# BPLC기반 전력산업용 보안H/W모듈 구현

백종목, 임용훈. 최문석
한국전력공사

# The Implementation of BPLC based AMR security Module

Jongmock Baek, Chunghyo Kim, Moonsuk Choi
KEPCO Research Institute

ABSTRACT

스마트 그리드환경에서 전기를 소비자에게 공급하는 스마트 Place영역에서 통신망은 국내에서 기술적인 여건상 전력선 통신기반의 인프라가 가장 빠르게 원격검침서비스에 활용되고 있다. 원격검침 시스템[1]은 댁내의 계량기와 전주상의 데이터 집속구간은 전력선 통신방식으로 구성되고 상위 서버와는 인터넷 망으로 구성되어 있으며 통신 토폴로지 구성측면에서 전력선통신 모뎀, 데이터집속장치 그리고 중앙의 서버로 3Tier구성 체계를 가지고 있으므로 여기에 적합한 보안 아키텍처의 구성이 필요하다. 본 논문에서는 전력선 통신망 기반의 원격검침 시스템에 적합한 보안기술을 설계하고 구현 하였다

## 1. 서 론

본 논문에서는 전력선 통신 (Power Line Communication, PLC) 을 이용한 원격검침시스템에 적용할 보안시스템을 설계하고 내부 기능을 H/W 보안모듈로 구현하고자 한다. 한전의 인증 및 검침서버[2]와 말단의 PLC 모뎀 혹은 개별 검침기 사이에 위치하는 IRM (Integrated Regional Manager) 간에 수집된 검침값을 안전하게 전송하기 위한 모듈구성과 통신절차를 정의하였다. 말단에 위치한 PLC 모뎀과 네트워크간 인터페이스는 물리 계층 (PHY) 과 접근제어 계층 (MAC)만으로 구성되며 별도의 암호코어 (Crypto Core)를 가진다. IRM도 이들과 동일한 하드웨어사양을 갖는다. IRM은 인증 및 검침서버에게 HFC(Hybrid Fiber Coaxial)망을 이용하여 암호화된 검침값을 전송하며 통신망에 독립적으로 보안기능을 보장하는 프로토콜을 적용하였다.

## 2. 전력IT용 원격검침 보안H/W 플랫폼 개발

### 2.1 원격검침용 보안시스템 개요

전력선 통신을 이용한 원격검침 보안서버는 크게 기기 인증[1]을 위한 CA, 기기 등록 및 UID,공개키,인증서 관리을 위한 RA, 검침데이타를 복호화 및 관리하는 MA로 구성된다. 검침데이터가 보관된 AMR서버와 통합망관리 기능을 수행하는 NMS서버와 연계하여 전체 인증/보안 진행을 하여 전력선통신을 이용한 원격검침 시스템에 있어 안전한 데이터 관리 및 신뢰할 수 있는 기기 인증을 하게 된다

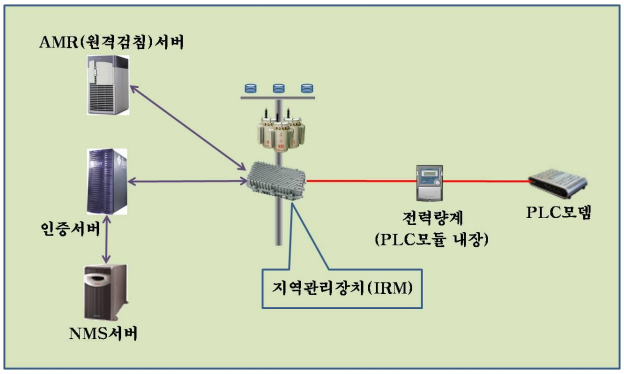


그림 1 보안 PLC망기반 원격검침시스템 구성도
Fig. 1 The AMR system based on security BPLC network

### 2.2 원격검침 보안시스템 아키텍처 설계

본 연구개발을 통하여 보안 프로토콜을 각 디바이스에서 구현하기 위한 보안H/W플랫폼을 개발하였고, 원격검침용 기기 인증 및 안전한 검침데이터 처리를 위한 보안인증서버를 개발하였다. 또한, IRM내에서 본 보안프로토콜 기능 지원을 위하여 SPU(Security Process Unit) 소프트웨어를 개발하였다. 이러한 결과물들을 적용하여 원격검침용 보안프로토콜을 기반으로 하여, 초기 기기 등록 및 인증과정, 그리고 검침데이터의 암복호 과정을 구현하였고 각 디바이스간의 상호 연동과정을 통합테스트를 통하여 검증하였다.

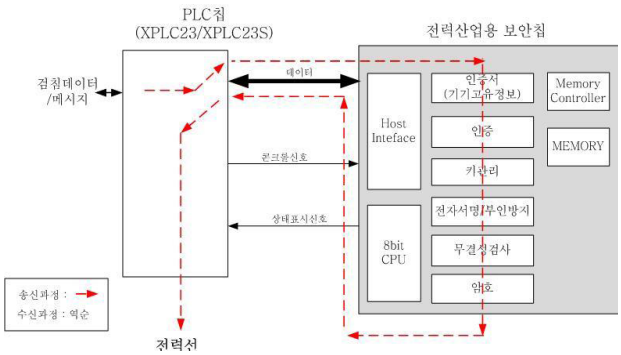


그림 2 원격검침용 보안모듈 기능구성
Fig. 2 The structure of security module function block

보안인증서버는 보안시스템의 중앙관제 성격을 가지며 초기

에 IRM, 전력량계와 같은 기기의 인증 및 등록을 관장하게 된다. 이때, 사전에 인증서버에 등록된 각 기기의 고유정보를 사용하여 기기의 유효성 및 적합성을 검증함으로써 인증 및 등록 절차를 수행한다. 보안시스템은 검침데이터에 대해 인증서버와 전력량계간에 End to end privacy를 보장하며 IRM내에서는 검침데이터에 대한 암복호 과정이 수행되지 않지만 IRM기기에 대한 초기 인증 및 등록과정에서 인증서버와 신호를 교환할 때 암복호 과정이 수행되며 기기 인증서에 대한 안전한 저장 및 관리 역할을 한다. 또한, IRM SPU(Security Process Unit) 프로그램은 IRM내의 보안H/W플랫폼과 기존 IRM내의 프로세스(DGU)와의 인터페이스를 원활히 하는 역할을 한다. 보안인증서버에서 내려온 정보를 IRM내 보안H/W플랫폼에 전달하고 반대로 보안H/W플랫폼에서 올라온 정보를 보안인증서버에 전달하는 역할을 수행한다.

### 2.3 프레임 구조 및 통신 프로토콜 설계

프레임 구조는 보안H/W플랫폼을 중심으로 하여 각 디바이스 간 인터페이스를 규정하고 있으며, 통신 프로토콜은 원격검침용 보안프로토콜을 기반으로 하여, 초기 기기 등록 및 인증을 위한 사전 운용 단계, 그리고 데이터 검침을 수행하는 검침 운용 단계 등의 단계별로 구분하고 각 단계에서 연관된 디바이스 간 통신 및 제어를 위한 프로토콜을 정의 하였다.

IRM 보안H/W플랫폼 MPLC간 통신은 Serial Control Frame을 통해 이루어진다. 계량기단의 SPLC와 보안H/W플랫폼간 통신은 SSMP protocol을 이용하며 보안H/W플랫폼 Meter 간 통신은 해당 Meter의 검침 protocol packet을 이용한다. 보안H/W플랫폼에서는 SSMP fram내 MSG의 Value에 포함된 검침 protocol packet을 Meter로 전송하고 Meter로부터 전송된 검침 protocol packet은 적절한 프로세스 후 SSMP frame을 생성하여 SPLC에 전송한다.

### 2.4 보안 H/W 플랫폼 개발

원격검침용 보안 프로토콜을 구현하기 위하여 주요 H/W엔진 부분은 RTL 코드로 설계하고 Verilog로 H/W엔진을 개발하였다.

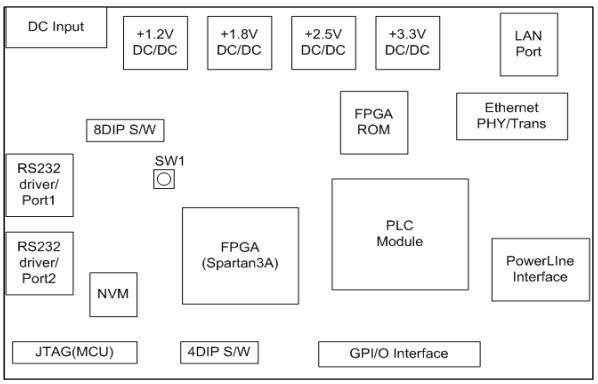


그림 3 보안 H/W 플랫폼용 에뮬fp이터 보드 구성도
Fig. 3 The structure of security H/W flatform Board

개발과정에서 각 설계 블록은 시뮬레이션을 통하여 검증했으며 각 보안H/W엔진 간의 원활한 구동과 외부 디바이스와의 원활한 인터페이스를 위하여 M8051 MCU기반의 펌웨어를 개발하였다. 개발한 보안H/W엔진 및 내장 펌웨어를 실제 하드웨어 상에서 검증 및 구현하기 위하여 FPGA기반의 에뮬레이터 보드를 제작하였고, 설계한 보안모듈엔진을 FPGA상에 포팅하여 검증하였다.

#### 2.3.1 보안 H/W엔진 RTL설계

효율적인 보안H/W 엔진 설계를 위하여, 먼저 내부 아키텍쳐를 설계함후 각 구성 요소간의 상호 작용 및 처리 속도등을 고려하여 최적의 내부 버스구조를 설계하였다.

#### 2.3.2 H/W 에뮬레이터 보드 제작

원격검침용 보안프로토콜 알고리즘을 RTL기반의 하드웨어로 설계 및 구현하고 검증하기 위하여 하드웨어 에뮬레이터 보드를 개발하였다.

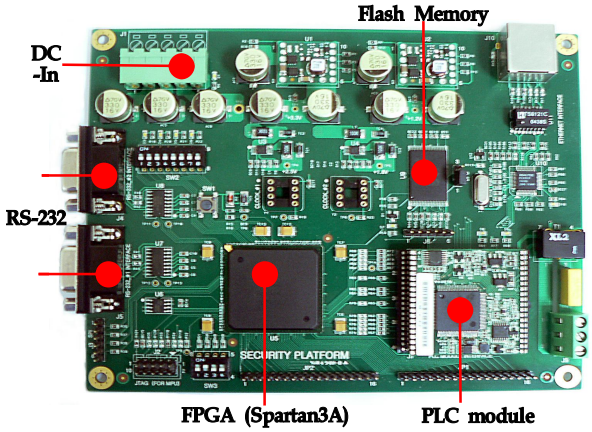


그림 4 보안 H/W 플랫폼용 에뮬레이터 보드
Fig. 4 Security emulator board

## 3. 결 론

본 연구는 PLC 기반의 AMR 시스템의 안전성 보장을 위해 필수적인 보안 H/W 플랫폼을 개발했다. 전기원격검침사업이 본격적으로 시작되고 특히 전력선 통신기반의 매체의 특성을 고려한 보안기술에 적용할수 있도록 설계되었다. 스마트그리드 환경에서 외부망과 연계되고 3rd party 사업자가 개입되는 개방형 환경에 적용되면 시스템 장비인증, 검침정보의 기밀성유지등의 보안성 확보에 기여 할 것으로 전망된다.

## 참 고 문 헌

[1] 최문석, 주성호, 임용훈. PLC기반 통합원격검침 시스템 설계. 2007. 대한전기학회 하계학술대회 논문집.
[2] 주성호, 최문석, 백종목, 임용훈. PLC기반 원격검침 인프라 보안시스템. 전력전자학회 추계학술대회 논문집.pp256 258.