'98 한국원자력학회 논문집

한국원자력학회

칼리머 인간-기계 연계계통의 데이터 관리 및 통신망 개념설계

Conceptual Design of Data Management and Communication Networks for KALIMER MMIS

차 경호, 권 기춘

한국원자력연구소

대전광역시 유성구 덕진동 150

요 약

칼리머(Korea Advanced LIquid MEtal Reactor: KALIMER) 인간-기계 연계 계통(Man-Machine Interface System: MMIS)의 하부 계통으로서 기능적으로 밀접한 연관 관계를 갖는 데이터 관리와 통신망의 개념 설계에 관하여 기술하였다. 데이터 관리와 통신망의 하부 모듈에 대한 기능과 설계 요건이 설정되어 검토되고 있다. 실시간 데이터의 취득(acquisition) 및 검증(validation), 데이터 베이스 처리, 데이터 로깅이 데이터 관리의 하부 기능으로 설계되며, MMIS 계통과 통신망의 데이터 인터페이스 설계를 위해 칼리머 MMIS 의 최상위 설계 요건(Top-Tier Requirements)을 통신망 설계의 입력 데이터로 반복적인 상세 설계가 수행된다.

Abstract

This paper describes the design progress for data management and communication networks to be co-operated as subsystems in KALIMER MMIS. Main functions and design bases are being established and validated for functional modules of these subsystems. Real-time data acquisition and signal validation, databases, and data logging have been designed as each functional module of data management while data interfaces of communication networks have been designed with the system information from Top-Tier Requirements for KALIMER MMIS. The conceptual design shall be refined through the iterative and detailed one.

I. 서 론

칼리머 MMIS 의 데이터 관리 및 통신망은 그 기능 및 최상위 설계 요건이 설정되어, 이에 따른 모듈 단위의 기능과 세부 설계 요건이 개발되어 왔다[1,3]. 칼리머 MMIS 의 통신망은 4 계층의 duplicated redundancy 로 개념화 되었으며, MMIS 계통간 원활한 데이터 통신을 위한 계통 데이터 베이스와 데이터 저장 관리가 데이터 관리의 주요 모듈로 설계된다. 칼리머 MMIS 의 분산 구조에 따른 데이터 전송, 통신망, 데이터 및 통신망 관리는 기존의 중앙 집중식 데이터 처리 방식의 MMIS 설계에 비해 계통 설계의 초기 단계에서부터 더 많은 설계요소(design elements)를 고려해야 한다. 그리고, 디지털 기술, Commercial-Off-The-Shelf(COTS) 등 MMIS 구현 기술의 발전 속도가 급속히 진전되는 기술 특징을 반영해야 한다. 안전에 직접적으로 영향을 주는 데이터 전송 및 통신망의 설계는 심층 방어 설계 개념에 상응하는 하드웨어 설계에 중점을 두고, 비안전 기능은 소프트웨어에 의한 기능 설계에 더 많은 비중을 주어 설계된다. 데이터 관리는 각 계통으로부터 데이터를 취득하기 위한 데이터 취득 모듈, 통신망을 통해 MMIS 의 다른 계통과 통신을 위한 입출력 모듈, 각 계통으로부터 취득한 데이터의 변환 및 저장 관리를 위한 데이터베이스, 그리고 데이터 로그를 위한 데이터 로깅 모듈이 설계되었다. 한편, 통신망은 개념적인 4 계층 구조에 기반한 MMIS 계통과의 인터페이스 요건 및 계통간 데이터 통신 요건이 개발 중이다.

II. 데이터 관리 계통의 개념설계

2.1 설계 개념 (Design Concept)

데이터 관리 계통은 통신망을 통해 제어 계통, 원자로 보호 계통, 계측 및 센서로부터 생성되는 데이터를 Human-System Interface(HSI), Supervisory Control System (SCS), 그리고 Operation Management System(OMS)가 필요로 하는 데이터 형식으로 변환 처리하여 저장 관리하거나, raw data 를 그대로 전송하는 기능을 갖는다. 이러한 데이터 관리 계통은 데이터 입출력 및 수집 모듈, 계통간 효율적인 데이터 전송 및 통신을 위한 데이터베이스 관리 모듈, 그리고 유지 보수를 위한 데이터 로깅 모듈로 구성된다. GE 의 액체 금속로인 프리즘(PRISM)의 경우, 데이터 관리는 "데이터 관리 컴퓨터(각 NSSS 당 1 개의 컴퓨터)"가 "블록(block)" 데이터를 처리하도록 설계되었다. 칼리머 MMIS 의 데이터 관리 계통은 개념적으로는 프리즘의 블록 데이터 I/O 기능에 해당하는 데이터 관리의 하부 모듈로써 데이터 수집과 데이터 통신 기능을 정의한다.

2.2 데이터 수집 및 입출력

데이터 수집 및 입출력은 통신망을 통해 제어, 모니터링, 경보 및 운전 관리를 위한 원자로 보호 계통, 센서 및 계측계통의 측정치(measurements), 그리고 제어 계통으로부터 계통 데이터를 수집하고, 이러한 계통 데이터를 요구하는 HSI, OMS, SCS 로 데이터를 전송하거나 데이터베이스로 저장 관리한다. 그리고, 통신망을 통하지 않고 직접 HSI 등에 전송되는 보호 계통의 모니터링을 위한 안전 데이터는 hard-wired 로 설계되므로 데이터 수집을 위해 사용될 수 없어, 원자로 보호 계통의 계통 데이터는 Isolator 를 거쳐 L2 통신망에 인터페이스한다. Isolation 을 거친 원자로 보호 계통의 계통 데이터는 통신망을 통해 데이터 관리 계통에 의해 수집되어 다른 계통에 전송되거나 데이터베이스에 저장 관리하도록 설계된다. Data validation, data I/O, real-time constraints, clock synchronization, 그리고 interface 가 주요 설계 요소(design elements)로 설정되었다.

2.3 데이터 베이스 및 관리 모듈

데이터 관리 계통의 데이터 수집 모듈에 의해 수집된 계통 데이터에 대해 각 계통이 요구하는 데이터 요건을 만족하도록 데이터 형식의 변환, 저장 및 관리, 수정(update), 그리고 운전원의 요구(request)를 위한 로그 데이터의 관리를 수행한다. 이러한 기능을 위해 계통 데이터 베이스를 상태 테이블(state tables)로 유지함으로써, 계통의 초기화 및 재초기화(re-initiation) 등에 효율적으로 이용될 수 있다. 그리고, 계통의 로깅 데이터도 데이터 베이스 형태로 저장, 관리하도록 설계된다. 데이터/블록 데이터는 각 계통이 필요로 하는 데이터 요구에 적합한 표준 데이터 형식에 따라 데이터베이스(변수의 그룹화)를 정의하고, 이러한 데이터베이스의 저장, 수정, 관리가 용이하도록 설계된다. 데이터 베이스의 정의는 사용할 계통의 실시간 요구 조건 및 데이터 베이스로 유지, 관리할 때 더 좋은 성능을 나타내는 계통과 프로세스를 기준으로 정한다. 한편, 안전 변수와 안전-관련 변수(safety-related parameters), 비안전 변수에 대해 각각의 데이터 베이스를 정의하는 것도 요구된다. 계통 데이터 베이스 모듈 설계를 위해 real-time constraints, data conversion 및 formatting, 질의(Database query) 설계, 데이터 베이스 설계, 성능(Performance)이 설계요소로 설정되었다.

2.4 데이터 로깅

칼리머 MMIS 의 데이터 관리는 유지 보수를 위해 운전원 및 엔지니어에게 시간, Shift, 날짜(daily)별 데이터와 통계치 데이터를 제공해야 한다. 이러한 데이터의 표준에 따라 계통 데이터를 로그하는 것이 로깅 모듈의 주요 기능이다. 각 계통의 요구(requests)에 대해 동일

한 접근 방법으로 필요한 데이터를 사용하도록 설계되며, 표준 데이터의 제공을 위해 각기 다른 응용(주기적 접근 및 프린트, 비주기적 접근 및 프린트 등)에 적합한 구조화된 데이터베이스를 이용한다. 그리고, 계통 데이터의 로깅에는 “fail-safe” 저장매체로 설계해야 한다. log triggering, storage, response time 이 주요 설계요소로 설정되었다.

2.5 Configuration

데이터 관리 컴퓨터의 하드웨어는 결함 허용을 위한 그림 1 과 같이 dual-architecture 로 구성하고, 2 중의 통신망 구조와 기능적으로 상호 연동되게 배치한다.

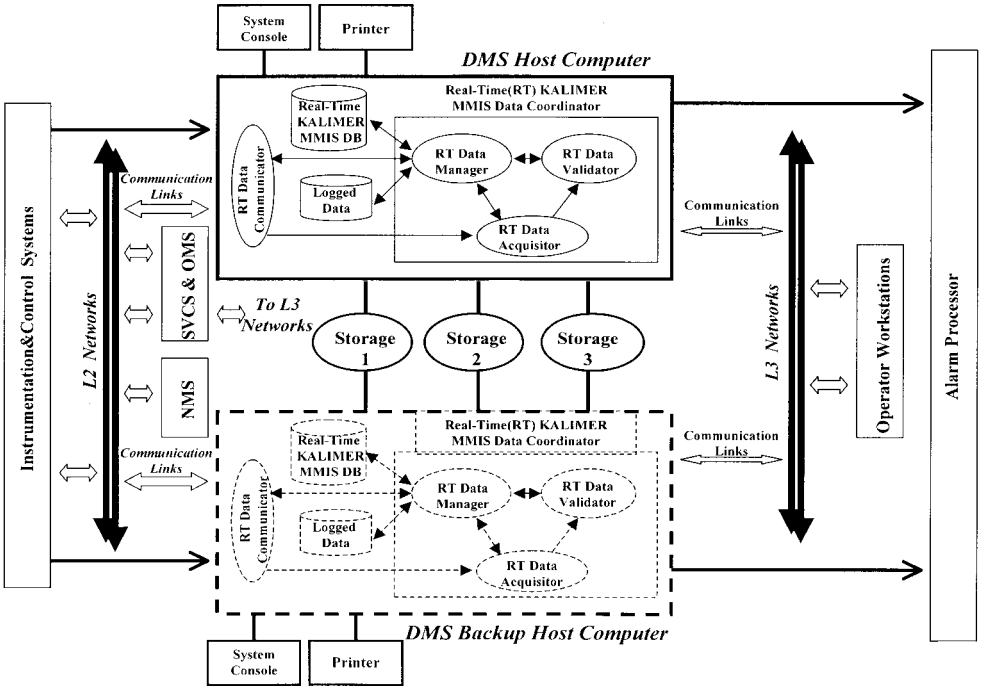

그림 1. 데이터 관리 계통 구조

데이터 관리 컴퓨터는 멀티 프로세서(CPUs) 및 redundant 저장 장치(fail-safe storage)를 갖도록 설계함으로써, 컴퓨터 자원(resources)의 고장에 대한 신뢰도를 보장할 수 있다. 운영체제를 포함한 시스템 소프트웨어는 가능한 COTS 를 설계에 이용하도록 한다. 각 모듈간 인터페이스(입출력 방식, 입출력 용량, 인터페이스 방식 등)과 통신망을 통해 다른 계통과의 인터페이스(데이터 통신 방식, 통신 용량, 인터페이스 방식, 부가적인 장치/모듈(Communication I/O cards))를 설계요소에 포함시킨다.

III. 통신망 개념설계

칼리머 MMIS 의 최상위 설계 요건(Top-Tier Requirements)을 통신망 설계의 기본 입력 데이터로 사용하였다. 이러한 통신망 설계를 위한 계통 정보의 분석을 위해 계통 데이터가 작성되었으며, 이러한 계통 데이터는 각 계통을 통신망과의 인터페이스뿐만 아니라, 통신망의 설계 요소를 결정하는 기본 데이터로 이용된다. 한편, 계통 데이터는 계통 데이터 베이스의 레코드/필드를 결정하는 데에도 활용된다.

3.1 MMIS 계통 데이터

MMIS 계통 데이터는 계통 이름(name or identifier), 안전 등급 분류(safety classification), 통신망을 통한 계통기능 (제어, 모니터링 등), 계통의 실시간 분류(경성, 연성 등), 계통의 물리적 위치, 계통의 외부 인터페이스(통신망에 통신 미디어(예, 통신 케이블)를 통해 계통을 직접 연결하는 직접 인터페이스 계통, 통신망에는 직접 연결되지 않으나 채널 등에 계통이 연결되어 통신망을 이용하는 간접 인터페이스 계통, 그리고 통신망에 연결되지 않으나 자체 망을 구성하는 독립 인터페이스 계통), 계통기기의 종류 및 기능, 계통의 입출력 데이터(처리방식, 입력 데이터, 출력 데이터, 데이터 전송방식, 데이터 set/종류), 신뢰도, 다른 계통과의 상호 연동 여부, 데이터 응답 시간, 통신망을 통한 중요한 운전 모드나 운전 조건의 존재 여부, 통신망과 연계된 고장 허용성 여부, 통신망과 연계된 공통 고장 원인(common-cause failure) 여부, 통신망과 연계된 다중성 여부, 주요 구현기술, 환경요인(cabling, wiring, 운전변수(operating parameters), EMI, 동작온도, 냉각 필요성 여부 등), 계통 초기화, 그리고 복구 및 유지보수 작업시 통신망 사용여부 등이 데이터 작성을 위한 항목으로 설정되었다. 이렇게 작성된 계통 데이터는 통신망 구조, 통신 프로토콜, redundant path, 통신매체, internetworking 등의 통신망 설계에 대한 요건을 결정하는데 중요한 역할을 한다.

3.2 주요 통신망 설계요건

3.1의 계통 데이터로부터 다음과 같은 설계 요건에 대한 검토 결과를 얻었다.

1) 안전 데이터 통신은 “상태기반 결정적(state-based deterministic), 다중(duplicated redundancy) 설계한다.
2) 안전망과 비안전망은 물리적으로 격리되게 설계한다. [그림 2]
3) 안전 데이터 통신망은 통신매체는 FDDI, 프로토콜은 표준 fieldbus에 준하여 설계한다.
4) 분산 실시간 제어를 위한 데이터 통신망은 최대의 신뢰도 및 성능을 갖도록 2중의 redundancy를 갖도록 설계한다.

5) 분산 실시간 제어를 위한 데이터 통신망도 상태기반 결정적 시스템으로 설계하며, 통신 프로토콜은 개방형 표준 FAP/MAP를 사용한다.

6) 데이터 망(L2)과 정보 망(L3)은 최대의 가용도(availability)를 갖도록 2중의 redundancy에 의한 TCP/IP 프로토콜로 설계한다.

7) 모든 통신망은 데이터 전송 에러에 대한 처리 및 복구 기능을 갖도록 설계한다.

최상위 설계요건의 계통 데이터와 3.2 의 설계요건을 반영한 통신망 구성은 그림 2 와 같다.

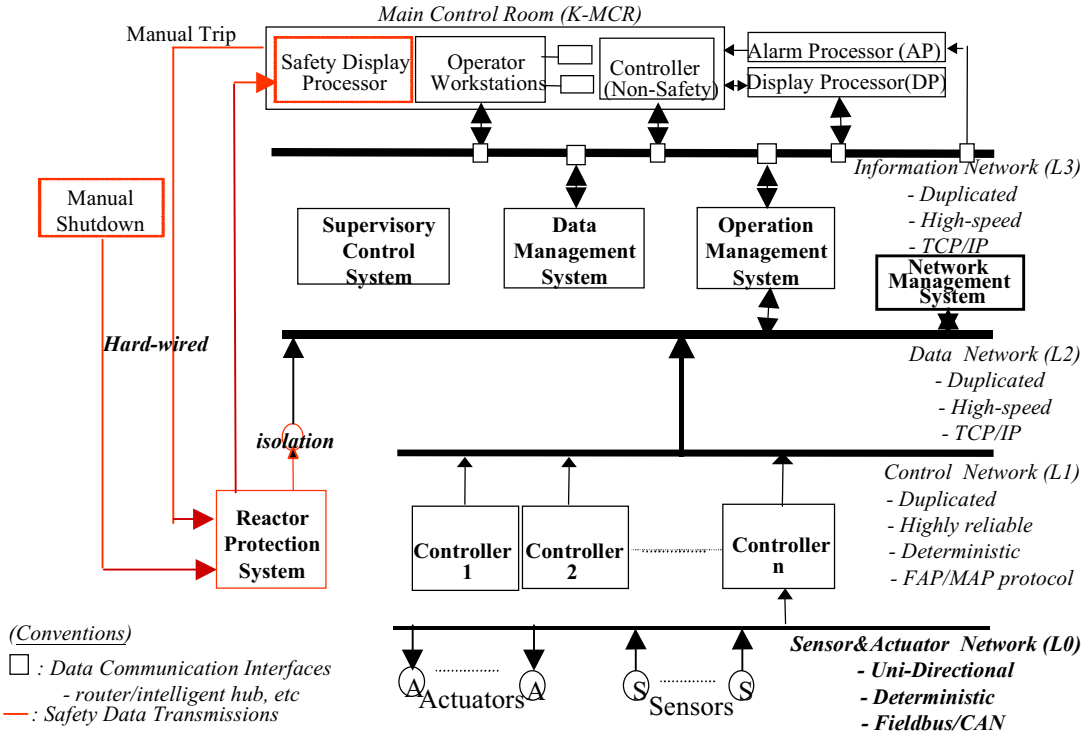

그림 2. 통신망 구조

IV. 결 론

칼리머 MMIS 는 미래형 원자로(advanced reactor)의 설계특징을 반영하여 설계되고 있다. 이러한 미래형 원자로의 MMIS 설계의 특징은 보수적인 안전개념(기계구조에 의한 심층방어 설계)을 수용하고, 아울러 COTS 등 첨단 기술을 반영한 MMIS 의 제어, 모니터링, 그리고 안전 기능을 동시에 고려해야 하는 기술적인 격차를 동시에 해결해야 한다. 이러한 이유로 인해 칼리머 MMIS 의 데이터 관리와 통신망 설계는 제어 및 운전에서의 자동화 정도에 부합하도록 하드웨어 설계에서는 심층 방어 개념을, 소프트웨어 설계는 공통 고장 원인을 최소화하기 위해 다양성 설계 개념을 적용한다. 한편, 미사일, 지진 등 알려진 외부 위

해도(hazards)와 마찬가지로 통신망의 설계에는 컴퓨터 바이러스의 침해, 통신 매체를 통한 예상치 않은 미래의 공격 무기 등에 대한 방어 대책이 EMI 격리 등 현재까지 알려진 안전 설계 요소에 덧붙여 고려되어야 하겠다. 결국, 미래형 원자로의 데이터 관리 및 통신망의 설계는 그 기능 설계뿐 아니라 내부 및 외부 위해도에 대한 심층 방어 설계도 중요한 설계 요소로 간주된다.

알 림

본 연구는 과학기술부의 원자력 연구개발 사업으로 수행되었음.

참고문헌

1. Cha Kyung Ho, et al., “Data Management and Communication Networks for Man-Machine Interface System in Korea Advanced LIquid MEtal Reactor: Its Functionality and Design Requirements(Vol.II),” Proceedings of the Korean Nuclear Society Spring Meeting, Suwon, Korea, pp.291-296, 29-30 May 1998.
2. Park Chang Kue, et al., “KALIMER Design Concept Report,” Annual Report No. KAERI/TR-888/97, 1997.
3. Kim Jung Taek, et al., “KALIMER MMIS Top-Tier Requirements (Rev.0),” Design Document No. KALIMER/IC000-DB-01/1997, 31 March 1998.
4. G.G. Preckshot, “Data Communications, “ NUREG/CR-6082, 1993.
5. U.S. NRC, “NUREG-0800: Data Communication Systems (Section 7.9),” 1991.
6. IEEE Power Engineering Society, “IEEE Application Guide for Distributed Digital Control and Power Plants (IEEE Std 1046),” 1991.
7. ABB-CE, ”NUPLEX80+ Advanced Control Complex Design Bases (Rev.1), “ NPX80-IC-DB790-01, 1994.
8. J. A. Scott, G.G. Preckshot, J.M. Gallagher, “Using Commercial-Off-the-Shelf(COTS) Software in High-Consequence Safety Systems (Manuscript),” UCRL-JC-122246, 1995.
9. 김 동훈 외, “원전 통신망 설계방법론 개발,” Technical Report No. KAERI/TR-700/96. 1996.