2001 추계학술발표회 논문집
한국원자력학회

SMART 안전계통 통신망 구조개발 설계요건
Design Requirements of Communication Architecture of SMART Safety System

박희윤, 김동훈
한국원자력연구소
대전광역시 유성구 덕진동 150

신용철
한국전력기술(주)

이재용
연세대학교

요 약

SMART 안전계통에 적용할 통신망의 구조를 설정하기 위해 상용 통신망으로부터 신뢰도, 성능에 관한 평가요소를 추출하고 적용 요구 수준에 따른 등급을 부여하였고 이를 바탕으로 안전 통신망의 핵심 요건인 예측 및 산출 가능한 결정론적 요건, 상태기반의 고정형 구조요건, 다른 시스템으로부터의 분리 및 격리요건, 신뢰도 요건, 증명 가능한 검증 및 확인요건을 제시하였다. 또한, 제시된 요건을 기반으로 통신망 설계요소 및 상용 통신망 기술 분석에 의하여 광케이블, 성형의 토폴로지, 동기전송, 일대일 물리적 링크와 연결지향형 논리적 링크, 고정할당 방식의 매체 접근제어를 설계요소로 선정하였다. 제안된 구조는 SMART 안전계통 통신망 설계에 기본 구조로 적용될 수 있다.

Abstract

To develop the communication network architecture of safety system of SMART, the evaluation elements for reliability and performance factors are extracted from commercial networks and classified the required-level by importance. A predictable determinacy, status and fixed based architecture, separation and isolation from other systems, high reliability, verification and validation are introduced as the essential requirements of safety system communication network. Based on the suggested requirements, optical cable, star topology, synchronous transmission, point-to-point physical link, connection-oriented logical link, MAC (medium access control) with fixed allocation are selected as the design elements. The

proposed architecture will be applied as basic communication network architecture of SMART safety system.

1. 서 론

SMART에서는 디지털기술을 이용하여 디지털 기기나 시스템간의 데이터전송 및 신호처리를 통해 전체적인 발전소의 가용율과 신뢰성이 제고할 수 있는 기술로 데이터 통신기술을 적용하고 있다. 디지털 기기 간의 데이터 전송을 위한 네트워크는 주어진 환경과 목적에 따라 신뢰성과 높은 성능의 정보전송이 이루어지도록 설계되어야 한다. 통신망의 설계는 통신망 구축에 필요한 분석을 통해 구현하게될 요구사항을 설정하고 기본 설계상수를 도출하여 기능적 구조를 분석하여 통신모델을 통해 통신망 구조개발을 완성한다. 통신망 구조를 설정하기 위해서 통신망의 목적을 수행하는데 요구되는 필요한 통신망 기능이 결정되어야 한다. 요구기능을 초과하는 통신망 구조는 불필요한 기능과 복잡성으로 인한 위험성과 성능결손이 존재하므로 최소기능 구현과 기능추가에 의한 장점이 균형을 이루도록 해야한다. 여기서는 통신망의 일반설계요건 중에서 안전성과 신뢰성이 가장 중요하게 취급되는 안전계통 통신망의 구조를 설계하기 위해 요구사항의 선정과 요구사항을 평가요소별 항목에 따라 설계요소별 평가를 수행하여 통신망 구조설정과 설계시 적용할 수 있는 안전계통 통신망 설계 필수요건을 설정하였다. 새로 설정된 설계 필수요건을 기준으로 통신망 설계요소를 평가하여 안전계통 통신망에 적용할 수 있는 전송매체, 토폴로지, 프로토콜, 망간접속장치를 선정하였고 SMART 안전계통 통신망 구조의 기본요소들을 설정하였다.

2. 안전계통 통신망설계 평가요소의 분류

통신망의 설계 또는 구현시의 평가 요소는 신뢰도, 성능, 운영의 크게 3가지로 분류할 수 있다. 신뢰도는 안전성, 보안을 포함한 신뢰성에 관한 모든 사항이며 성능은 용량, 확장성, 비용 등을 포함하는 시스템의 효율성을 나타내고, 운영은 이용자 연계와 관리사항을 포함하는 시스템 운전 사항관련이다. 이중 안전계통 통신망은 일반적으로 통신망에서 요구하는 비용 또는 효율성보다는 안전성을 최우선으로 하며 안전성을 보장하기 의해서는 시스템의 신뢰성, 결정론성, 검증성을 갖추어야 한다[1]. 또한 안전계통의 응용이 대부분 실시간 특성을 갖으며 이는 안전과 관련된 처리를 제한 시간 내에 반드시 수행해야 하는 경성 실시간 (Hard Real-Time) 특성을 의미한다. 안전계통 통신망 구조설계와 관련하여 신뢰도와 성능요소만 고려하며 각각에 대한 평가요소를 선정하고 최적의 통신망을 구현하기 위해 각 설계요소별 기술적합성의 판정과 적용을 위한 기준이 마련되어야 한다. 즉, 어느 설계기술이 어떤 평가 기준은 만족시키고 다른 평가 기준은 만족시키지 못할 때의 이 기술의 적합성 여부, 또는 두 개의 기술이 서로 비슷한 조건일 경우에 어느 기술을 선정할 것인가에 대한 판단 기준이 있어야 한다. 신뢰도와 성능에 대한 평가요소별로 분류하여 반드시 만족해야 하는 요소 (필수), 최우선으로 고려되어야 하는 요소 (최우선), 우선 고려 요소 (우선), 만족 권고 요소 (권고)의 4단계로 분류하였다[2]. 이들 적용기준은 통신망 구성 특성마다, 평가요소에 대한 분류등급이 다를 수 있으며 여기서는 안전계통 통신망 설계요건을 기준으로 선정하였으며 신뢰도와 성능에 대한 각 평가요소에 대한 적용등급을 표 1과 표 2에 나타내었다.

1) 필수 : 규제요건 또는 계통요건에 의하여 그 평가기준을 반드시 성취해야 하는 요소와 안전성이 요구되는 요건과 신뢰도 관련 중요요소

2) 최우선 : 필수요건을 제외한 사항 중 최우선으로 만족되어야 하는 평가기준으로 확장성, 표준화 등과 같은 설계목표 및 에러제어 관련 사항
3) 우선 : 필수와 최우선 두 기준을 제외한 성능관련 주요 요소로써 통신망 설계 기술사항 요소
4) 권고 : 통신망 이용 및 관리 측면에서 필요한 사항들에 대한 기준

표 1 신뢰도 평가요소의 등급

신뢰도 요소	요소정의	적용등급
1) 안전계통의 분리와 격리	규제요건에 의한 안전계통의 비안전계통과의 구조분리 및 상호접속의 격리요건	필수
2) 다중성	규제요건에 의한 안전계통의 채널 다중화 요건, 신뢰도 증진 및 고장대비를 위한 통신망 자체의 장치 및 경로의 다중화	필수
3) 다양성	하드웨어 및 소프트웨어를 포함한 통신망 장비 또는 경로의 공통원인고장 대비요건	우선
4) 하드웨어 및 소프트웨어 신뢰도	하드웨어 및 소프트웨어를 포함한 개별장치 및 시스템 전체의 평균고장간격 (MTBF)	필수
5) 가동률	통신망 시스템의 이용가능 확률	필수
6) 고장율	통신망 장치의 평균고장시간 및 전송에러율	필수
7) 제어의 결정성	구조 및 전송지연이 산출 가능한 결정론적 제어방법	필수
8) 접속 및 접근보안	장비에 대한 물리적 접근 및 시스템에 대한 접근성의 보호 및 제어	필수
9) 전송보안	전송 데이터의 보안, 통신망에서의 메시지 인증	필수

표 2 성능 평가요소의 등급

성능 요소	요소 정의	적용등급
가) 전송용량	데이터 전송속도 및 처리용량	필수
나) 전송지연	송신시각부터 수신을 성공하기까지의 시간간격	필수
다) 확장성	계통 및 기능의 추가에 대한 용이성과 용량	최우선
라) 유연성	접속성, 호환성, 교체의 용이성	최우선
마) 표준화	국제표준화의 정규 기술 및 개방형 제품의 판단	최우선
바) 전송효율	단위시간당 전송 가능한 정보량	우선
사) 채널 이용률	평균 채널 점유시간	우선
아) 에러제어	에러의 감지 및 복구 기능 능력	최우선
자) 유지보수	유지 및 보수를 위한 설비 및 용이성	최우선
차) 비용	설계, 설치 및 유지보수 비용	권고
카) 단순성	기술의 간결, 명료, 단순성	권고
타) 실시각 성능	실시각 제어 및 감시를 위한 요건 구비 및 기능능력	필수

3. 안전계통 통신망 필수요건

안전계통은 기능의 중요성으로 인해 일반 상용 또는 산업분야에 적용하는 방법과는 다른 엄격

한 절차와 요건에 따라 설계, 구현 및 검증을 수행해야 하고 안전계통에 적용되는 통신망도 안전계통의 특성 및 요건에 맞는 방식과 구조를 갖추어야 한다.
통신망 구조를 평가하기 위해 적용할 수 있는 주요 평가적용 요소는 신뢰도요소 중 분리 및 격리, 하드웨어 신뢰도, 에러율, 접속 및 접근보안에 대해 평가해야 하고 성능요소에는 유연성, 확장성, 전송용량, 전송지연, 보수 및 유지, 에러제어, 실시각 성능, 비용등을 고려해야 하지만 본 논문에서는 안전계통에 적용하고자 하는 통신망의 구조 설계에 적합한 평가요소들인 다중성, 고장율, 전송용량, 전송지연, 실시각 성능 등을 만족할 수 있는 통신망 설계요건을 다음과 같이 설정하였다[3][4].

1) 사건기반(Event-Based) 보다는 상태기반(Status-Based)이어야 한다.

안전계통을 위한 통신구조는 전송 노드수, 전송량, 전송경로 등이 고정적이어야 한다. 사건기반 구조의 경우에는 전송량과 전송지연시간의 가변성으로, 과도상태 또는 비정상 상태에서의 전송 예측이 매우 어렵다. 따라서, 고정된 데이터량과 전송로에 의하여 일정간격으로 전송하는 상태기반 전송구조를 갖도록 해야 한다.

2) 결정론적이어야 한다.

안전계통을 위한 통신망은 예측 가능한 명확한 전송구조이어야 한다. 비결정론적인 구조는 예상치 않은 메시지에 의한 전송지연시간의 초과나 미감지 에러에 의한 요구 전송기능을 상실할 수 있다. 결정론적 요건은 정상 상태 뿐만 아니라 에러 복구 상태시에도 고려되어야 한다. 전송 기능에 포함되는 불확실한 행위에 대한 요소를 배제하고 전송 에러에 대하여 명확한 감지 및 복구 절차가 마련되어야 한다. 비결정론적 특성이 나타나는 에러복구에 대해서는 그 조건을 정의해야 하며 비결정론적인 동작으로 인한 기능의 영향을 분석하고 심층방어 또는 다양성으로 보상됨을 정의해야 한다.

3) 통신경로에 대한 분리 및 격리 구조를 갖추어야 한다.

안전계통의 중복 모듈간과 비안전계통간의 데이터 전송은 물리적으로 분리되고 전기적으로 격리된 구조를 갖도록 하여 다른 모듈 또는 시스템의 고장으로 인한 영향을 차단할 수 있어야 한다. 이를 위해서는 전송로 연계 부분의 물리적, 전기적인 차단 기능과 함께 단방향 전송구조를 갖도록 해야 한다.

4) 신뢰도에 대한 정량적 근거를 제공할 수 있어야 한다.

통신망 신뢰도는 안전계통의 신뢰도 요건을 만족할 수 있어야 하며 이를 증명할 수 있는 데이터의 확보 (고장율, MTBF 등) 또는 분석, 시험에 의한 정량적 수치 및 근거를 마련할 수 있어야 한다.

5) 검증 및 확인이 가능해야 한다.

안전통신망을 위한 모든 구조, 하드웨어, 소프트웨어는 검증 및 확인이 가능해야 한다. 프로토콜은 도달성 분석 (Reachability Analysis)에 의하여 검증된 프로토콜 사양으로 구현해야 하며 위

험성 (Hazard)를 갖지 않음을 증명해야 한다. 또한, 케이블을 비롯한 모든 장치는 온도, 습도 등의 환경에 검증된 제품을 이용해야 한다. 검증 및 확인이 가능하도록 하기 위해서는 가능하면 이미 증명된 기술이나 방법론을 이용하는 것이 바람직하며, 불확실한 동작이나 검증이 불가능한 복잡한 방법론을 배제하고 단순하면서도 전송이 확실히 보장되는 구조로 설계해야 할 것이다.

4. 안전계통 통신망 설계요소 분석

일반적으로 통신망 설계 시 고려 또는 결정해야 할 설계요소는 전송매체, 토폴로지, 프로토콜, 망간 접속장치로 분류 할 수 있으며 설계요소에 대한 평가항목으로는 2장에 제시된 많은 평가요소들이 있지만 위에서 언급한 평가요소들 중 필수로 평가된 신뢰도요소와 성능요소들을 기반으로 설정된 안전계통 통신망 설계 필수요건 5가지를 적용하여 설계요소들을 평가하였고 그 결과를 표 3에 요약하였다.

1) 전송매체

통신망의 전송매체로는 트위스티드 페어, 동축케이블, 광 케이블 및 무선이 이용되고 있다. 안전통신망의 전송매체로서의 평가 기준은 요건에서 제시한 항목중 3) 분리 및 격리, 4) 신뢰도 데이터, 5) 검증 및 확인 요건이 적용 대상에 해당한다. 전송매체의 선정을 위해서는 전송간의 분리 및 격리 요건, 검증 및 확인 요건 중 환경 검증성이 가장 중요하다.

2) 토폴로지

안전통신망은 시스템 특성상 지역적 제한을 갖는 단일 규모 통신망이며 따라서, 근거리망의 통신망 토폴로지인 성형, 버스형 및 링형이 이용된다. 토폴로지의 평가는 요건의 1) 상태기반, 2)결정론적, 3) 분리 및 격리 4)신뢰도가 평가 기준으로 이용될 수 있다. 1) 상태기반 요건과 2)결정론적 요건은 결국 고정적이며 예측 가능한 구조를 갖추어야 한다는 것이며 3) 분리 및 격리요건은 토폴로지 구조가 전송과 수신간의 물리적 분리와 전기적 격리가 용이한 구조를 갖추어야 하는 요건으로서, 중앙 장치에 의한 물리적인 분리 또는 격리가 가능한 성형이 유리하다. 4) 신뢰도 요건은 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.

3) 프로토콜

안전계통은 단일규모의 실시간 제어 시스템의 응용에 이용되므로 복잡한 구조나 고 기능을 갖는 통신망을 요구하지 않는다. 따라서, 실시간 데이터의 확실한 전송이 목적이며 이는 OSI 7 계층 프로토콜 구조 중 물리계층, 데이터링크계층 및 응용계층의 3계층으로 구성함이 적절하다. 이중, 응용계층은 각 시스템의 기능과 목적에 따라 선택하게 되므로 여기서는 물리계층과 데이터링크계층에 대해 분석하였다[5].

물리계층이 제공하는 기능은 크게 인코딩, 동기화, 멀티플렉싱 및 매체연계의 4가지로 분류할 수 있다. 매체연계는 매체선택에 따른 여러 연계조건으로서 매체에 부합되는 일반적인 요건을 따르면 되고 인코딩 방식은 여러요소에 의하여 결정되는데, 안전통신망을 위한 인코딩은 전송매체에 따라 선호되며, 동기화 및 에러 구조를 만족시키며 비트에러율이 개선되는 일반적인 요건에 따른

다. 동기화는 비트의 시작과 끝의 동기화와 수신측의 비트 펄스 간격의 동기화가 요구되는데, 동기전송 방식이 유리하며 시스템의 구조에 따라 별도의 클럭라인 또는 자기 클럭킹코드를 선택할 수 있다. 멀티플렉싱은 물리계층 중 안전통신망의 특성에 가장 중요한 기능으로서, 안전통신망이 컴퓨터간 짧은 거리의 디지털 통신 목적이므로 시분할 멀티플렉싱이 이용되어야 하며 1)상태기반, 2)결정론적, 5)확인 및 검증 요건에 따라 통계적 시분할 보다는 동기 시분할 방식을 이용해야 한다. 멀티플렉싱은 공통매체의 전송권한을 위한 2계층의 매체접근제어 (MAC, Medium Access Control)와 밀접한 관계를 갖게 되므로 연계하여 결정해야 한다.

데이터링크계층의 기능은 링크제어, 흐름제어, 에러제어, 접근제어로 크게 구성된다. 링크제어는 물리적 링크 방식으로 일대일 링크 구조를 갖는 것이 안전통신망에는 적절하고 논리적 링크는 1)상태기반과 2)결정론적 요건에 의하여 연결지향형인 Connection-Oriented 방식의 결정이 타당하다. 안전통신망은 고정적, 결정론적인 방식으로 설계하므로 이미 예측 및 계산된 충분한 버퍼크기를 할당해야 하며 따라서 흐름제어가 요구되지 않도록 해야 한다. 에러제어 방식은 안전통신망의 경우 경성 실시간 특성을 갖고 있는 단순구조가 바람직하고 에러감지 후의 재전송시에는 데이터량과 전송지연시간의 변화로 1)상태기반과 2)결정론적 요건의 만족여부 및 5)확인 검증에 어려움을 겪게 되므로 통신망은 감지 후 단순경보 기능이 적절하다. 에러감지 기능은 신뢰성으로 판단할 때 CRC 방식이 적절하다. 접근제어 방식은 여러 노드가 공통매체 또는 접속 수단을 이용하는 통신망 특성상 이들 노드간에 이용권한을 부여하는 기능으로서 1)상태기반, 2)결정론적, 5)검증성 요건에 명확하게 부합될 수 있는 접근방식이 적합하다.

표 3 안전통신망의 설계요소 선정

설계요소			선정	비고	주요 평가기준
전송매체			광케이블		3, 4, 5
토폴로지			성형	응용 환경에 따라 유연성을 갖음	1, 2, 3, 4
프로토콜	물리계층	인코딩	매체에 따름		간섭, 잡음, 동기
		동기화	동기전송	별도의 클럭라인 또는 Self-Clocking	전송속도
		멀티플렉싱	시간분할		2
		매체연계	매체에 따름		
	데이터링크계층	링크제어	일대일, 연결지향		2, 3
		흐름제어	N/A	버퍼 용량 계산 요	1, 2
		에러제어	CRC	단순감지	2, 4
		접근제어	고정할당		2, 5
망간접속 장치			적용에 따름		2, 3, 4

4) 망간 접속장치

망간 접속장치는 안전통신망이 여러 하부망으로 구성되거나 안전 통신망이 다른 비안전 통신망에 전송연계를 갖는 구성에서, 이를 연계 및 접속하는 장치로 이용되는 설계요소이다. 망간 접

속장치에 대한 요건은 3)분리 및 격리 요건이 가장 중요하며 안전망간 또는 안전망과 비안전망간의 데이터 전송은 물리적 분리 및 전기적으로 격리되어야 하며 단방향성으로 구현해야 한다. 또한, 안전망간의 접속시에는 2)결정론적 요건에 따라 접속장치 내에서의 지연시간을 포함한 모든 동작이 예측 가능한 방식으로 구현해야 한다.

5. 제안하는 안전계통 통신망 구조

새로 설정한 안전계통 통신망 필수요건에 적합한 통신망 기본설계요소들에 대한 분석을 통해 SMART 안전계통 통신망의 구조에 적용될 전송매체, 토폴로지, 프로토콜, 망간접속장치를 결정하였다. 전송부하와 전송지연시간에 대한 분석을 통해 데이터 프레임의 크기를 최적화할 수 있고 안전기능이 충분히 발휘될 수 있는 실시간요건을 만족하는 전송용량을 산정할 수 있다. 그러나 상세한 전송주기, 프레임 크기, 전송량 등에 대한 선정은 적용할 계통의 설계확정과 적용 통신망의 프로토콜과 전송구조에 따라 결정되어진다. 표 3에 제시된 항목을 만족하는 성형의 토폴로지를 갖고 링크제어 방식의 일대일 연결지향형이며 고정할당형인 통신망 기술을 상용망을 이용해 분석하면 안전계통 통신망은 회선교환 방식의 TDM 버스 교환기술이 적합하며 근거리망의 디지털 데이터 전송에 해당하는 안전계통 통신망을 위해서는 기본 설계요소와 교환기술을 접목해야 한다. 제안하는 안전계통 통신망의 요소와 기술을 정리하면 다음과 같다.

1) 전송매체는 광 케이블을 이용한다.
2) 전송권한 부여는 고정할당형인 시분할방식을 이용한다.
3) 물리적 구조는 일대일 링크의 성형 교환방식을 이용한다.
4) 논리적 구조는 연결지향형을 이용한다.
5) 흐름제어 기능은 고정적인 데이터량에 맞는 버퍼크기를 할당함으로써 배제한다.
6) 에러제어는 단순감지인 Backward Detection의 CRC를 이용한다.
7) 상용 적용 기술은 동기식 TDM 버스 교환방식을 이용한다.
8) 인코딩, 매체연계는 상용의 광케이블 적용 방법을 이용한다.

6. 결 론

안전계통 통신망의 구축을 위한 요건을 도출하고 도출된 요건에 적합한 설계요소와 상용기술을 분석, 선정하였으며 선정된 설계요소와 기술을 기반으로 안전계통 통신망의 적용하기 위한 통신망 기본구조를 설정하였다.

일반 통신망에서 요구되는 경제성이나 효율성보다 안전계통 통신망은 안전성이 가장 중요한 요건이며 안전계통의 기능을 충분히 발휘할 수 있도록 하고 안전성을 고려한 통신망 설계는 주요 요건인 상태기반, 결정론적, 확실한 분리와 격리, 신뢰성 및 검증성을 만족하는 구조로 개발해야 한다. 주요 요건을 기반으로 통신망의 설계요소를 분석하여 전송매체는 광케이블, 토폴로지는 성형, 프로토콜은 일대일의 연결지향형인 동기방식의 고정형 접근제어를 선정하였고 선정된 설계요소를 만족할 수 있는 통신망 기술은 시간분할 방식인 TDM 버스 교환기술의 회선교환 방식이 안전계통 통신망에 적합한 것으로 판단하였다.

제안된 구조는 원자력플랜트 시스템 중 안전성이 가장 중요시되는 안전계통의 통신망 기본구조로 활용될 수 있다.

참 고 문 헌

[1] "Safety Assesment of Computerized Control and Protection Systems", Report of Technical Committee Meeting, IAEA-TECDOC-780, 1994

[2] 김동훈, "원전 통신망 설계기술", KAERI/AR-443/96, 1996.

[3] G. G. Preckshot, "Data Communications", NUREG/CR-6082, 1993.

[4] "정보통신 및 프로토콜 공학", 전자통신연구원, 1999.

[5] William Stallings, "Data and Computer Communications", Prentice Hall, 1997.