Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.24, NO.5, Oct. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.5.1001

DCU 보안요구사항 분석 및 CC v3.1 기반의 보호프로파일 개발*

조 영 준,† 김 신 규‡
한국전자통신연구원 부설연구소

Analysis of Security Requirements on DCU and Development Protection Profile based on Common Criteria Version 3.1*

Youngjun Cho,† Sinkyu Kim‡
The Attached Institute of ETRI

요 약

스마트그리드 환경에서 이용되는 기기들은 양방향 통신이 가능하기 위해 다양한 통신 인터페이스를 가짐으로 기존 IT기술이 가지고 있는 보안 취약점을 그대로 가질 수 있다. 이러한 보안 위협과 공격에 대한 피해를 최소화하기 위해 스마트그리드 기기의 보안기능과 이에 대한 평가 · 인증에 대한 필요성은 증가하고 있다. DCU는 스마트 미터의 정보를 중간 수집하여 유틸리티에 전송하는 중간 집계 장치로, 가정 내 위치하는 스마트 미터와 유틸리티 내부의 서버와 중간 위치에 설치되어 DCU가 공격받는 경우, 중간 거점으로 활용되는 등 위험성이 존재한다. 그러나 현재 DCU 보안성 평가와 관련된 연구가 미흡하여 DCU의 보안성을 확보하고 이를 평가, 인증할 수 있는 방법이 존재하지 않는다. 본 논문에서는 DCU의 보안성을 평가할 수 있는 보호프로파일을 개발하여 향후 개발자 또는 판매자에게는 보안목표명세서 작성에 도움을 주고, 사용자에게는 제품의 선정 및 운용관리에 활용할 수 있도록 한다.

ABSTRACT

Smart Grid Devices could have security vulnerabilities that have legacy communication networks because of the fact that Smart Grid employs bi-directional communications and adopted a variety of communication interface. Consequently, it is required to build concrete response processes and to minimize the damage of the cyber attacks including security evaluation and certification methods. DCU is designed to collect meter data from numerous smart meter and send to utility's server so DCU installed between smart meter and utility's server. For this reason, If DCU compromised by attacker then attacker could use DCU to launching point for and attack on other devices. However, DCU's security evaluation and certification techniques do not suffice to be deployed in smart grid infrastructure. This work development DCU protection profile based on CC, it is expected that provide some assistance to DCU manufacturer for development of DCU security target and to DCU operator for help safety management of DCU

Keywords: DCU, Smart Grid, Protection Profile, Common Criteria

접수일(2014년 8월 29일), 수정일(1차: 2014년 10월 6일, 게재확정일(2014년 10월 6일)
* 본 연구는 2012년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.(2012101050004A)
† 주저자, ycho@ensec.re.kr
‡ 교신저자, skkim@ensec.re.kr(Corresponding author)

I. 서 론

차세대 전력망으로 기대되고 있는 스마트그리드는 기존의 폐쇄적인 전력망 구조를 기반으로 최신 ICT (Information Communication Technology)기

술을 접목하여 이루어지는 양방향 전력 서비스이다. 양방향 전력 서비스가 실현되면, 현재보다 더욱 효율적인 전력 생산 및 관리, 제어가 가능하며 전력회사는 다양한 부가 서비스를 제공할 수 있고, 개방정인 운영시스템 특성으로 인해 신재생 에너지 발전, 전기차 등 청정 녹색 기술의 접목이 용이하다.

국내에서는 이러한 스마트그리드 환경 구축의 일환으로 진화된 검침 인프라인 AMI(Advanced Metering Infrastructure) 구축이 진행 중에 있으며, 이와 관련된 AMI 보안 요구사항 분석, 키 관리 기술 등의 보안 기술에 대한 연구가 활발히 진행 중에 있다[1][2].

AMI를 구성하는 대표적인 기기로 스마트 미터, DCU를 들 수 있다. AMI를 구성하는 주요 기기 중 스마트 미터의 경우 이의 보안성을 시험 평가하기 위한 보호프로파일 개발과 관련된 연구가 진행된바 있다[3]. 그러나 한 개 이상의 스마트 미터로부터 데이터를 수집하여 유틸리티 서버로 전송하는 DCU에 대한 보호프로파일에 대한 연구는 미흡하다. DCU는 스마트 미터와 유틸리티의 중간 거점에 위치하고 있어, DCU가 공격받을 경우 다른 DCU, 스마트 미터로 공격이 전이될 수 있으며, 나아가 유틸리티 서버의 공격 거점으로 활용될 수 있어 이에 대한 보안 대책이 필요하다. 이에 본 논문에서는 DCU의 기능을 분석하고 취약점 및 보안 요구사항을 식별하여 DCU의 보안성을 평가할 수 있도록 하는 보호프로파일을 개발한다.

II. DCU 분석 및 관련 보호프로파일

2.1 DCU(Data Concentration Unit) 기능

2.1.1 DCU의 정의

DCU(Data Concentration Unit, 데이터 집중장치)는 일반적으로 AMI(Advanced Metering Infrastructure) 환경에서 하나 이상의 스마트 미터(Smart Meter)가 송신 또는 수신하는 검침 데이터, 제어 명령 관련 메시지를 스마트그리드 운영 서버(MDMS, Metering Data Management Server)로 중계하는 역할을 수행한다. 일반적인 DCU 구성 환경은 Fig.1.과 같다.

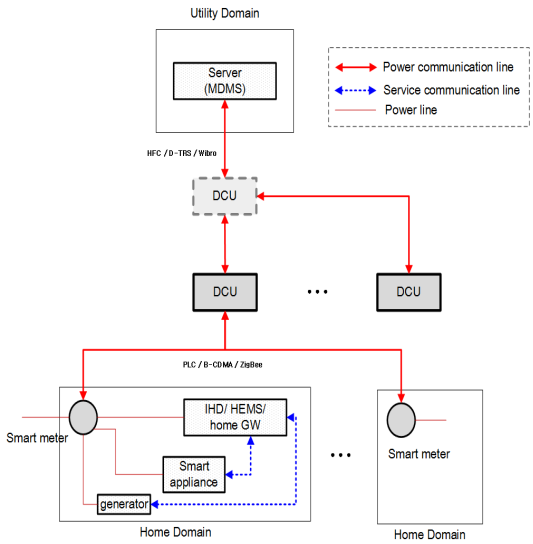

Fig. 1. Common structure of the DCU

2.1.2 DCU의 기능 분석

DCU의 일반적인 기능은 전력량계 데이터 수집, 수집된 정보 상위 전송, 인근 DCU 연계 기능, 변압기 감시 기능, 통신망 중계가 있다.

전력량계 데이터 수집은 스마트 미터에서 검침한 데이터를 일정 시간 간격으로 수집하는 기능을 의미하며, 수집된 정보 상위 전송 기능은 한 대 이상의 여러 스마트 미터로부터 수집된 검침 정보를 상위 유틸리티 서버 또는 다른 상위 DCU로 전송하는 기능을 의미한다. 인근 DCU 연계 기능은 DCU와 유틸리티 서버가 직접 통신이 불가능할 경우, 다른 DCU를 거쳐 서버로 전송할 수 있도록 DCU간 연계 기능을 의미한다. 변압기 감시 기능은 변압기의 상태 정보를 수집하여 상위 서버에 이를 알릴 수 있는 기능으로 경우에 따라 이 기능이 존재하지 않을 수 있다. 통신망 중계 기능은 HAN(Home Area Network) 영역의 스마트 미터와 WAN(Wide Area Network) 영역의 서버 사이에 위치한 DCU가 서로 다른 통신 프로토콜을 사용할 경우, 이를 중계할 수 있도록 하는 기능을 의미한다.

2.2 보호프로파일

공통평가기준(CC, Common Criteria)은 IT 정보보호시스템을 평가하기 위한 기준으로 기존 각

국가마다 서로 다른 보안 평가 기준을 하나의 평가 기준으로 통일한 것으로 상호협정을 맺은 국가 간 동일한 평가 기준을 이용할 수 있도록 해준다. 보호프로파일(PP, Protection Profile)은 평가 대상의 범위, 환경 등을 설정하고 대상 제품에서 요구되는 보안기능을 제시하여 향후 CC 인증을 위한 제품 개발 시 보안기능의 제안요청서와 유사한 역할을 수행한다.

국내에서는 정철조 등이 AMI 환경의 주요 기기 중 하나인 스마트 미터에 대한 보호프로파일 개발에 대한 연구를 수행하였다[3]. 정철조 등이 수행한 연구에서는 스마트 미터에 존재하는 취약성, 보안 요구사항을 분석하고 EAL 5 등급의 보호프로파일을 제시한다. 그러나 제시한 보호프로파일은 국내 등록되어 사용되는 보호프로파일은 아니며, 현재 국내 IT 보안인증사무국에 등록된 스마트 미터, DCU 등 스마트그리드 관련 기기의 보호프로파일은 존재하지 않는다.

독일에서 개발한 보호프로파일인 “Protection Profile for the Gateway of a Smart Metering System” 에서는 WAN, HAN, LMN(Local Metrological Network) 사이에서 일종의 방화벽 역할을 수행하는 게이트웨이를 대상으로 한다[4]. 이 프로파일은 평가보증등급은 EAL 4+ 이다.

마찬가지로 독일에서 개발한 보호프로파일인 “Protection Profile for the Security Module of a Smart Meter Gateway” 에서는 스마트 미터링 시스템에서 사용하는 암호 서비스 제공을 위한 암호 모듈을 대상으로 한다[5]. 이 암호모듈의 평가보증등급은 EAL 4+ 이다.

III. DCU 보안 요구사항 분석

3.1 DCU 보안 취약점

본 절에서는 2011년 InGuardians 사에서 발표한 AMI 공격 방법[6], 2012년 김신규 등이 연구한 AMI 보안 취약점 점검 항목[7], 2012년 Florian Skopik 등이 조사한 스마트 미터링 인프라의 위협과 취약점[8]을 참고하여 DCU에 해당하는 주요 취약점을 물리적 접근을 통한 취약점, 네트워크 접근을 통한 취약점으로 분류하여 식별한다.

3.1.1 물리적 접근 취약점

DCU의 물리적 접근 취약점은 버스 스니핑, 메모리 덤프, 관리용 통신 포트 접근 취약점이 있다.

버스 스니핑 취약점은 데이터가 이동하는 버스를 스니핑하여 중요 정보를 획득하는 것으로 Travis Goodspeed[9]는 이를 이용하여 ZigBee Chip을 분석해 ZigBee 키를 획득하는 내용을 발표했다.

메모리 덤프 취약점은 내부 메모리에 덤프를 수행하여 메모리에 저장된 중요 정보를 획득할 수 있도록 한다. 메모리에 통신에 사용되는 키 값 등이 평문으로 저장된 경우 공격자는 이를 획득하여 공격에 사용할 수 있다.

관리용 포트 접근 취약점은 관리자에게 허용된 관리 포트를 통해 접근하여 허가받지 않은 사용자가 관리자 권한을 획득할 수 있는 취약점이다. 이 취약점과 관련하여 Kurt Rosenfeld 등[10]은 기기의 관리에 사용되는 JTAG을 이용한 공격을 제시하였다.

3.1.2 네트워크 접근 취약점

DCU의 네트워크 접근 취약점으로는 ZigBee 취약점, PLC 취약점, 인증 취약점, 응용프로토콜 취약점이 존재한다.

ZigBee, PLC 취약점은 DCU에서 해당 통신 프로토콜을 사용할 때, 해당 통신 프로토콜의 알려진 취약점에 대한 것으로 이를 이용한 공격이 가능할 수 있다.

인증 취약점은 DCU 인증 과정에서 인증 과정을 우회할 수 있도록 하거나 연속적인 인증 시도를 통한 권한 획득, 인증 메시지의 재전송 공격 또는 중간자 공격 등을 가능하게 할 수 있다.

응용프로토콜 취약점은 안전하지 않은 펌웨어 업데이트를 이용한 악성 펌웨어 설치를 가능하도록 하거나 제어 메시지의 변조가 가능하도록 하는 취약점으로 공격자는 이를 이용하여 DCU를 악성코드에 감염시키거나 변조된 제어메시지를 송신하도록 할 수 있다.

3.2 DCU 보안 요구사항

본 절에서는 위에서 살펴본 취약점으로 인한 피해를 방지하기 위해 DCU에 요구되는 보안 요구사항을 분석한다.

3.2.1 보안 관리 기능

보안 관리 기능은 DCU가 가지고 있는 보안 속성, 보안 기능 관련 데이터 등 과 관련된 사항을 관리하는 기능을 의미한다. 예를 들면, 접근통제 목록, 데이터 유효기간 설정 등의 기능이 있다.

보안 기능 관리를 위해서, DCU가 수행하는 특정 보안 기능의 행동(보안 기능 시작, 중지, 변경 등)을 인가된 사용자만 이용할 수 있도록 해야 하며, 보안 속성(보안 기능 수행을 위한 설정 값)에 대한 행동(보안 속성 디폴트 값 변경 또는 삭제 등)을 인가된 사용자만 수행할 수 있도록 강제할 필요가 있다

3.2.2 보안 감사 기능

보안 감사는 보안과 관련된 모든 이벤트들의 행위자, 시간, 행위 등을 기록하는 기능을 의미하며, 보안 감사 기능에는 안전한 보안 감사 저장과 지정된 이벤트에 대해 관리자에게 알려주는 기능도 포함된다. DCU에 인가되지 않은 접근이 여러 차례 발생되거나, 일반적이지 않은 행동이 탐지된다면 이에 대해 관리자에게 알려주는 기능이 포함되어야 한다. 스마트그리드 환경에서 운영 연속성은 중요하며, 침해사고 발생의 예방과 사후 조치를 위해 보안 감사 기능이 요구된다.

3.2.3 식별 및 인증 기능

식별 및 인증 기능은 DCU에 접근하는 모든 객체들에 대한 신원을 설정하고 증명을 수행하는 기능을 의미한다. 이는 접근 객체에 대해 인가된 사용자의 명확한 식별과, 인가된 사용자에 해당하는 보안속성과 정확한 연결을 의미한다.

식별 및 인증 보안 기능에는 사용자 인증 수행 시, 인증 실패 횟수에 따라 이를 탐지하는 기능, 이전에 사용된 인증 데이터의 재사용을 방지하도록 하는 기능, 다른 인가된 사용자로 신원을 속일 수 없도록 정확한 사용자를 식별하는 기능 등이 포함된다.

또한, 식별 및 인증 보안 기능은 접근 통제, 암호화 지원 등 다른 보안 기능들의 성공적인 수행을 위해 의존하는 기능으로, 정확한 식별 및 인증 기능사용으로 다른 보안 기능이 효과적으로 수행될 수 있도록 한다.

3.2.4 데이터 보호 기능

데이터 보호 기능은 DCU에 저장된 민감한 정보가 노출되지 않도록 안전하게 보호하는 기능을 의미하며, 여기서 민감한 정보는 DCU가 저장한 검침 데이터 이외에 보안 속성 값, 인증 데이터 등을 포함한다.

DCU에는 다수의 스마트 미터가 전송한 전력 검침 데이터를 포함하고 있으며, 변압기 상태 정보, 스마트 미터 또는 서버와 통신을 수행하기 위한 인증 데이터 등이 있다. 이러한 데이터를 보호하기 위해 데이터에 대한 접근 통제, 허용되지 않은 정보 흐름 제한, 불필요하게 남아있는 잔여 정보 삭제 등의 기능을 수행할 수 있다. 데이터 보호를 위한 가장 일반적인 방법은 암호화 메커니즘을 적용하는 것이 있다.

3.2.5 암호화 지원 기능

암호화 지원 기능은 암호화 메커니즘을 사용할 때, 이를 완벽하게 사용할 수 있도록 해주는 기능으로 하드웨어, 펌웨어, 소프트웨어로 구현될 수 있다. 특히, 높은 수준의 보안 목적 달성을 위해 식별 및 인증, 데이터 보호, 접근 통제 등 다양한 보안 기능들이 암호화 기능을 주로 이용한다. 이 때, 암호화 지원 기능은 암호 키 관리, 암호 연산 기능을 통해 암호화 메커니즘을 지원할 수 있도록 한다.

DCU에서 서버 또는 스마트 미터와 상호 인증을 통한 안전한 통신 경로를 구축할 때, 암호 기능이 이용될 수 있으며, 민감한 정보의 안전한 저장을 위해서도 암호 기능이 이용될 수 있다.

3.2.6 안전한 업데이트 기능

안전한 업데이트 기능은 DCU에서 사용하는 펌웨어, 소프트웨어의 취약점이 발견되거나 서비스 운영 중 필요로 인해 업데이트가 필요한 경우, 이를 안전하게 수행할 수 있도록 해주는 기능을 의미한다. 업데이트 파일에 악성코드가 있는 경우 업데이트를 수행하는 모든 DCU가 감염될 수 있어 대규모의 피해가 발생할 수 있다.

DCU의 안전한 업데이트 기능은 업데이트 파일의 무결성 확인 및 배포자의 유효성 검증 등의 과정을 포함하여 오프라인 또는 온라인 업데이트 시 안전하게 업데이트를 보증할 수 있다.

3.2.7 접근 통제 기능

접근 통제 기능은 인가된 사용자가 인가된 역할만을 수행할 수 있도록 해주는 기능으로, 식별 및 인증 기능을 우선 수행하여, 신원이 확인된 객체에 대해 허가된 행동만을 수행하도록 제한하는 기능을 포함한다.

DCU에 접근한 유지보수 관리원이 저장된 정보를 위변조 하거나 연계된 다른 DCU가 저장된 데이터에 접근하려고 하는 등 허가되지 않은 행위를 통제할 수 있도록 해주는 기능을 포함하며, 정확한 접근 통제는 식별 및 인증 보안 기능에 의존하는 특징이 있다.

3.2.8 물리적인 보호 기능

물리적인 보호 기능은 물리적인 접근을 통해 발생할 수 있는 민감한 데이터 노출, 데이터 위변조, 도난 등에 대해 보호하는 기능을 의미한다.

DCU는 전신주 위에 설치될 수 있으며, 이 경우 물리적인 접근이 어려우나, 공개된 장소에 설치되어 있는 만큼 전문적인 기술이 있는 위협원으로부터 안전하지 못하다. 도난, 파괴 등 발생 시, 이를 관리자에게 신속히 전달하는 기능과 데이터 노출, 위변조를 방지하기 위한 탬퍼 프루핑 기능 등이 물리적인 보호 기능에 해당한다.

IV. DCU 보호프로파일 개발

4.1 TOE 정의

TOE(Target of Evaluation)는 DCU로 2장에서 설명한 것과 같이 스마트 미터(시간대별 사용량을 측정하여 그 정보를 송신할 수 있는 기능을 가지고 있어 시간대별 전력 사용량 측정이 용이)로부터 검침 데이터 등을 중간에서 수집하여 AMI Server로 전송하는 역할을 수행하는 기기라 할 수 있다.

4.2 보안문제 정의

4.2.1 보안위협원

보안위협원은 TOE 및 TOE의 운영환경에 위험을 초래할 수 있는 요소를 의미한다. TOE에 위협원이 될 수 있는 잠재적인 존재는 전력망 운영자, 현장 유지보수원, 인증되지 않은 외부 객체, 자연적 재해 위협원이 있을 수 있다.

○ 전력망 운영자

전력을 제공하고 필요에 따라 TOE 제어가 가능한 주체로 신뢰된 운영자, 부적절한 행위를 하는 운영자, 기존에 권한이 부여되었던 운영자 등이 될 수 있다.

○ 현장 유지보수원

현장에서 TOE를 유지보수 역할을 수행하는 현장 유지보수원은 TOE의 접근 권한을 부여받으며, 의심없이 물리적 접근이 가능한 주체를 의미한다.

○ 인증되지 않은 외부 객체

TOE에 인증을 수행하지 않은 객체로 해커, 테러리스트 등의 TOE환경 외부로부터 접근 가능한 주체를 의미한다.

○ 자연적 재해 위협원

지진, 홍수, 화재와 같은 환경적인 원인으로 발생될 수 있는 위협원이 존재할 수 있다.

4.2.2 보안 위협

TOE에 대한 보안 위협은 3장에서 살펴본 보안 취약점, 보안 요구사항 등을 통해 다음과 같이 정리할 수 있다. 제시하는 위협은 이 후, 위협 평가에서 식별하기 위해 T1, T2와 같이 숫자를 부여한다.

○ T1.위장공격

위협원은 인가된 사용자/시스템으로 가장하여 정당한 사용자/시스템으로 위장하여 TOE에 접근할 수 있다.

○ T2.인증 우회

위협원은 TOE의 인증 메커니즘을 우회하여 인가된 사용자/시스템의 권한을 획득할 수 있다.

○ T3.연속적인 인증 시도

위협원은 TOE에 접근하기 위해 연속적인 인증을 시도하여 인가된 사용자/시스템의 권한을 획득할 수 있다.

○ T4.데이터 유출
위협원은 불법적인 접근을 통해 TOE에 저장된 데이터를 습득할 수 있다.

○ T5.데이터 위·변조
위협원은 불법적인 접근을 통해 TOE에 저장된 데이터를 위조 또는 변조할 수 있다.

○ T6.서비스 거부
위협원은 TOE 자원에 과부하를 걸어 서비스 요청을 처리하지 못하도록 하여 서비스 제공을 방해할 수 있다.

○ T7.하이잭 공격
위협원은 기존에 인증에 성공한 통신 연결을 도용하여 사용할 수 있다.

○ T8.도청
위협원은 TOE가 송신 및 수신하는 메시지를 습득하여 내용을 살펴보고 이를 분석할 수 있다.

○ T9.중간자 공격
위협원은 TOE가 송신 및 수신하는 메시지에 대해 불법적인 데이터 삽입 및 변조할 수 있다.

○ T10.재전송 공격
위협원은 수집된 통신 데이터를 이용하여 불법적인 재전송 행위를 수행할 수 있다.

○ T11.감사기록 실패
위협원은 감사 기록 저장소의 저장용량을 소진시키거나 동시에 대량의 감사 사건을 발생시켜 정상적인 감사기록 생성을 방해할 수 있다.

○ T12.악성 코드
위협원은 악의적인 행동을 하는 악성 코드를 TOE에 설치하여 이를 이용하거나 다른 스마트 미터 또는 유틸리티 서버로 악성 코드를 전파시킬 수 있다.

○ T13.물리적 공격
위협원은 TOE 자체에 물리적인 접근을 통해 파손, 도난, 불법적인 접근 등을 수행할 수 있다.

4.2.3 조직의 보안정책

조직의 보안정책은 TOE를 운영하는 조직이 갖추고 있는 내부의 보안정책을 의미하며, 본 논문에서는 다음과 같은 보안정책을 조직의 보안정책으로 제시한다.

○ P.감사
TOE가 송신 및 수신하는 네트워크 트래픽 중 TOE 보안 정책에서 명시한 메시지에 대해 모두 기록하며 보안 관련 이벤트 발생 시, 해당 이벤트를 기록한다.

○ P.암호 알고리즘
TOE는 조직의 보안 정책에서 정하는 안전한 표준 암호 알고리즘을 사용한다.

○ P.비밀성
TOE가 송신 및 수신하는 네트워크 트래픽을 TOE 보안정책에서 정한 메시지는 TOE에 의해 암호화 및 복호화를 수행한다.

○ P.안전한 관리
인가된 관리자, 사용자는 안전한 방법으로 TOE를 관리 및 사용한다.

○ P.역할
사용자의 역할은 관리자 및 일반 사용자로 구분되며, 각 역할에 따라 TOE를 관리하거나 운영, 사용한다.

4.3 보안목적 도출

4.3.1 TOE에 대한 보안목적

TOE에 대한 보안목적은 TOE에 의해서 직접적으로 다루어지는 보안목적이다. TOE에 대한 보안목적은 다음과 같다. 보안 목적은 보안기능 요구사항과 비교를 위해 O1, O2와 같이 숫자를 부여한다.

○ O1.가용성
TOE는 우발적 또는 외부의 공격에 의해 고장이 발생 시 최소한의 보안기능을 유지하여 정상적인 서비스를 제공해야 한다.

○ O2.감사

TOE는 보안과 관련된 행동에 대한 책임을 추적하기 위해 보안 관련 사건을 정확하게 기록하고 안전하게 유지해야 하며, 기록된 감사데이터를 관리자가 적절하게 검토할 수 있는 수단을 제공해야 한다. 또한 감사데이터가 포화 상태로 도달하는 경우, 대응기능을 제공해야 한다.

○ O3.관리

TOE는 TOE의 인가된 관리자가 TOE를 효율적으로 관리할 수 있는 관리 수단을 안전한 방법으로 제공해야 한다.

○ O4.식별 및 인증

TOE는 TOE의 정보 흐름 통제를 받는 IT 실체와 TOE에 접근하고자 하는TOE 관리자를 식별 후 TOE 접근을 허용하기 전에 사용자의 신원을 인증해야 한다.

○ O5.역할

TOE는 사용자 역할을 관리자 및 일반 사용자로 구분해야 하며, 역할에 따른 보안 정책 및 보안기능, 접근제어 기능을 제공해야 한다.

○ O6.잔여정보제거

TOE는 TSF가 사용하는 작업영역에 사용 종료 시, 사용자 데이터나 TSF 데이터를 남기지 않는 것을 보장해야 한다.

○ O7.저장데이터 보호

TOE는 TOE에 저장된 TSF 데이터를 인가되지 않은 노출, 변경, 삭제로부터 보호해야 한다.

○ O8.전송데이터 보호

TOE는 전송되는 사용자 데이터 또는 TSF 데이터를 인가되지 않은 노출 및 변경으로부터 보호해야 한다.

○ O9.이상패킷차단

TOE는 다른 기기들로부터 수신되는 이상패킷에 대해 탐지 및 차단이 수행되어야 한다.

○ O10.시간동기화

TOE는 신뢰성 있는 시간정보를 제공해야하며 외부의 신뢰성 있는 전용 시스템으로부터 신뢰성 있는 시간정보를 업데이트할 수 있어야 한다.

4.3.2 운영환경에 대한 보안목적

운영환경에 대한 보안목적은 TOE가 보안기능성을 정확하게 제공할 수 있도록 운영환경에서 지원하는 기술적/절차적 수단에 의해 다루어야 하는 보안목적이다. 운영환경에 대한 보안목적은 다음과 같다.

○ OE.신뢰된 관리자

TOE의 인가된 관리자는 악의가 없으며, TOE 관리 기능에 대해 적절히 교육을 받았고, 모든 관리 지침 및 행동 절차에 따라 정확하게 의무를 수행해야 한다. 또한 자신의 권한을 타인에게 양도하지 않아야 한다.

○ OE.운영체제 보강

TOE 및 운영환경의 인가된 관리자는 운영체제의 취약점에 대한 보강작업을 수행하여 TOE와 다른 응용프로그램간의 간섭이 없음을 보장해야 한다.

○ OE.안전한 업데이트

TOE는 외부에 인증 주체로부터 제공될 수 있는 업데이트 소프트웨어의 무결성을 확인하여 업데이트 처리가 될 수 있도록 해야 한다.

○ OE.물리적 보호

TOE는 외부에 노출되어 위협원들의 접근이 용이해 도난 및 고장 등의 위협으로 안전할 수 있도록 조치를 해야 한다.

○ OE.상호운용성

TOE와 통신하는 AMI를 구성하는 모든 장비와의 상호운영성을 보장하기 위해 표준으로 제정된 프로토콜을 사용해야 한다.

○ OE.타임스탬프

TOE는 TOE 운영환경이 제공하는 신뢰할 수 있는 타임스탬프를 사용해서 보안관련 사건을 정확히 기록해야 한다.

Table 1. TOE Security Functional Requirements

Class	Component	
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAA.2	Profile based anomaly detection
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.2	Complete access control
	FDP_ACF.1	Security attribute based access control
	FDP_RIP.1	Subset residual information protection
	FDP_SDI.1	Stored data integrity monitoring
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_SOS.1	Verification of secrets
	FIA_UAU.1	Timing of authentication
	FIA_UAU.4	Single-use authentication mechanisms
	FIA_UAU.6	Re-authentication
	FIA_UID.1	Timing of identification
Security Management	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_MTD.2	Management of limits on TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Privacy	FPR_UNO.1	Unobservability
Protection of TSF	FPT_FLS.1	Failure with preservation of secure state
	FPT_ITC.1	Inter-TSF confidentiality during transmission
	FPT_ITI.1	Inter-TSF detection of modification
	FPT_PHP.1	Passive detection of physical attack
	FPT_RCV.3	Automated recovery without undue loss
	FPT_RCV.4	Function recovery
	FPT_STM.1	Reliable time stamps
	FPT_TST.1	TSF testing
TOE ACCESS	FTA_SSL.3	TSF-initiated termination
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel

4.4 보안요구사항 도출

보안요구사항은 보안기능요구사항과 보증요구사항으로 서술한다. 보안요구사항은 위에서 제시한 모든 보안 목적을 충족시켜야 한다. 본 논문에서 제시하는 요구사항은 공통평가기준 v3.1 r4를 기준으로 한다.

4.4.1 보안기능 요구사항

보안기능 요구사항은 보안목적을 달성하기 위해 TOE가 수행해야 하는 기능을 나타낸 것으로 목록은 Table 1.과 같다. Table 2.는 보안기능과 보안목적의 대응 관계를 나타낸 것이다.

Table 2. Mapping between Security Objectives and Security Functional Requirements

	O1	O2	O3	O4	O5	O6	O7	O8	O9	O10
FAU_ARP.1		×								
FAU_GEN.1		×								
FAU_SAA.1		×								
FAU_SAA.2		×								
FCS_CKM.1			×	×						
FCS_CKM.4				×		×				
FCS_COP.1				×			×			
FDP_ACC.2							×			
FDP_ACF.1					×		×			
FDP_RIP.1						×	×			
FDP_SDI.1							×			
FIA_AFL.1				×						
FIA_SOS.1				×						
FIA_UAU.1				×						
FIA_UAU.4				×						
FIA_UAU.6				×						
FIA_UID.1				×	×		×			
FMT_MOF.1			×							
FMT_MSA.1			×		×		×	×		
FMT_MSA.3			×		×		×	×		
FMT_MTD.1			×							
FMT_MTD.2			×							
FMT_SMF.1			×		×					
FMT_SMR.1			×		×					
FPR_UNO.1							×	×		
FPT_FLS.1	×									
FPT_ITC.1								×	×	
FPT_ITI.1								×	×	
FPT_PHP.1							×			
FPT_RCV.3	×									
FPT_RCV.4	×									
FPT_STM.1										×
FPT_TST.1	×		×							
FTA_SSL.3								×		

4.4.2 보증 요구사항

보증 요구사항은 위에서 제시한 보안기능 요구사항의 보증을 위한 내용으로 공통평가기준 3부의 보증 컴포넌트로 구성된다. DCU 보호프로파일의 평가보증등급(EAL, Evaluation Assurance Level)은 DCU의 운영 환경, 위험도를 고려하여 PP 개발자의 판단으로 등급이 결정된다. 국내에서는 윤신숙 등[11]이 평가보증등급 산정을 위한 기준을 연구한 바 있다. 본 논문에서는 윤신숙 등[11]이 제시한 방법을 이용하여 DCU의 정보가치와 위협등급을 판별한다. DCU의 정보가치는 IATF 기준에 따라 DCU의 주요 정보인 검침 정보가 노출될 경우, 패턴을 분석하여 개인의 생활 습관, 거주 여부 등 개인정보가 노출될 수 있으며 검침 정보의 위조 또는 변조로 인해 정상거인 서비스 제공 불가 등 서비스에 심각한 피해를 입힐 수 있어 V3 등급으로 산정한다. DCU의 윤신숙 등[11]이 제안한 수치화 접근법을

Table 3. Assessment of DCU's Circumstances of Threat

Threat	Resource	Skill	Intensity	Priority	Possibility
T1	1	1	3	1	1
T2	1	1	3	1	1
T3	1	1	3	1	1
T4	1	1	3	1	2
T5	2	1	3	1	2
T6	2	2	3	1	2
T7	2	3	3	1	2
T8	1	2	2	1	2
T9	2	2	3	1	1
T10	1	2	3	1	2
T11	2	2	2	2	1
T12	2	3	3	2	2
T13	2	2	3	2	2
13	$2x$ 40	$2x$ 46	x 37	x 16	x 21

Average Circumstances of Threat = (40+46+37+16+21) / 13 ≒ 12.31

적용하여 분석한 DCU의 보안 위협 상황 평균값은 Table 3.과 같이 12.31로 위협 등급 T7에 해당한다. 이에 따라 DCU 보호프로파일의 평가보증등급은 EAL 4로 산정할 수 있으며, 유사한 환경에서 운용되는 기기 보호프로파일인 정철조 등[3]이 제안한 스마트 미터 보호프로파일(EAL 5)과 독일에서 개발한 스마트 미터 게이트웨이 보호프로파일[4](EAL 4+)과 유사하다.

V. 결 론

본 논문에서는 DCU의 보안 취약점에 대해 살펴보고 보안 취약점에 따른 보안 요구사항을 파악하여 DCU의 보안성을 평가할 수 있는 CC v3.1 기반의 보호프로파일을 개발하였다. 본 논문에서 개발한 보호프로파일의 평가보증등급은 EAL 4 수준으로 산정되었다.

본 논문에서 개발한 보호프로파일을 이용하여 향후 국가 전력 기반 시설에 설치될 DCU의 보안성을 평가 및 인증하는 체계 구축에 기초자료로 활용할 수 있으며, DCU 개발자에게는 보안을 고려한 DCU 개발에 도움을 줄 수 있을 것으로 판단되며, DCU를 도입하고자 하는 유틸리티 또는 그 사용자에게 보안성을 확보한 제품 선정에 참고자료로 활용될 수 있다. 나아가 스마트그리드 기기와 관련된 보안성 평가 및 인증 체계 구축에 공통평가기준을 활용하는 방안을 고려할 경우 본 논문에서 개발한 DCU 보호프로파일을 참고하여 스마트그리드 기기 보안 규격 개발에 활용될 수 있을 것으로 판단된다.

References

[1] Gunhee Lee, Jungtaek Seo, and Eungki Park, "Analysis of Security Threats and Security Requirements on Smart Grid," Review of The Korea Institute of Information Security & Cryptology, 21(7), pp. 7-17, Nov. 2011.

[2] Jaeduck Choi and Jungtaek Seo, "Seperate Networks and an Authentication Framework in AMI for Secure Smart Grid," Journal of The Korea Institute of Information Security & Cryptology, 22(3), pp. 525-536, Jun. 2012.

[3] Chul-Jo Jung, Sun-Ki Eun, Jin-Ho Choi, Soo-Hyun Oh, and HwanKoo Kim, "Protection Profile for Smart Meters: Vulnerability and Security Requirements Analysis," Journal of The Korea Institute of Information Security & Cryptology, 20(6), pp. 111-125, Dec. 2010.

[4] BSI, "Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)," v1.3, Mar. 2014. (http://www.commoncriteriaportal.org/files/ppfiles/pp0073b_pdf.pdf)

[5] BSI, "Protection Profile for the Module of a Smart Meter Gateway(Security Module PP)," v1.02, Oct. 2013. (http://www.commoncriteriaportal.org/files/ppfiles/pp0077b_pdf.pdf)

[6] Justin Searle, "Advanced Metering Infrastructure Attack Methodology," BlackHat EU 2011, Mar. 2011.

[7] Sinkyu Kim, Yuseok Jeon, and Jungtaek Seo, "Study on Vulnerability test items for Advanced Metering Infrastructure,"

Review of The Korea Institute of Information Security & Cryptology, 22(5), pp73-78, Aug. 2012.
〔8〕 Florian Skopik, Zhendong Ma, Thomas Bleier, and Helmut Grüneis, "A Survey on Threats and Vulnerabilities in Smart Metering Infrastructures," International Journal of Smart Grid and Clean Energy, Vol. 1, No. 1, Sep. 2012.
〔9〕 Travis Goodspeed, "Extracting Keys from Second Generation ZigBee Chips," BlackHat USA 2009, Jul. 2009.
〔10〕 Kurt Rosenfeld and Ramesh Karri, "Attacks and Defenses for JTAG," Design & Test IEEE, Issue. 99, Mar. 2013.
〔11〕 SinSook Yoon, Daesuk Jang, HwanKoo Kim, SooHyun Oh, JaeCheol Ha, and SeokWoo Kim, "A Study of Evaluation Assurance Level Estimation Criteria for Development of Protection Profile," Review of The Korea Institute of Information Security & Cryptology, 17(6), pp57-66, Dec. 2007.

〈저자소개〉

사 진

조 영 준 (Youngjun Cho) 정회원
2008년 8월: 성균관대학교 컴퓨터공학과 졸업
2010년 2월: 성균관대학교 전자전기컴퓨터공학과 석사
2010년 2월~2011년 12월: 한국인터넷진흥원 주임연구원
2011년 12월~현재: 한국전자통신연구원 부설연구소 선임연구원
〈관심분야〉 스마트그리드 보안, 국가기반시설 보안, 보안성 평가・인증

사 진

김 신 규 (Sinkyu Kim) 정회원
2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터과학과 석사
2014년 2월: 연세대학교 컴퓨터과학과 박사
2003년 12월~현재: 한국전자통신연구원 부설연구소 선임연구원/실장
〈관심분야〉 스마트그리드 보안, 국가기반시설 보안, 취약점 분석