

## 스마트미터의 원격 펌웨어 업그레이드 기법 고찰

김형규\*, 최재곤\*  
LS산전\*

### A Study of Remote Firmware Upgrading Schemes

Hyung-Kyu Kim\*, Jae-Gon Choi\*  
LS Industrial System\*

**Abstract** - 국내 스마트 그리드 산업 발달이 가속화 됨과 더불어 스마트 미터에 대한 표준도 구체화 단계에 접어들고 있다. 현재 한전 표준 저압 전력량계 규격에 원격 펌웨어 업그레이드 기능이 추가가 되면서 기존 스마트 미터에 기능을 추가하기 위한 방법에 업계의 관심이 쏠리고 있으며, 물리적인 원격 펌웨어 업그레이드 방법에 대한 1차적인 접근 뿐 아니라 미터의 기능에 최적화 되기 위한 업그레이드 과정의 구성방법, 안정적이고 강인한 펌웨어 전송 및 업그레이드를 위한 구체적인 방법까지 총체적으로 연구될 필요가 있다. 본 논문에서는 원격 펌웨어 업그레이드 방법을 위한 일반적인 방법들에 대한 고찰과 장 단점을 논하고 실제 하드웨어를 구성하여 DLMS프로토콜을 통해 원격업데이트 기능을 구현하였다.

#### 1. 서 론

스마트 미터란 스마트 그리드의 최 말단에 위치하는 기기로 1차적인 기능으로는 소비자들의 사용 전력량의 계량을 담당하고 있다. 스마트 미터에 대하여 명확히 정의된 것은 없으나 한국 스마트 그리드 협회에서 발표한 현재 스마트 미터에 대한 국내외적인 동향은 다음과 같다.<sup>[1]</sup>

- 국내 전력량계는 KSC 1214 및 IEC 62052, 62053 규격을 만족 (해외(북미형)의 경우 ANSI C12 규격을 만족)
- ANSI C12.19 표준은 스마트 미터를 비롯한 End device에 데이터 종류를 정의한 표준
- 현재 NIST에서 기존의 전력량계를 업그레이드 하는 표준화를 우선 표준화 대상에 포함하여 (PAP00: Meter Upgradability Standard) 진행 중이며 ANSI C12.19 표준이 유틸리티 회사에서 사용하기에 복잡하여 PAP05:Standard Meter Data Profiles에서 이를 단순화 시키는 작업을 진행
- 국내에서는 전력사용 비율에 따라 발생하는 펄스를 count하여 유효·무효·역률·Peak 등을 시간대별(실시간) 측정하며 부하기록 및 원격검침이 가능한 스마트미터를 개발예정
- 양방향 통신, 요금제 (TOU 외 CPP, RTP 등), tamper detection, 원격 firmware 업그레이드 등이 한전 표준 저압 전력량계 규격에 반영될 예정
- 규격을 만족하는 스마트 미터는 2020년까지 총 1조 4,740억원을 투입하여 저압수용가 1,800만호에 전량 보급할 예정

이 중 한전 표준 저압 전력량계에 반영될 주요 기능에 포함된 것이 원격 펌웨어 업그레이드 기능으로써, 기능 구현 방법에 대한 구체적인 고찰이 필요한 상황이다.

#### 2. 본 론

##### 2.1 전력량계의 구성

하드웨어의 구성은 어떻게 구현하느냐에 따라 다를 수 있으나 기본적인 전력량계의 주요 기능과 현재 MPU(Micro Processing Unit)에서 제공하는 기능이 대부분 비슷하기 때문에 본 논문에서 제시하는 접근법들은 일반적으로 모든 경우에 통용될 수 있는 방법들이라 할 수 있다.

기본적으로 디지털 전력량계는 Calibration Factor나 에너지 정보를 저장할 공간으로 EEPROM(electrically erasable programmable read-only memory)을 사용하고 있으며, 메인 프로그램은 MPU에 내장된 Flash 영역을 사용하고 있음을 기본 전제로 한다. 본 논문에서는 실제 구현한 하드웨어를 기본으로 하여 각 기법별 장단점을 세부적으로 소개하고자 한다. 본 논문에서 구현한 하드웨어 구성은 표 1과 같다.

**〈표 1〉 디지털 전력량계의 하드웨어 구성**

	Model	비고
MPU	Teridian <sup>[2]</sup>	8051기반
EEPROM	M24M01 <sup>[3]</sup>	1Mbit
통신	DLMS <sup>[4]</sup>	Image Transfer

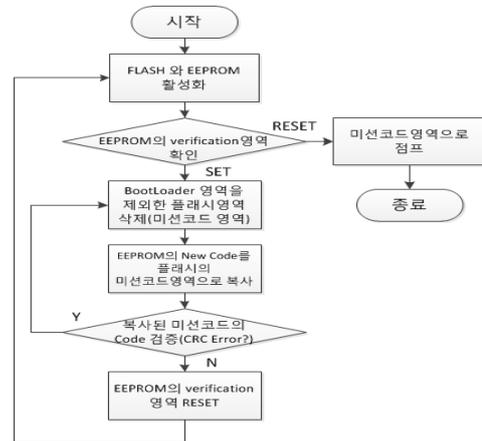
설명의 용이함을 위하여 펌웨어 업그레이드를 위한 새로운 코드를 New Code로 명명하기로 하였다. New Code를 전력량계로 전송하기 위하여 DLMS프로토콜의 Image Transfer를 사용하였다.

##### 2.2 원격 펌웨어 업그레이드 기법들

원격 펌웨어 업그레이드를 위한 방법으로는 세가지 접근법이 있다. 각 기법에는 그에 따른 장단점이 있으나 이는 기본적인 하드웨어 구성에 따라 차이가 있을 수 있다. 구현의 기본적인 방법은 비슷하나 추가적으로 고려해야 할 문제나 업그레이드 과정 자체가 상이할 수 있으므로 현재 상황에 맞는 방법을 채택하여 구현하여야 한다.

###### 2.2.1 기법 1 : EEPROM에 New Code를 다운로드하는 기법

통신으로 New Code를 EEPROM으로 다운로드한 후 펌웨어를 교체하는 방식이다. 이 경우 코드는 세가지 부분으로 나뉘게 되는데, 첫째 FLASH의 0번지에 위치하는 부트로더, 둘째 FLASH의 나머지 영역에 위치하는 기존의 메인 프로그램인 미션코드영역, 그리고 EEPROM에 다운로드된 New Code이다. 업그레이드를 위한 부트로더의 순서도는 그림 1과 같다.



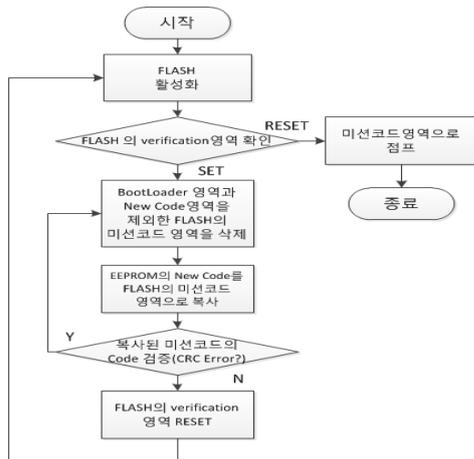
**〈그림 1〉 기법 1의 부트로더 순서도**

이 기법을 위하여서는 미션코드가 EEPROM에 저장되어야 한다. 따라서 통신을 통한 다운로드는 EEPROM에 바로 이루어지게 되므로 다운로드 및 CRC체크 중간에 미터의 동작이 멈추지 않아도 된다는 장점이 있다. 그리고 FLASH공간에 추가적인 공간이 요구되지 않으므로 FLASH용량이 큰 고가의 MPU가 필요치 않다. 그러나 EEPROM인 만큼 다운로드 속도가 느린편이며 코드 크기만큼의 EEPROM의 용량이 추가적으로 필요하게 된다.

###### 2.2.2 기법 2 : FLASH 영역에 New Code를 다운로드하는 기법 1

이 기법은 기법 1과 유사하나 New Code를 다운로드하는 영역이 FLASH 영역이라는 부분만 기법 1과 다르다. 이 경우 코드는 FLASH의

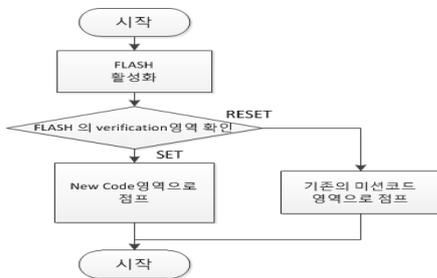
0번지에 위치하는 부트로더, FLASH의 상위영역에 위치하는 미션코드, 그리고 FLASH의 하위영역에 위치하는 New Code 이렇게 세부분으로 나뉘게 된다. 기법 2의 업그레이드를 위한 부트로더의 순서도는 그림 2와 같다. 전체적으로 기법 1과 동일하나 EEPROM의 영역이 FLASH의 남은 영역인 점만 다르다. 따라서 다운로드 속도 자체는 기법1에 비해 현저히 빠르며, 외부의 추가적인 EEPROM을 사용하지 않아도 되므로 하드웨어적으로 대단히 안정적이다. 그러나 FLASH 영역이 일반 코드의 두배가 필요하므로 고가의 MPU가 필요하며, 무엇보다 큰 단점은 New Code의 다운로드 시와 CRC체크 시 모두 미터가 멈춰야 한다는 점이다. 본 논문에서 사용한 MPU의 FLASH 쓰기 속도는 20  $\mu$ s/byte이다. 이는 EEPROM보다는 월등히 빠른 속도가기는 하나, 다운로드가 완료될 때까지 미터의 동작이 완전히 멈춰야 하므로 동작이 멈추는 것을 최소화해야 하는 관점에서는 적합하지 않은 방법이다.



〈그림 2〉 기법 2의 부트로더 순서도

### 2.2.3 기법 3 : 미션 코드 시작 주소 변경 기법

이 기법 역시 기법 2와 마찬가지로 FLASH의 미션코드 영역을 반으로 나누어 남은 절반 부분에 New Code를 다운로드 하는 기법이다. 그러나 기법 2와 다른점은 각 영역의 코드, 즉 기존의 미션코드와 다운로드가 완료된 New Code 모두 각각의 주소에서 실행이 가능한 상태인 점이다. 양쪽의 코드 모두 즉각적으로 바꾸어 실행 할 수 있으므로 미터는 항상 여분의 구동가능한 펌웨어를 가지고 있다고 볼 수 있다. 기법 2와 마찬가지로 EEPROM에 다운로드하는 것에 비해 대단히 안정적이며, 새로운 코드로의 변경은 간단한 주소의 스위칭일 뿐이므로 시간지연이 전혀 발생하지 않는다. 따라서 코드의 불백이 대단히 용이하다는 장점을 가지고 있다. 그림 3처럼 부트로더 역시 매우 간단하다. 그러나 역시 New Code의 다운로드가 플래시 영역에 이루어 져야 하므로 다운로드 동안 미터가 멈춰야 한다는 단점이 있다. 그래도 기법 2에 비해서 기법 3이 갖는 매력트는 기법 1, 2와 달리 부트로더에서 플래시를 지우고 복사하는 부분이 빠져 있으며, 업그레이드 자체에 시간이 걸리지 않는다는 것으로 이는 곧 기법 3과 기법 1이 업그레이드를 위해 미터를 멈춰야 하는 시간에는 큰 차이가 없을 수 있다는 것을 의미한다.



〈그림 3〉 기법 3의 부트로더 순서도

## 2.3 펌웨어 업그레이드 기능의 실제 구현

표 1에서 제시한대로 하드웨어를 구성하여 구현하였다. 미터의 동작이 멈추는 시간을 최소화 해야하는 것을 첫째 조건으로 삼고, 기존 데이터를 저장하는데 이미 EEPROM을 사용하고 있으므로 기법 1의 방법이 원격 펌웨어 업그레이드 기능을 구현하는데 가장 적합하다고 판단하였다. 부트로더와 미션코드 모두 KEIL 컴파일러를 사용하여 실행파일을 컴파일 하였고, 부트로더와 업그레이드전의 미션코드를 통합한 코드를 미터

에 다운로드한 상태에서 원격 펌웨어 업그레이드를 위하여 New Code를 전송하도록 하였다. 이때 DLMS 통신 프로토콜을 이용한 다운로드를 하기 위하여 New Code에 해당하는 펌웨어의 실행파일을 bin형식으로 변환하여 전송하도록 하였다. 이는 Teridian IC의 FLASH영역이 4개의 bank로 구성되어 있고 KEIL 컴파일러가 컴파일해 주는 방식이 BIN형식이 아니기에 추가의 변환 프로그램을 구현하여 DLMS 프로토콜의 Image Transfer를 사용하기 쉬운 형태로 하기 위함이다. 변환되어 전송된 New Code는 EEPROM의 New Code 영역에 그대로 저장되고, 부트로더가 이를 해석하여 FLASH의 각 bank에 복사하게 된다.

DLMS 프로토콜을 통해 New Code가 전송되고 EEPROM에 저장되어 완료되는 과정동안은 미터 본연의 기능 수행에 부담이 되지 않도록 프로그램을 구성하였기 때문에 다운로드의 속도는 크게 중요하지 않은 부분으로 시간은 따로 정확히 측정을 하지 않았다. 다운로드 완료후 CRC 체크를 하여 이상이 없을 시에 EEPROM에 기 설정된 4바이트의 verification 영역에 이상이 없을 것을 알리는 값을 저장하여 이미지가 정상적으로 다운로드되었음을 확인하도록 하였다.

다운로드가 완료된 상태에서 코드를 리셋하면 그림 1의 순서도대로 verification영역이 SET되어 있음을 확인하고 FLASH영역을 삭제한다. 삭제 속도는 40ms/page이며 부트 코드 영역을 제외하면 60 페이지 정도이므로 이론적으로 삭제에만 2.4초가 걸리게 된다. FLASH의 쓰기 속도는 20  $\mu$ s/byte이지만 복사의 안정성을 위해 페이지를 쓸 때마다 일정 수준의 딜레이를 주어 구현하였다. 결국 실제로 부트로더가 동작하여 FLASH를 삭제하고 New Code를 미션코드 영역으로 복사하여 구동되는데까지는 평균 30초 정도가 걸렸다. 이는 현재 프로토 타입으로써 최적화 과정을 통해 더욱 시간을 단축시킬 여지가 있는 부분이다.

## 3. 결 론

본 논문에서는 원격 펌웨어 업그레이드를 위한 세가지 기법들을 소개하고 스마트미터에 적용하기에 적합한 기법을 실제 구현하여 그 안정성과 동작시간에 대한 결과를 고찰하여 보았다. 미터IC는 Teridian IC를 사용하였으며 KEIL 컴파일러를 사용하여 펌웨어를 구현하였다. 이 기법들은 스마트 미터 이외에도 원격으로 펌웨어의 업그레이드가 필요한 디바이스들에게도 확장 적용 가능하므로 각 기법별 특징과 장,단점을 고려하여 각각의 경우에 맞게 구현 하는데 본 논문이 도움이 될 수 있을 것으로 기대한다. 실제 구현시에는 정상적이지 않은 상황 까지 고려하여 안정적인 펌웨어 업그레이드가 되도록 하여야 하므로 추가적인 케이스 스터디와 최적화를 위한 연구가 진행 중에 있다.

## [참 고 문 헌]

- [1] 한국스마트그리드 협회, “지능형 소비자(Smart Place) 표준화 동향”, 논문지명, 한국스마트그리드 협회, 정보자료실, 2010
- [2] STMicroelectronics, ‘DATASHEET of M24M01-W’, <http://www.st.com>
- [3] Teridian SMICONDUCTOR CORP., ‘DATASHEET of 71M6531D/F’, Revision 1.3 , <http://www.teridian.com>
- [4] 오정환, 이영주, 박재성, 김병섭, 조선규, 이진, ‘DLMS/COSEM에 기반한 전사식 전력량계의 전력정보 모델링’, 2006 대한전기학회 전력기술 부문회 추계학술대회 논문집, 2006.11, page(s): 3-432