원자로 보호계통 데이터 통신망의 설계 적합성 분석

강영두, 고정수, 구철수, 김복렬
한국원자력안전기술원

Compatibility Analysis of Communication Networks for the Reactor Protection Systems

Young doo, Kang, Jung soo, koh, Cheol Soo, Goo, Bok ryul, Kim
Korea Institute of Nuclear Safety

Abstract - 원자력 발전소의 원자로보호계통(Plant Protection Systems)은 그 특성상 안전성과 신뢰성을 중시하며, 매우 엄격한 설계 요건을 요구한다. 또한 원자로 보호계통에 사용되는 데이터 통신망은 최악의 예상된 조건에서도 신뢰할 수 있는 성능을 보여야 하며, 실증 시험을 통해 확인되어야 한다. 이러한 특성을 고려하여 국산화과제로 개발 중인 원자로보호계통의 데이터 통신망은, 개방형 통신 프로토콜인 프로피버스(Profibus)를 적용하고 있다. 본 논문에서는 적용된 통신 프로토콜인 Profibus에 대한 성능 모델을 제시하고, 제시된 성능 모델을 통해 데이터통신망이 결정론적(Deterministic) 요건을 만족할 수 있는 성능 특성을 분석하고자 한다. 이를 통해 Profibus를 적용한 데이터 통신망이 요구되는 성능, 신뢰성, 독립성 및 건전성 요건을 만족하도록 하기 위한 설계 요건을 제시하고자 한다.

1. 서 론

원자력발전소의 통신 네트워크는 최근 일반 산업계에서의 급속한 네트워크 설계기술의 발달에 힘입어 성능 및 신뢰성 측면에서 많은 발달이 이루어졌다. 최근에는 원전 계측제어 시스템의 국산화 개발과제(KNICS)를 통해 원자로 보호계통이 PLC를 기반으로 설계되고 있다[1]. 이러한 원자로 보호계통은 바이스테이블, 동시논리, 자동시험 및 연계 프로세서 등으로 구성되어 있으며, 원자로의 정지 변수를 입력받아 사고 조건시 원자로를 안전한 방향으로 정지시키는 기능을 가지고 있다. 원자로 보호계통의 데이터 통신망은 결정론적인 프로토콜을 사용하여 실시간 성능을 만족해야하며, 채널간 연계시 물리적, 전기적 및 기능적으로 독립성 요건을 만족해야 한다[2]. 이러한 고 신뢰성의 통신망을 위해 현재 세계 표준화가 되어있는 Profibus를 적용하여 설계가 이루어지고 있다. Profibus 통신 프로토콜은 현재 산업용 자동화 분야에 널리 사용되고 있으나[3], 실시간 요구조건을 가지는 원자력 산업과 같은 신뢰성 및 안전성을 요하는 시스템에 적용하기 위해서는 설계 초기부터 세심한 사항에 대한 고려가 필요하다. 즉, 네트워크에 접속된 스테이션의 수나 메시지의 생성량, 각 스테이션에서 사용되는 통신 서비스 등에 따라 최적의 네트워크 성능 및 신뢰성을 보장할 수 있도록 설계가 이루어져야 한다[4]. 현재까지 네트워크 성능 변수의 선정에 관한 많은 연구가 이루어져 왔으나, 하지만, 필드버스의 특성상 이론적인 방법보다는 숙련된 경험을 바탕으로 하는 시스템 전체의 응답 시간 측정 등을 통한 통신 네트워크 설계가 이루어져왔다. 따라서, 본 논문에서는 원자로 보호계통의 데이터 통신망 설계에 있어 제안된 Profibus 통신 프로토콜의 성능 모델을 제시하고, 이를 통해 원자로보호계통의 데이터 통신망이 실시간 특성을 가질 수 있는 타이밍 분석을 위한 기법을 제시하고, 최적의 통신망 설계를 위한 방안을 제시하고자 한다. 궁극적으로 이러한 성능 분석을 통해 Profibus를 적용한 데이터 통신망이 요구되는 성능, 신뢰성, 독립성 및 건전성 요건을 만족하기 위한 설계 요건을 제시하고자 한다.

2. 본 론

2.1 KNICS 원자로 보호계통 설계 개요

KNICS의 원자로 보호계통은 4개 채널로 구성되며, 각 채널은 그림과 같은 구조를 갖는다. 원자로 보호계통 각 채널은 하나의 캐비닛으로 구성되며, 각 캐비닛은 전기적, 물리적으로 격리된 room에 설치되며, 각 room은 주제어실과 동일한 운전 환경을 갖는다. 원자로 보호계통 각 채널은 다음과 같은 기기들로 구성된다.

- 계열 1/2 비교논리(BP) 및 동시논리(CP) 프로세서
- 자동시험 및 연계 프로세서(ATIP)
- 캐비닛 운전원 모듈(COM)
- 기타 개시회로 및 하드웨어 장치들

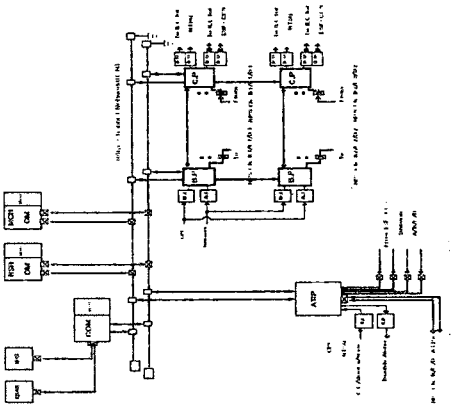


그림 1 . KNICS 원자로 보호계통 구성

각 채널의 비교논리 프로세서는 입력 모듈을 통해 취득된 안전 변수를 트립 설정치와 비교하여 트립 및 예비트립 상태신호를 출력한다. 이 출력신호는 SDL을 통해 동일 채널 및 타 채널의 동시논리 프로세서로 전송된다. 동시논리 프로세서는 동일 채널 및 타 채널의 트립 상태신호를 입력받아 2/4 동시논리를 수행하고, 트립 조건이 만족되면 원자로를 자동 정지하고 공학적안전설비 작동개시신호를 발생시킨다. 또한, 자동시험 및 연계프로세서는 비교논리 및 동시논리 프로세서의 기능이 정확하게 작동하고 있는지를 시험하며, COM은 각 채널의 운전상태와 유지보수 화면을 제공한다.

이러한 원자로 보호계통의 데이터 통신망은 다음과 같이 구성되어 있다.

- SDL(Safety Data Link) : BP의 트립 상태신호를 동일 및 타 채널의 CP로 전송
- ICN(Intra-Channel Network) : 각 채널 내에 설치된 디지털 제어기기와 캐비닛 운전원 모듈을 연결하며, 운전 상태 및 정보 신호를 교환
- ICDN(Inter-Channel Data Network) : 각 채널간의

정보를 공유하기 위한 통신망

각각의 통신망은 세계 표준화 Profibus를 적용하여 설계가 이루어지고 있으며, SDL은 Profibus의 데이터링크 계층을 이용하는 FDL(Fieldbus Data Link) 방식을, ICN 및 ICDN은 셀 단위의 통신을 지원하는 Profibus-FMS (Fieldbus Message Specification)을 적용하여 설계한다.

2.2 Profibus 설계 특성

Profibus는 필드레벨에서 Cell 레벨 네트워크에 연결되어 분산설치 되어있는 PLC 등의 serial fieldbus 시스템의 특성을 정의하고 있다. Profibus는 OSI 참조모델을 준용하며, 사용자 계층의 특징에 따라 DP, PA, FMS의 세 가지로 구분한다.

Profibus의 물리계층은 RS-485 규격을 적용하며, 토큰 버스 형태의 토폴로지를 사용한다. 전송 속도는 전송 길이에 따라 9.6kbps에서 12Mbps까지 지원이 가능하다. 데이터링크계층은 MAC, LLC 기능이 정의되어 있으며, 토큰 패싱(마스터/슬레이브, 마스터/마스터)과 폴링(마스터/슬레이브)방식을 사용한다. 마스터는 전송 권한의 설정을 위해 T_{TR}, T_{RR}, T_{TH}로 정의되는 3개의 타이머를 가진다.

T_{TR} : 토큰이 버스를 1회전하는데 예상되는 시간

T_{RR} : 실제 토큰이 1회전하는데 소요되는 시간

T_{TH} : 토큰을 가진 스테이션에서 전송에 허용된 시간

Profibus-FMS의 응용계층에는 FMS, LLI(Lower Layer Interface) 및 FMA7(Fieldbus Management App.7)이 포함된다. FMS는 통신객체와 응용서비스를 정의하며, LLI는 응용서비스와 FDL을 접속하는 기능을 정의하고 있다. 또한, FMA7은 네트워크 관리 기능을 정의한다.

일반적인 Profibus의 데이터 필드는 다음 그림과 같이 정의된다.

표 1. Profibus의 데이터 필드

SD	LE	LEr	SD	DA	SA	FC	DSAP	SSAP	DU	FCS	ED
68H			68H				3CH	3EH			16H

SD : start delimiter, LE : data의 길이,
SA : source address, DA : destination address
DSAP : destination service access point
LEr : Hemming distance에 대한 반복
SSAP : source access point
FC : frame control, FCS : frame check sequence
DU : data unit, ED : end delimiter, SC : Cod

2.3. 원전 통신망 설계 요건

원전 안전계통에 적용되는 통신 네트워크는 원전의 안전성을 고려하여 매우 심도 깊은 설계 요건을 가진다. 안전계통의 통신 네트워크는 관련된 모든 계통의 성능 요건을 만족하는지를 검토해야하며, 안전계통이 결정론적인가를 확인해야 한다. 원자로보호계통을 포함한 안전계통에 사용되는 데이터 통신계통은 event-based 구조보다는 state-based 구조로 설계되어야 한다. 또한, 안전 관련 통신 네트워크가 UREG/CR-6082에서 언급하고 있는 15가지의 성능 현안 사항에 대해 만족하는지를 확인해야 한다. IEEE Standard 7-4.3.2의 부록 G에서는 데이터 통신 네트워크의 독립성 요건에 대해, 안전 채널간의 통신이 단방향 및 양방향 통신일 경우의 독립성 요건과, 안전과 비안전 채널간의 단방향 및 양방향 통신이 이루어질 경우의 전기적, 물리적, 기능적인 격리 문제에 대해 정의하고 있다. 이러한 여러 요건을 기반으로 원전 안전계통의 통신망을 설계해야 하며, 이는 모 계통과 동등한 수준의 설계등급, 품질요건 및 기술기준을 적용 받아야 함을 의미한다.

2.4 통신 네트워크 성능 평가

원자력발전소 안전계통에 사용되는 디지털 계측제어계통의 응답시간 관점에서의 성능 평가는 첫째, 각 프로세서에서 측정된 변수에 할당한 시간 프레임 또는 timing deadline 제한시간과 통신 지연시간을 고려하여 합산한 전체 응답시간이 사고해석 또는 운영기술지침서(Tech. Spec)의 요구 값보다 적거나 같은지, 둘째 각 프로세서에서 각 트립 변수의 시간 프레임을 만족할 수 있도록 관련 변수들을 적절하게 scheduling할 것인지가 주요 관건이다. 첫 번째 사항은 시스템 구성 요소들에 대한 timing 분석을 통해 확인 및 검증되어야 할 사항이고, 두 번째 현안은 관련 변수들에 대한 실행 가능성 분석을 통해 확인되어야 한다.

Profibus에 접속되는 제어 루프에서 주기적 혹은 비주기적으로 발생되는 제어 데이터는 네트워크의 데이터 지연 시간이 시스템의 sampling 주기를 초과하지 않도록 하는 동시에, 전송되는 데이터를 sampling한 시점에서 제어 신호 혹은 정보 신호가 목적지까지 도달하는 시점까지의 경과 시간으로 정의되는 루프 지연 시간이 미리 정해진 한계치를 초과하지 않도록 설계해야 한다. 즉, 데이터 지연 시간의 초과로 인해 Profibus에 접속된 노드들의 성능 요구 사항을 만족시키지 못하는 경우가 발생할 수 있다. 이러한 경우를 대비하여 Profibus의 대역폭은 실시간 · 주기적 및 비주기적인 데이터들에게 적절히 할당되어 성능 요구 사항을 만족시키도록 설계되어야 한다. 이를 위해 Profibus의 타이밍 요건을 충족시키기 위한 파라미터 설정 기법에 대해 제안하고자 한다.

본 장에서 제안하는 KNICS 원자로보호계통의 통신망으로 설계하고 있는 Profibus-FMS에 대한 성능 분석을 위해, 네트워크의 타이밍 설정 기법을 제안한다. 이를 위해 다음과 같이 가정한다.

1. 네트워크 모듈의 송신 버퍼회로의 크기는 overflow가 발생되지 않고 모두 저장이 가능하다.
2. 원자로보호계통의 통신 에러는 존재하지 않는다.
3. Profibus 네트워크의 마스터 스테이션은 최소한 하나의 높은 우선순위 메시지 전송을 보장한다.

이를 위해 특정 마스터 스테이션 k에서의 연속적인 토큰 수신 시간을 T^k_{cycle} 정의한다.

2.4.1 네트워크 및 메시지 모델

특정 프레임으로 구성되어 있는 토큰이 논리적인 링 형태로 구성된 n개의 마스터 스테이션을 순차적으로 회전하면서 순차적으로 마스터 스테이션을 활성화 시킨다. 이 때, 전파지연, 토큰 전송 지연 등의 논리적인 링에서 발생할 수 있는 지연을 τ로 정의한다. i번째 높은/낮은 우선순위 메시지는 다음과 같이 정의한다.

$$Sh_i^k = (Ch_i^k, Dh_i^k), \quad Sl_i^k = (Cl_i^k, nlp^k) \qquad (1)$$

여기에서, Ch_i^k는 높은 우선순위 메시지를 수행하는데 필요한 최대 시간이고, Dh_i^k는 deadline과 관계있는 메시지 cycle을 의미한다. nh^k는 k번째 스테이션의 높은 우선순위 메시지를 의미하며, 또한, nlp^k는 높은 우선순위 메시지를 제외한 나머지 모든 전송 가능한 메시지를 의미한다.

Profibus-FMS의 시간분석을 위해 각 스테이션에서 토큰이 도착하였을 때, 각 스테이션은 큐에 저장되어 있는 높은 우선순위 메시지의 처리 및 전송이 가능하다고 가정한다. 즉, deadline 이내의 모든 스테이션에서 데이터 전송이 끝난다고 가정한다. 이를 위해 다음과 같이 정의할 수 있다.

$$\min_i\{Dh_i^k\} \geq T^k_{Cycle}, \ \forall_k \qquad (2)$$

여기에서, T_{Cycle}은 두 연속적인 토큰을 수신하는 최대 경과시간으로 정의한다. 각각의 스테이션이 모든 높은 우선순위 메시지를 전송할 수 있다면, T_{Cycle}의 범위는

$$T_{Cycle} \leq \Sigma_{k=1}^{n}\Sigma_{i=1}^{nh^k} Ch_i^k + Cl \times \Sigma_{k=1}^{n} nlp^k + \tau \qquad (3)$$

위 두 식을 이용해 다음과 같이 표현할 수 있다.

$$\min_{i,k}\{Dh_i^k\} \geq \Sigma_{k=1}^{n}\Sigma_{i=1}^{nh^k} Ch_i^k + Cl \times \Sigma_{k=1}^{n} nlp^k + \tau \qquad (4)$$

이 식을 통해 T_{Cycle}은 가장 작은 실시간 메시지 deadline보다 작아야 함을 알 수 있다.

다음으로, Profibus-FMS의 실시간 특성을 결정지을 수 있는 timing parameter를 설정하고자 한다. 이를 위해, k번째 스테이션에서 토큰이 수신되면, k번째 스테이션은 메시지를 전달하는 충분한 시간이 있다고 가정하면, T_{TR}은 다음과 같이 정의할 수 있다.

$$T_{TH} = T_{TR} - T_{RR} \tag{5}$$

$$T_{TR} \geq T_{Cycle} + max_{k=1,\ldots,n}\{\Sigma_{i=1}^{nh^k} Ch_i^k\} \tag{6}$$

이를 다시 풀어 쓰면,

$$T_{Cycle} \leq T_{TR} - max_{k=1,\ldots,n}\{\Sigma_{i=1}^{nh^k} Ch_i^k\} \tag{7}$$

과 같다.

결국 (3) 식과 (7)식을 통해 다음과 같이 정의할 수 있다.

$$T_{TR} \geq \Sigma_{k=1}^{n}\Sigma_{i=1}^{nh^k} Ch_i^k + \Sigma_{k=1}^{n}(nlp^k \times Cl^k) + \tau + max_{k=1,\ldots,n}\{\Sigma_{i=1}^{nh^k} Ch_i^k\} \tag{8}$$

위에서 정의한 식을 이용하여 네트워크의 실시간을 보장할 수 있도록 하는 Profibus-FMS의 T_{TR}의 lower bound를 찾을 수 있다. 이와 같은 계산을 통해 k번째 스테이션에서의 MAC(medium access control) 알고리즘은 다음과 같다.

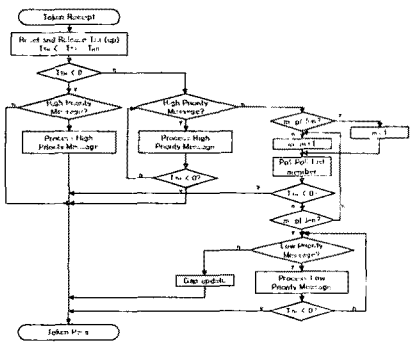


그림 2. T_{TR} 계산을 통한 MAC 알고리즘

이를 통해 네 개의 임의의 마스터 스테이션에서의 데이터 전송을 도식적으로 표현한 그림은 다음과 같다.

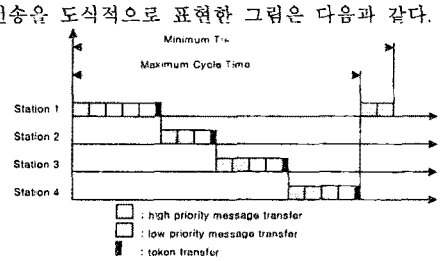


그림 3. 데이터 프레임의 전송

여기에서 $nh^{1,2,3,4} = 2$, $nlp^1 = 3$, $nlp^2 = 1$, $nlp^3 = 2$, $nlp^4 = 2$로 주기적인 데이터 특성을 가정하였으며, 이는 제어 대상의 플랜트 특성에 따라 정의할 수 있다. 원자로 보호계통의 데이터의 구조에 대해서는 현재 개발이 진행중이며, 경우에 따라 고정된 우선순위가 제공될 수도 있다. 이러한 특성의 Profibus 네트워크가 실시간 성능을 만족하기 위해 위에서 제시한 기법을 통해 네트워크의 타이밍 파라미터를 구하면 다음과 같다. 이를 위해 다음과 같이 파라미터를 정의하였다.

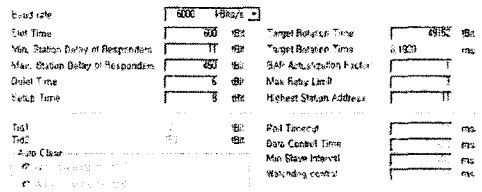
최대 메시지 길이 : 2ms
네트워크 전송 속도 : 1Mbps
logical ring latency delay, τ : 1ms

이를 통해 계산된 T_{TR}의 lower bound는 36.1ms임을 알 수 있다. 이는 주기적인 메시지 데이터를 갖는 네 개의 스테이션을 갖는 Profibus 통신 네트워크가 실시간 결정론적 특성을 만족하기 위해 정의할 수 있는 최소한의 토큰 회전 시간을 의미한다. 하지만, 위에서 제시한 모델은 네트워크 전송속도가 원자로 보호계통의 성능과는 차이가 있다.

따라서, 이러한 계산식을 근거로, 원자로보호계통 설계와 유사한 조건을 통해 재 계산해보면, Profibus-FMS 네트워크에서의 T_{TR}의 lower bound는 7.0ms로 계산되어진다.

표 2. 모의 실험을 통한 계산값

파라미터	설계상 계산 값
스테이션 수	12
Baud Rate	6000kbps
Baud Rate Watchdog	20ms
Message Length(Ch)	0.384ms
T_{TR}	7.0ms



이는 네트워크상에서의 메시지 생성량, 메시지의 길이, 오류제어 등이 정확히 고려하지 않은 경우이므로, 실제 네트워크 설계시에는 이러한 사항들을 고려하여야 할 것이다.

만약 특정 스테이션의 T_{TH}가 너무 크다면, 다른 스테이션들이 사용할 수 있는 T_{TH}가 작아지게 될 것이다. 따라서, 네트워크 설계 단계에서부터 시스템 전체의 응답시간 및 성능 특성, 우선순위 메시지의 생성량 등의 시스템 파라미터에 따라 적절한 T_{TR}을 설정함으로써, 메시지의 전송 지연을 최소화시켜야 할 것이다.

3. 결 론

본 논문에서는 원전 안전계통의 하나인 원자로보호계통 데이터 통신망에 대해 실시간 결정론적 통신망을 구현하기 위한 방법을 논하였다. 원자로 보호계통에 적용하는 Profibus-FMS에 대한 성능 모델을 제시하고, 이를 통해 결정론적인 특성을 만족하도록 하는 T_{TR} 선정 방법에 대해 제시하였다. 이러한 접근 방법을 데이터 통신망 설계에 반영하여 신뢰성 있는 통신망을 구축하는 방안을 제시하였다. 또한, 원자로보호계통 데이터 통신망이 전송 지연 없이 실시간성을 만족하여 원하는 신뢰성 및 건전성을 유지하도록 검증하고자 한다. 향후 모의 실험 및 실증 시험을 통해 원자로보호계통의 결정론적인 특성을 검증하고, 원자력 안전성에 부합하기 위한 관련 요건을 만족하는지 여부에 대해 검증하고자 한다.

[참 고 문 헌]

[1] 송승환 외, "디지털 보호계통 제어기기 통신망 기술", 제 2회 원자력학회 전기학회 공동 I&C 기술 Workshop, 2002
[2] KINS/RR 122, 데이터 통신 및 독립성 평가기술 개발, 2002. 3 한국원자력안전기술원
[3] M. Popp, The Rapid Way to Profibus DP
[4] NUREG/CR 6082, Data Communications, Lawrence Liver more national Laboratory, 1993