지명령에는 탈퇴 노드의 주소와 탈퇴 이유가 포함된다.

안전망통신망의 동기화는 비콘 프레임을 수신하고 해독함으로써 수행된다. 노드는 전이중 구조에 의하여 항상 비콘 추적 상태이다. 유효한 비콘이 수신되면, 비콘에 포함된 정보를 상위계층에 전달한다. 정해진 주기 동안 2회 이상 비콘을 발견하지 못하면 MAC의 초기화를 통해 재 가입을 시도한다.

GTS는 통신 단계에 따른 어느 한 그룹의 노드 또는 교환 장치가 어느 시간 구간에 대한 송신 채널의 독점적 사용권을 갖도록 한다. GTS는 안전통신망 각 망의 구성에 따라 고정적으로 할당되며 VDTP 구간에 대한 최소 길이의 보장을 고려해야 한다. 노드 또는 교환기는 가입 요청시 전송 단계에 따라 미리 할당된 그룹 GTS 번호를 받는데, 기 할당된 GTS 길이를 초과하는 요청시에는 거절된다. GTS는 노드나 교환기의 그룹에 할당되므로 개별노드의 탈퇴에 의한 GTS 제거는 발생하지 않는다. 중앙교환기는 비콘을 통해 GTS별로 시작 시간과 길이 정보를 알려준다.

IEEE 802.15.4와 비교한 안전통신망 프로토콜의 주요 개선사항은 구체적으로 다음과 같다.

- IEEE 802.15.4는 CSMA/CA를 기본 사양으로 하고 GTS를 선택 사양으로 하고 있으나 안전통신망은 GTS를 기본 사양으로 채택함으로써 데이터에 대한 전송 보장과 전송 지연시간의 결정론성을 개선하였다.
- IEEE 802.15.4의 GTS는 개별 노드에 대하여 동적 할당 방식을 사용함으로 인하여 GTS 자원의 이용이 제한적이지만 안전통신망은 그룹 노드에 대한 고정적 할당 방식을 사용함으로써 GTS의 사용을 보다 효율적이고 안정적으로 개선하였다.
- IEEE 802.15.4의 망 운전 시작은 가입과 탈퇴 및 재구성이 불확실하고 혼합되어 있으나 안전통신망은 비콘 정보에 망의 비 운전모드와 운전모드를 구별하고 망 제반 상황을 확인 후 운전모드를 시작함으로써 초기 모드의 불확실성을 배재 하였다.
- 안전통신망은 계층적 성형 구조에 따른 교환 장치의 MAC 레벨의 스위칭을 위하여 관리 기능이 추가되었다.
- IEEE 802.15.4는 망 가입과 GTS 요청을 별개의 기능으로 제공하고 있으나 안전통신망은 이를 통합하여 단순화하고 GTS 할당이 명확히 이루어지도록 하였다.
- IEEE 802.15.4는 데이터 및 관리 명령 대부분에 ACK 기능을 포함하지만 안전통신망은 주기적 전송 특성을 반영하고 관리 명령을 축소함으로써 노드에 의한 탈퇴 요청의 경우에만 ACK를 포함하도록 하여 전송 지연시간 등의 결정론성 특성을 개선하였다.
- IEEE 802.15.4는 반이중 전송방식을 채택하고 있으나 안전통신망은 전이중 전송방식을 적용하여 트랜스미터의 상태 관련 제반 기능을 단순화 하고 데이터 수신 기능을 명확히 하였다.

3.3 안전통신망 설정 값

안전통신망 프로토콜을 위한 주요 설정 값은 표 5와 같다. 정확한 설정은 실제 제작 후, 정밀한 성능 시험 결과에 따라 재 설정해야 하며, 본 논문에서는 예비 분석 및 그에 따른 결과를 제시하였다. 표 5의 결과는, 전송 연계수를 포함한 프레임 오버헤드와 40% 성능 여유 및 30% 확장 용량을 고려하여 최대 연계 데이터량을 산출하고, 100 Mbps 링크 용량에 따른 전송 요구 시간, 노드 및 교환 장치 처리 지연시간, 전파 진행지연 및 전송 여유 등을 고려하여 msec 단위로 제시한 것이다. 표 6의 GTS 길이는 전송 주기를 고려하지 않은 순수 요구 GTS 길이이며, 하드웨어 설계 분석과 제작 후 성능시험에 의하여 정말 측정 후 전송 주기를 고려한 GTS 길이가 확정될 것이다. 그림 5는 설정값에 따른 안전필수 채널 A망 (SC-A)의 수퍼프레임 구조를 보여준다 (*비콘 전송 시간은 최대 추정치).

표 5 안전통신망 주요 설정 값
Table 5 MAC Constants for Safety Network

망 종류	수퍼 프레임 길이 (msec)	요구 GTS 개수 및 길이 (msec)						
		개수	GTS 1	GTS 2	GTS 3	GTS 4	GTS 5	GTS 6
SS-A (B,C,D)	250	6	1	2	4	4	2	1
SC-A (B,C,D)	25	6	2	2	2	2	2	2
SS-M	250	3	1	2	1			
SC-M	25	3	1	1	1			
SS-R	250	2	1	1				
SC-R	25	2	1	1				

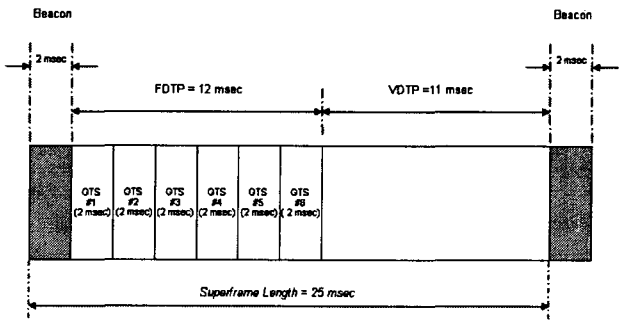


그림 5 안전필수 채널 A망 (SC-A) 수퍼프레임 구조
Fig. 5 Superframe Structure of SC-A

4. 원전 안전통신망 프로토콜 검증

원전 안전통신망의 프로토콜 오류는 치명적인 결과를 초

래할 수 있으므로 개발된 안전통신망 프로토콜은 체계적으로 검증되어야 한다. 본 논문에서는 검증 방법론에 따라 검증 절차를 설정하고 형식 명세 기법인 SDL (Specification & Description Language)을 이용하여 프로토콜을 명세화하고 이를 simulation과 validation 기법을 이용하여 검증하였다.

프로토콜 검증은 프로토콜 규격으로부터 표현된 프로토콜 명세의 정확성 (correctness), 안전성 (safety), 일관성 (consistency) 및 필연성 (liveness) 등의 특성을 알아보는 것이다 [13]. 요구된 특성을 만족하기 위하여, 안전통신망 프로토콜은 교착상태 (deadlock), 차폐성 (livelock) 및 도달성 (reachability)과 함께, 잘못된 상태전이 (missing state transition), 중복된 상태 전이 (redundant state transition), 실행 할 수 없는 상태전이 (non-executable state yransition), 상태의 모호성 (state ambiguity), 명세되지 않은 수신 (unspecified reception), 명세되지 않은 송신 (unspecified transmission) 등의 프로토콜 설계 오류를 검증 대상으로 하고 [5] 그림 6과 같이, 설계된 프로토콜 규격의 정형 명세화, 구문/의미 분석(syntactic/semantic analysis)을 통한 명세화 오류 검증, 주요 기능에 대한 시뮬레이션, 도달성 검증을 위한 validation의 4단계로 수행하였다.

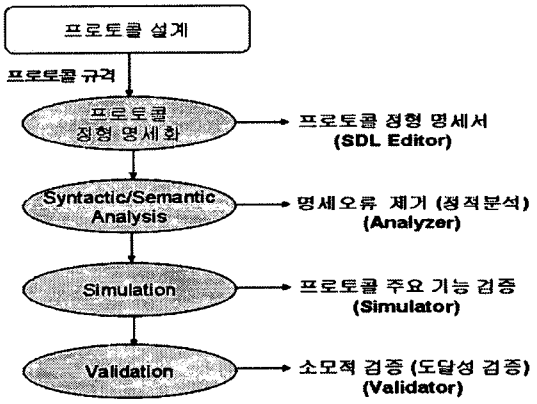


그림 6 안전통신망 검증절차

Fig. 6 Validation Procedure for Safety Network

4.1 프로토콜 정형 명세화

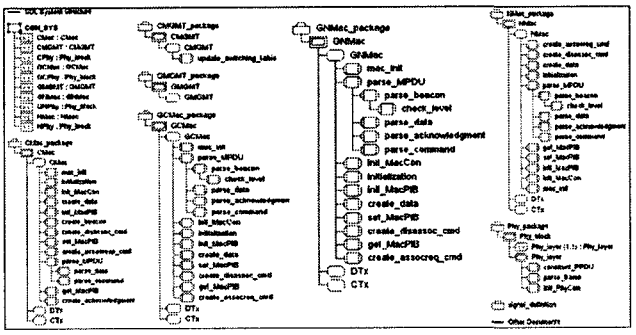


그림 7 안전통신망 프로토콜 SDL 명세파일의 구성

Fig. 7 File Composition of SDL Specification for Safety Network

본 논문에서는 정형 명세 언어인 SDL을 사용하여 프로토콜을 명세화 하였으며 명세 및 분석 도구로는 Telelogic사의 Tau SDL Suite를 이용하였다. 명세화는 전체 시스템 구성, PHY, MAC별 블록 구성 및 세부 프로세스 구성의 순서로 수행하였다. 작성된 프로토콜 명세에 대한 파일의 구성은 그림 7과 같으며, 시스템 구성은 그림 8과 같다. 그림 9에는 노드의 MAC 블록을, 그림 10에는 CSW MAC 프로세스 중 비콘 전송 부분에 대한 예를 제시하였다.

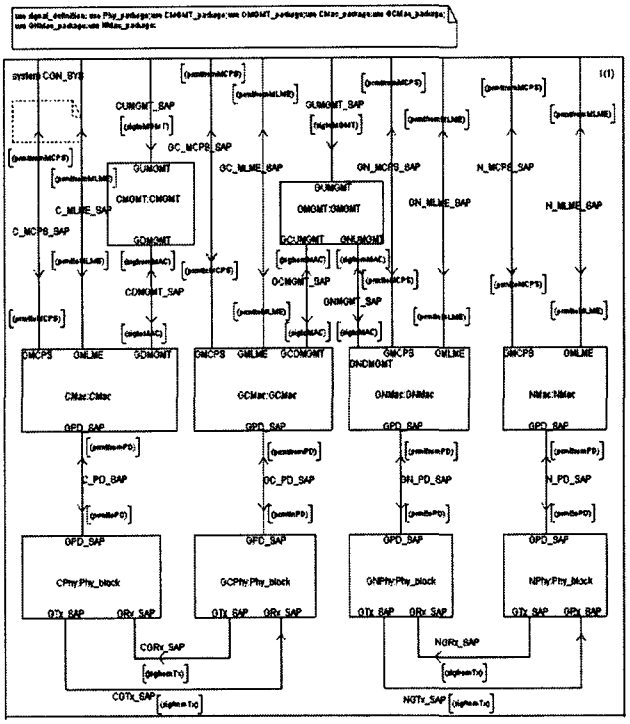


그림 8 시스템 구성

Fig. 8 System Configuration

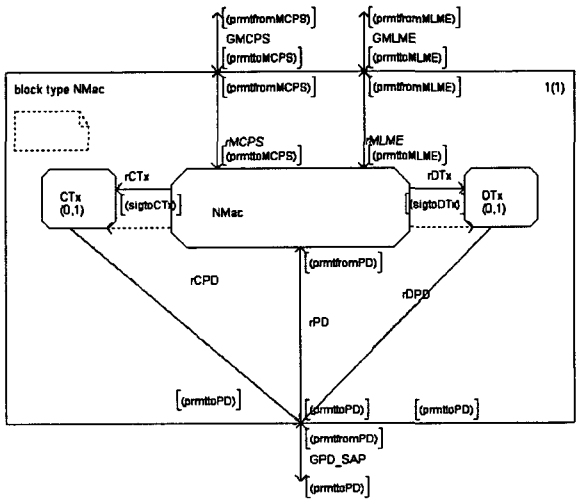


그림 9 노드 MAC 블록

Fig. 9 Block for Node MAC

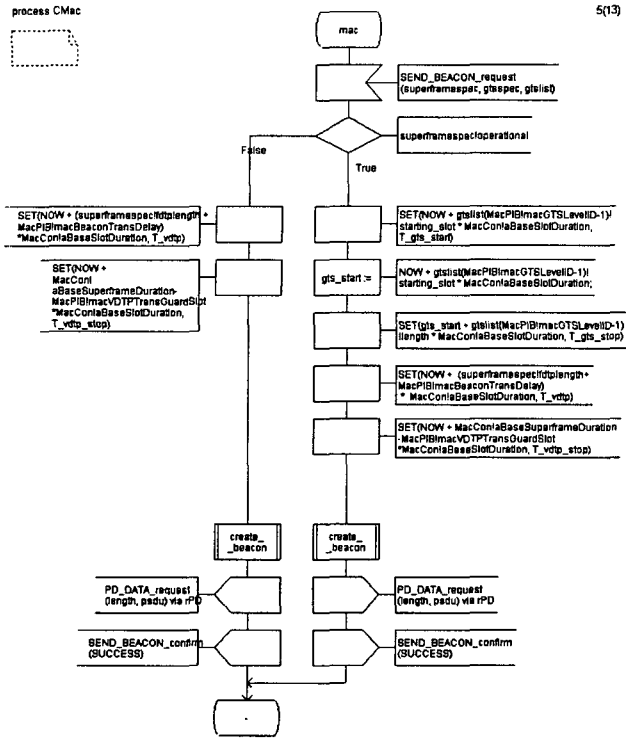


그림 10 CSW MAC 프로세스 중 비콘 전송
Fig. 10 Beacon Transmission Process for CSW MAC

4.2 프로토콜 검증

SDL로 명세화 프로토콜은 Telelogic사의 Tau SDL Suit의 정적 분석도구인 Analyzer를 이용하여 명세 오류에 대한 검증이 수행되었다. Analyzer는 SDL 명세서의 구문(syntax)과 의미 (semantics)에 대한 오류를 검사하는 과정에 사용된다. 정의되지 않은 문자나 기호 및 신호의 사용, 시스템이나 블록 구조의 입출력 지정 오류 등 명세서의 모든 표현과 구조에 대한 오류를 검사한다. 따라서 Analyzer를 이용한 분석 과정을 통해 명세서의 오류를 제거하고 검증된 안전통신망 프로토콜에 대한 SDL 명세를 획득하였다.

정적분석 도구인 Analyzer에 의하여 구문과 의미적 오류 검증이 수행된 프로토콜 명세는 시뮬레이션에 의한 동적 분석이 수행되었다. 본 논문에서는 Telelogic사의 Tau SDL Suite의 동적 분석도구인 Simulator를 이용하여 명세화된 프로토콜을 모델링 하고 시나리오에 의한 동작 상태를 MSC로 검증하였다. 시뮬레이션은 초기화, 비콘 전송과 수신, 망 가입과 탈퇴, 망의 시작과 GTS 설정, GTS 데이터 전송 등의 프로토콜의 주요 기능을 대상으로 하여, 명세에서 규정된 기능을 적절하게 만족하는지, 교착상태 (deadlock)나 livelock (차폐성) 또는 규정되지 않은 수신 등의 상태 오류가 존재하는지를 확인하고 제반 오류를 수정하였다. 그림 11은 시뮬레이션 결과에 대한 예로써, GTS 데이터 전송 기능에 대한 MSC 결과를 보여주고 있다.

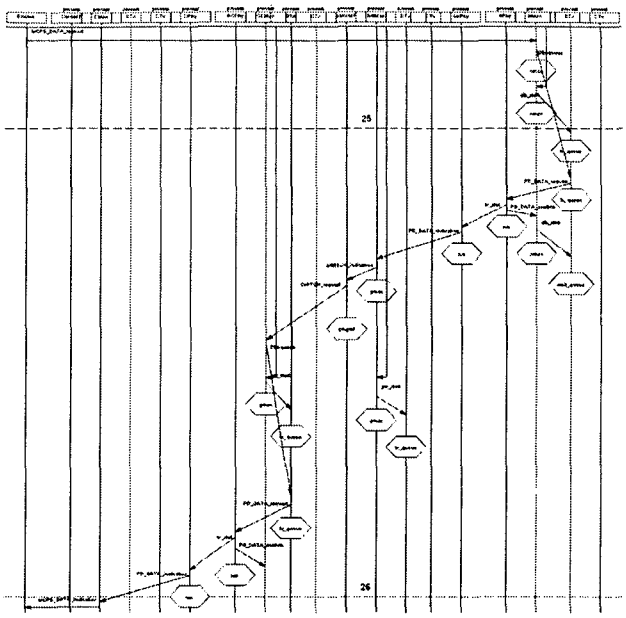


그림 11 GTS 데이터 전송 (Node to CSW)
Fig. 11 GTS Data Transmission (Node to CSW)

Validation 과정에서는 상태 공간 탐색 (state space exploration) 기술을 이용하여 명세화된 프로토콜의 행위를 검증하였다. 본 논문에서 이용한 자동 탐색 도구인 Telelogic사의 Tau SDL Validator는 단계별 행위 트리를 수동으로 추적하는 "Navigator", 무작위 탐색을 위한 "Random Walk", 전체 시스템의 탐색에 의한 도달성 검증을 위한 "Bit-State"와 "Exhaustive" 등의 기능을 제공한다, 본 논문에서는 Navigator와 Random Walk를 이용하여 예비 검증을 수행한 후 전체 시스템에 대한 도달성 검증을 수행하였다. 도달성 검증 도구 중 "Exhaustive"는 소모적 방법으로서, 모든 상태와 천이 정보를 저장하고 검사함으로써 매우 정확한 결과를 얻을 수 있지만 메모리의 한계로 인하여 규모가 작은 시스템에 적용할 수 있다[14]. "Bit-State"는 Hash 테이블을 이용하여 검사함으로써 메모리 한계 문제를 해결한 효율적인 방법이나 서로 다른 상태를 동일하게 인식할 수 있는 충돌이 발생할 수 있다. 명세화된 안전통신망 프로토콜의 SDL 시스템은 규모상 "Exhaustive" 방법으로는 검증이 불가능하기 때문에 "Bit-State" 방식을 사용하여 도달성 검증을 수행하였다. 본 논문에서는 CSW, GSW 및 노드별로 Bit-State 방식을 사용하여 명세화된 SDL 시스템의 초기 상태로부터 발생 가능한 모든 상태로의 도달과 오류 미 발생을 확인함으로써 개발된 프로토콜의 도달성 검증을 수행하였다. Validation 과정에서는 7개의 오류를 감지하고 수정하였는데, 그림 12와 같이, 대부분 전송된 신호의 사용이 정의되지 않아 발생한 오류이다. 그림 13은 제반 오류가 제거된 CSW의 Bit-State에 의한 도달성 검증 결과이다. 그림 13에서 "No of reports"는 Bit-State 탐색 수행 중 발생된 오류의 수를 나타낸다. 따라서 오류 보고서가 0이면 이는 명세화된 프로토콜에 오류가 존재하지 않음을 의미한다.

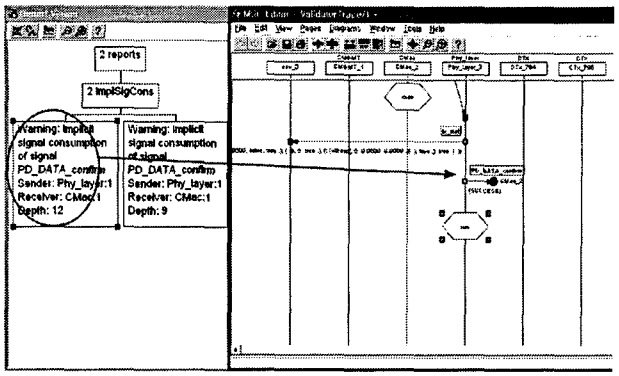


그림 12 Random Walk에 의한 오류 보고의 예
Fig. 12 Example of Error Report by Random Walk

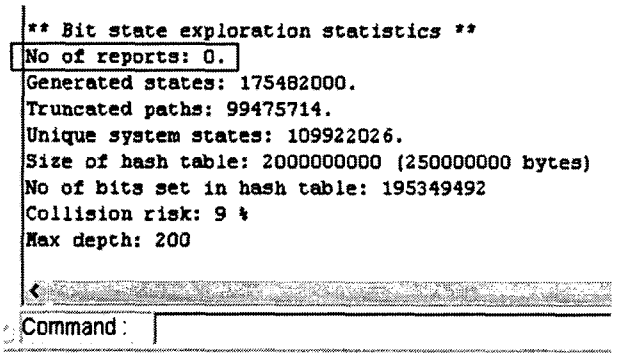


그림 13 Bit-State 검증결과 (CSW)
Fig. 13 Validation Result of Bit-Sate (CSW)

5. 결 론

안전통신망 프로토콜 개발을 위하여 안전통신망 구조를 설정한 후 프로토콜을 설계하고 이를 검증하였다. 설정된 안전통신망은 12개의 하부망으로 구성되며 성형의 토폴로지, 일대일의 연결 지향형 링크 제어 및 고정할당형 접근 제어를 기본 설계요소로 한다. 또한 계층적 성형으로 구성된 교환 장치 및 노드간의 1 주기 데이터 교환을, 전송 순서에 따른 시분할 고정형 전송으로 완료하는 전송 구조이다. 설계된 안전통신망 프로토콜은 IEEE 802.3 (Fast Ethernet) PHY와 수정된 IEEE 802.15.4 (LR-WPAN) MAC을 결합한 구조를 갖는다. 안전통신망에 불필요한 IEEE 15.4의 MAC 기능을 삭제하고 단순화하였으며 특히, IEEE 15.4 MAC의 선택 사항인 GTS 전송을 안전통신망의 주기적 데이터 전송을 위한 기본 방식으로 설정하고 GTS를 개별노드가 아닌 전송 단계에 따른 노드 그룹에 할당하였다. 설계된 안전통신망 프로토콜은 SDL을 이용하여 정형 명세화되고, Telelogic사의 SDL 분석 도구인 Analyzer를 이용한 명세 오류 검출 및 제거, Simulator를 통한 기능 및 교착상태, 차폐성 등의 상태오류 검출 및 제거, Validator를 이용한 도달성 분석에 의하여 검증되었다.

개발된 프로토콜은 원전 안전성의 필수 요건인 결정론적 구조와 검증성을 보유함으로 원전 안전통신망에 충분히 적용될 수 있을 것이다.

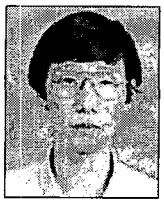
감사의 글

본 연구는 과학기술부의 원자력연구기술개발사업 일환으로 수행되었습니다.

참 고 문 헌

[1] C.H. Kim. "Design Specification for Digital Plant Protection System for UCN 5&6", N0696-IC-DS560, 1998.
[2] "Safety Assesment of Computerized Control and Protection Systems", IAEA-TECDOC-780, 1994.
[3] 김동훈, "원전 통신망 설계방법론 개발", KAERI/TR-700/96, 1996.
[4] Robert J Hoss, "Fiber Optics", Prentice-Hall, 1993.
[5] G. G. Preckshot, "Data Communications", NUREG/CR-6082, 1993.
[6] "Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications", IEEE Std 802.3-2002.
[7] Hans-Georg Göhring, "Token Ring - Principles, Perspectives and Strategies", Addison-Wesley, 1992.
[8] J.R. Pimentel "Communication Networks for Manufacturing", Prentice-Hall, 1990.
[9] "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications", IEEE Std 802.11-1999.
[10] "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)", IEEE Std 802.15.3-2003.
[11] "Wireless MAC and PHY Specifications for Low-Rate Wireless Personal Area Networks", IEEE Std 802.15.4, 2003
[12] "Plant Communication and Computing Architecture Plan Methodology", Vol 1.2, EPRI-TR-102306, 1993
[13] "정보통신 프로토콜 공학", 한국전자통신연구원, 1999
[14] Laurent Doldi, "Validation of Communications Systems With SDL", Wiley, 2003.

저 자 소 개



김 동 훈 (金 東 勳)

1961년 4월 5일생. 1984년 항공대학교 항공전자과 졸업. 2001년 한남대 대학원 정보통신공학과 졸업(석사). 2003년 동 대학원 박사과정 수료. 1987~현재 한국원자력연구소 책임 연구원

Tel : 042-868-8252
Fax : 042-868-8916
E-mail : dhkim4@kaeri.re.kr

박 성 우 (朴 聖 宇)

1962년 9월 13일생. 1985년 연세대 전자공학과 졸업. 1989년 Texas A&M Univ.(석사). 1991년 University of California 컴퓨터 공학과 졸업 (공학박사) 1992~현재 한남대학교 교수

Tel : 042-629-7398
E-mail : swpark@hannam.ac.kr

김 정 헌 (金 政 憲)

1976년 7월 22일생. 2003년 한남대 정보통신공학과 졸업. 2005년 한남대 대학원 정보통신공학과 졸업(석사). 2005~현재 한국원자력연구소 전문연구원

Tel : 042-868-8321
Fax : 042-868-8916
E-mail : xirius.kim@gmail.com