Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.703

EMS/SCADA의 DNP3 연계구간 보안성 평가·인증 기술 연구*

김 종 완,[1†] 손 태 식[2‡]
[1]아주대학교 컴퓨터공학과, [2]아주대학교 정보컴퓨터공학과

A Study of Security Certification and Accreditation for DNP3 linkage section in EMS/SCADA*

Jongwan Kim,[1†] Taeshik Shon[2‡]
1Division of Computer Engineering, Ajou University
[2]Division of Information Computer Engineering, Ajou University

요 약

기존의 EMS/SCADA에서 제어시스템과 필드디바이스 간의 연계시스템은 데이터의 신뢰성을 높이기 위해서 외부 네트워크와의 망 분리를 통한 접근 통제를 하였지만 현재는 운영의 효율성 증대와 체계적 관리, 경제적 측면을 고려한 외부 망과의 연결 필요성이 증가하고 있는 추세이다. 이런 발전한 연계구간은 과거에 비해 더 많은 보안 취약점을 갖게 되었으며, EMS/SCADA 연계구간에서의 통신은 특별한 관리 방법이 필요하다. 본 논문에서는 국내 환경을 고려하여 EMS/SCADA 연계구간에서 주로 사용되는 시리얼 DNP3와 TCP/IP기반 DNP3를 적용한 보안성 평가·인증기술을 제시하였다. 제시하는 보안성 평가·인증기술은 자원 안전성 테스트와 악성 패킷 테스트 2가지 세부 평가로 나누어 안전성을 평가하며 각각의 보안 요구사항 및 평가방법을 도출하여 기존의 평가·인증 기술들과의 차별성을 제시하고자 하였다.

ABSTRACT

The linking system between the control system and the field devices in the existing EMS/SCADA, in order to increase the reliability of the data, and access control through the separation of external network. Currently, There is a tendency that the need for connection to an external network that takes into account the economic aspect, systematic management and efficiency of operations is increasing. Such is evolved linkage section, is to have more security vulnerabilities than in the past, Eventually communication EMS/SCADA linkage section requires special management method. In this paper, taking into account the domestic environment, were presented the security Certification and Accreditation technology that was applied to serial DNP3 and TCP/IP based DNP3 that are mainly used in EMS/SCADA linkage section. Presented to security of Certification and Accreditation technology, divided into Resource Robustness Test and Malicious Packet Test for evaluate the safety. Each of the security requirements and evaluation method in proposed technology, is an attempt to present the differentiation of the existing Certification and Accreditation technology.

Keywords: Certification, Accreditation, Evaluation, DNP3, EMS/SCADA

접수일(2015년 4월 8일), 수정일(2015년 5월 12일), 게재확정일(2015년 5월 14일)

* 본 연구는 2015년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (No. 20131020402090)

† 주저자, jonglan@ajou.ac.kr
‡ 교신저자, tsshon@ajou.ac.kr(Corresponding author)

I. 서 론

EMS(Energy Management System)/SCADA(Supervisory Control And Data Acquisition)는 전력계통 전송 시스템과 발전 시스템의 성능을 최적화하기 위해서 제어 및 감시를 수행하는 시스템이다. 이러한 EMS/SCADA 시스템은 국가 주요 기반 시설의 근간이 되기 때문에 보안 사고가 발생할 시 막대한 금전적 피해뿐만 아니라 국가 안보에 위협이 될 수 있다.

과거에는 데이터 신뢰성을 높이기 위해 외부 네트워크와의 망 분리를 통하여 접근을 통제하였다. 그러나 현재 EMS/SCADA는 기존의 폐쇄적 통신망 및 전용 시스템에서 벗어나 운영의 효율성 증대와 체계적인 관리, 경제적 측면을 고려한 외부 망과의 연결 필요성이 증가되고 있는 추세이다. 아래 Fig.1.은 EMS/SCADA에서의 제어 센터(Control Center)와 변전소에 해당하는 필드 디바이스(Field Device)의 연계 구간을 국내 환경에 맞게 도식화한 그림이다[10].

해당 연계 시스템은 데이터 취득 및 관리, 원격제어와 같은 기능을 수행하게 된다. 이때 실시간 데이터의 전송은 데이터 수집을 관리하고 통신 가능한 프로토콜로의 변환을 해주는 FEP(Front End Processor)를 통해 필드 디바이스인 RTU(Remote Terminal Units)값을 직접 처리하는 방법과 Datalinker를 통해 지역변전소인 RCC(Regional Control Center)로부터 데이터를 취득하는 방법이 존재한다.

하지만 발전한 연계 시스템은 과거보다 더 많은 잠재적 취약점을 갖게 되었다. 예를 들어, 현재 전력제어시스템과 변전소간의 통신에서 쓰이는 전용프로토콜 중 하나인 DNP3 프로토콜은 보안을 고려하지 않았기 때문에 이에 대한 보안 취약점은 여전히 노출되어 있는 상황이다. 그 외에도 일반적인 네트워크와의 연계로 인해 TCP/IP 네트워크가 갖고 있던 사이버 공격 취약점과 연계로 인한 새로운 보안 위협에 노출되어 있다[8].

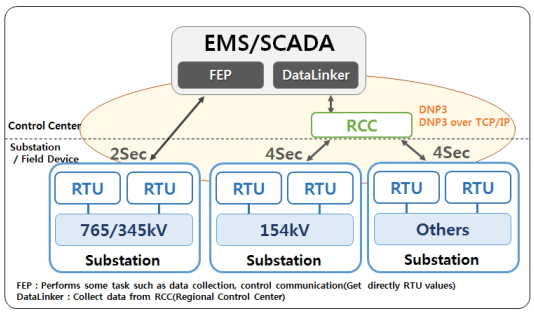

Fig. 1. EMS/SCADA linkage Section Structure

앞서 살펴본 바와 같이 보안 필요성이 증가함에 따라 EMS/SCADA 연계구간에서의 특별한 관리 방법이 필요하다. 보안성 평가·인증기술은 디바이스 구성 및 시스템에 대해서 관련 보안 표준들을 만족하고 있는지를 확인하고 잠재적인 취약점에 대한 방어 대책을 마련할 수 있다. 그리고 시스템의 안정적인 운영을 도모하기 위한 기초를 마련할 수 있다. 현재 보안성 평가·인증 제도는 특히 국외에서 활발히 진행되고 있으며, 실제 인증을 받은 제품의 사용 여부는 중요 사항으로 여겨진다. 이러한 이유로, 국내 환경을 고려하여 EMS/SCADA 연계구간에서의 평가·인증기술이 있어야 한다.

본 논문에서 2장은 EMS/SCADA 평가·인증기술 동향 분석을 하며, 3장은 제안하는 EMS/SCADA 기반의 DNP3 연계구간 보안성 평가·인증기술 제시한다. 4장은 논문에서 제시하는 연계구간 보안성 평가·인증기술과 기존 평가·인증기술들을 비교한다. 마지막으로 5장에서는 결론을 맺는다.

II. EMS/SCADA 보안성 평가·인증기술 동향 분석

현재 EMS/SCADA 제어시스템과 필드디바이스의 부분에 대해서 진행하는 기관 및 제도는 따로 없기 때문에 산업제어시스템 전반에 걸쳐 인증을 수행하는 대표적인 Achilles Certification과 ISASecure Certification 프로그램을 통하여 통신 보안성 인증 제도를 살펴본다.

2.1 Achilles Certification

Achilles Communication Certification은 ISA SP99의 국제 사이버 보안 표준과 NERC CIP 미국 정부 규제를 따르는지 확인하는 절차를 수행한다. 산업용 디바이스의 네트워크 안전성(robustness)을 점검하는 본 인증은 검사 강도에 따라서 2가지 레벨의 인증을 제공하며, 임베디드 장치와 호스트 기반 장치, 제어 응용프로그램, 네트워크 구성 요소 전반에 거쳐 수행할 수 있다. 레벨 1

은 대상 OS 레이어 2-4 계층 안의 신뢰성 및 견고성에 대해서 사전 정의된 정책을 따르고 있는지 확인하는 작업을 한다. 레벨 2는 레벨 1의 모든 항목을 포함한 확장된 형태로서 보다 엄격한 테스트와 많은 모니터링을 통하여 요구사항의 성공/실패를 점검한다. 또한 레벨 2는 ISASecure Certification의 인증을 연계하고 있다. 이런 각각의 인증 점검은 2가지 종류로 수행되며, Resource Exhaustion Test와 Invalid Packet Tests이다. Resource Exhaustion Test는 대상 디바이스의 특정 리소스를 소모(exhaust)시키는 테스트를 실시하여 이에 대한 안전성을 점검한다. Invalid Packet Tests는 대상 디바이스에 유효하지 않은 악성 패킷을 전송하여 이를 확인한다[12].

하지만 본 인증 기술은 ISA SP99표준과 NERC CIP 표준을 따른다는 명시만 존재할 뿐 평가·인증 제도에 대한 상세한 점검 요구사항을 알 수가 없다. 또한 EMS/SCADA 연계 시스템에서 주요하게 사용되는 DNP3 프로토콜에 대한 명시는 되어있으나 세부사항에 대한 언급이 부족하다.

2.2 ISASecure Certification 프로그램

EDSA(Embedded Device Security Assurance) CRT(Communication Robustness Testing)는 총 6가지(Ethernet, ARP, IPv4, ICMPv4, UDP, TCP) 프로토콜에 특화된 공통된 요구사항들을 통하여 임베디드 장치에 대한 안전성을 평가한다. CRT 인증 절차는 안전성(Robustness)을 확인하기 위하여 실제로 잘 알려진 취약점 및 네트워크 공격을 수행하여 성공/실패를 점검한다. CRT 기본 구성은 크게 6가지로 분류되며 총 69가지의 요구사항을 갖는다.

2010년부터 실질적인 규격 문서가 제공되었으며, 2011년 일부 업데이트를 수행하였지만 현재까지 문서의 추가 개정은 진행된 바가 없다. EDSA-CRT는 제어시스템 보안 관련 ISA/IEC 62443(ISA 99 국제표준)표준을 인증 절차의 근간으로 사용한다. 그리고 세 가지 보안 레벨을 두어 보안의 중요도를 나누고 있다. CRT와 같은 경우는 모든 보안 레벨에 관하여 동일한 평가를 수행한다[2].

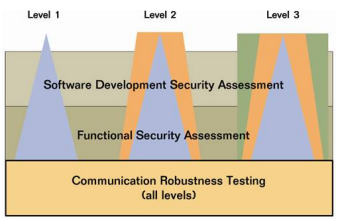

Fig. 2. ISASecure certification offer three levels of recognition for a device

EDSA-CRT는 기본적으로 임베디드 장비에 국한되어 있는 내용이 많으므로 시스템 전반에 있어 보안성을 평가한다고 보기 약하다. 또한 ISASecure Certification 프로그램은 아직 DNP3와 같은 전력제어시스템에서 사용되는 전용프로토콜에 대해서 연구 진행 중인 것으로 확인 되었다.

앞서 살펴본 보안성 평가·인증기관들은 국내 EMS/SCADA 연계구간에서 사용되는 DNP3에 대한 분석이 부족하고, 이에 평가하는 방법이 없기 때문에 실제로 국내 환경에 적용하기는 부족함이 있다고 볼 수 있다.

III. 제안하는 연계구간 보안성 평가 · 인증 기술

본 장에서는 EMS/SCADA 연계구간에서 국내 환경을 고려한 시리얼 DNP3 및 TCP/IP 기반 DNP3에 대한 보안성 평가·인증 기술을 제시한다.

3.1 제안하는 연계구간 보안성 평가 · 인증 구조

2장에서 설명한 Achilles Certification와 ISASecure Certification 프로그램과 마찬가지로 ISA 99/IEC 62443 표준을 근간으로 하여 EMS/SCADA 연계구간 보안성 평가·인증 기술을 제시한다. NIST 800-53/82를 통하여 통신평가를 위한 위험 관리 및 평가, 보안프로그램 개발, 산업제어시스템 보안구조, 보안기술 적용에 대한 내용을 참고한다. 연계구간에서 사용되는 프로토콜에 대한 내용은 IEEE 1815-2010 표준을 통한 DNP3와 RFC 문서들을 통한 TCP/IP 프로토콜을 참고하여 요구사항을 제시하고 전반적인 사이버 자산과 관련된 보안 사고를 확인, 분류, 대응, 보고하는 절차에 대한 내용은 NERC-CIP-008을 참고하였다.

통신의 안전성(Robustness)을 점검하기 위하여 실제로 알려진 취약점 및 네트워크 공격을 테스트하는 '통신평가'(Communication Evaluation)는 두 가지 레벨의 검사 강도를 갖는다. 레벨 1은 기본

적인 운영을 위해 최소한으로 필요한 요구사항을 제시하고 이를 확인한다. 각각의 평가에 대한 레벨 2 검사를 수행 시 엄격한 테스트와 더 많은 모니터링(Monitering)을 통하여 점검해야 한다.

'통신평가'는 자원 안전성 테스트와 악성 패킷 테스트 2가지 세부 평가로 나누어 안전성을 점검한다. 자원 안전성 테스트는 대상 DUT(Device Under Test)의 특정 리소스를 소모(exhaust)시키는 테스트를 실시하여 안전성을 점검한다. 악성 패킷 테스트는 대상 DUT에 유효하지 않은 악성 패킷을 전송하여 이를 확인한다. '통신평가'를 위한 평가·인증 제도의 기준이 되는 표준 및 가이드라인과 전체 구성은 아래 Fig.3.에서 살펴 볼 수 있다.

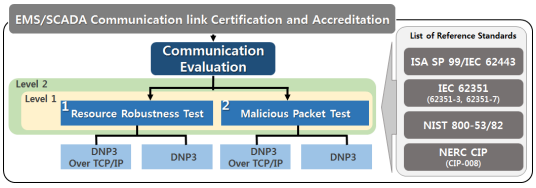

Fig. 3. Configuration of Accreditation system for Communication Evaluation

3.2 제안하는 연계구간 보안성 평가·인증 항목

제안하는 연계구간 보안성 평가·인증 세부 항목인 자원 안전성 테스트와 악성 패킷 테스트는 Achilles Certification와 ISASecure Certification 프로그램에서 수행하는 안전성 테스트 방식을 참고하여 따른다. 각각의 구성은 NERC CIP의 방식인 개요, 요구사항, 측정에 대한 목차를 갖는다. 또한 각각의 목차는 세분화된 요구 사항을 제시하여 점검 기준을 마련한다.

점검을 수행하는 동안 DUT는 정상 동작을 유지해야 하며 아래와 같은 동작이 발생 시 인증 실패라고 할 수 있다. 본 내용은 Achilles Certification 방식을 참고하였다[12].

- Program Instability : 테스트 수행 중 응용프로그램의 출동 또는 재시작
- Network Unavailability : 테스트 수행 중 네트워크 트래픽에 대한 응용프로그램의 응답 거부
- Excessive Resource Usage : 테스트 수행 중 중요한 메모리 누출(leak) 또는 비정상적인 CPU 이용률 발생

아래 Fig.4.는 통신평가를 위한 테스트 환경을 간략하게 도식화하였다.

자원 안전성 테스트 및 악성 패킷 테스트의 요구사항 및 측정방법은 국내 EMS/SCADA 연계구간에서 주요하게 사용되는 시리얼 DNP3 및 TCP/IP 기반 DNP3에 대해서 중점적으로 다루고 있다.

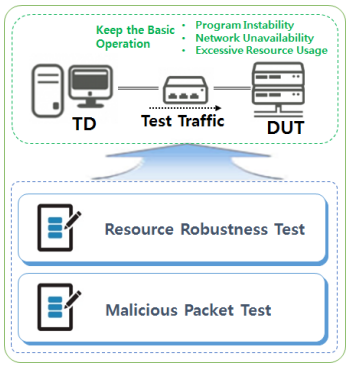

Fig. 4. Testing environment for Communication evaluation

3.2.1 자원 안전성 테스트

개요 : 대상 DUT의 특정 자원을 소모시키기 위한 테스트를 수행한다. 예를 들어, 해당 DUT의 메모리 자원을 오버플로우(Overflow)하기 위한 빠른 속도의 패킷을 보낸다.

요구사항 : EMS/SCADA 연계시스템에서 자원 안전성 테스트를 위한 요구사항이 존재하며 이를 만족해야 한다. 요구사항의 일부 목록과 내용은 Achilles Certification에서 참고하였다[12]. 아래에는 요구사항별 사용되는 용어에 대한 설명을 한다.

- 스톰(Storm) : 패킷을 처리하는 디바이스의 능력은 패킷 속도에 따라 다르므로, 스톰 테스트는 해당 DUT가 처리할 수 있는 최댓값을 결정하기 위해 다른 처리율 제한(Rate Limit)을 이용하여 여러 번 수행하도록 한다. 스톰 기능을 통해 생성된 패킷을 통하여 자원 안전성 테스트를 수행한다. 각 요구사항은 아래 Table 1.에서 확인 할 수 있다.

측정 : 요구사항에서 제시한 요구사항 별 측정 기준을 마련한다. 모든 측정 방법은 시리얼 DNP3 및 TCP/IP 기반 DNP3를 고려하여 작성되었다. 또한 level 2 이상의 더 높은 보안 평가·인증이 필요한 경우 기울임 글씨체로 표현하였다. 모든 측정은 해당 DUT 제어 및 동작 기능의 필수 서비스 유지 불가

Table 1. Basic Requirement for Resource Robustness Test

Requirement Name	Requirement Description
TCP/IP Unicast Storm	TD generate TCP/IP Packet storm at the Unicast way. and TD send packet storm to the DUT. Target DUT examine for robustness to control and operation of feature while dealing with the storm.
TCP/IP Multicast or Broadcast Storm	TD generate TCP/IP Packet storm at the Multicast or Broadcast way. and TD send packet storm to the DUT. Target DUT examine for robustness to control and operation of feature while dealing with the storm.
TCP/IP Fragmented Storm	TD generate fragmented TCP/IP Packet storm. and TD send packet storm to the DUT. Target DUT examine for robustness to control and operation of feature while dealing with the storm.
TCP/IP Scan Robustness	Target DUT examine robustness for excessive TCP/IP Port Scan Function. when DUT was connected external network or Internet.
TCP/IP SYN Flood	TD generate SYN Flood Packet. Target DUT examine for robustness to control and operation of feature while dealing with the many kinds of new connecting response.
TCP/IP LAND Attack	TD generate TCP/IP LAND Packet. in each packet the source and destination address are the same and the source and destination port are the same. Target DUT to continuously reply to itself.
DNP3 Serial Communication Storm	TD generate DNP3 Packet storm at the serial communication. and TD send packet storm to the DUT. Target DUT examine for robustness to control and operation of feature while dealing with the storm.
DNP3 Fragmented Storm	TD generate fragmented DNP3 Packet storm. and TD send packet storm to the DUT. Target DUT examine for robustness to control and operation of feature while dealing with the storm.
DNP3 LAND Attack	TD generate DNP3 LAND Packet. in each packet the source and destination address are the same and the source and destination port are the same. Target DUT to continuously reply to itself.
DNP3 Unsolicited Response Storm	TD generate Unsolicited Response Message storm when certain conditions are satisfied without a master request. and TD send packet storm to the DUT. Target DUT examine for robustness to control and operation of feature while dealing with the storm.
Keep the Unused Connection Attack	Attacks continue to maintain a connection after a successful connection. at this time, Target DUT examine for robustness to control and operation of feature.

및 정지와 같은 기본 동작을 유지 못할 시 실패로 간주하며, 성공/실패로 점검을 진행한다. 일부 목록과 내용은 Achilles Certification에서 참고하였으며 [12] 각 측정방법은 아래 Table 2.에서 확인 할 수 있다.

3.2.2 악성 패킷 테스트

개요 : 대상 DUT에 유효하지 않은 악성 패킷을 전송하여 테스트를 수행한다. 만일 EMS/SCADA 연계구간에서 상태 감시 및 운영에 있어 핵심적인 데이터들이 위·변조될 경우 제어 센터 기능이 무력화 될 수 있으며, 잘못 측정된 값에 의존한 잘못된 제어 명령은 전체 전력망이 마비되는 상황을 발생시킬 수 있다.

요구사항 : EMS/SCADA 연계구간에서 악성 패킷 테스트를 위한 요구사항이 존재하며 이를 만족해야 한다. 요구사항의 일부 목록과 내용은 Achilles Certification에서 참고하였다[12]. 아래에는 요구사항별 사용되는 용어에 대한 설명을 한다.

Table 2. Measurement Methods for Resource Robustness Test

Requirement Name	Measurement Methods
TCP/IP Unicast Storm	• The test case generates identical packets. • Each Packet contain a null payload and all flags are set to 'Zero' • The source address is set to the TD address and the destination address is set to the DUT address.
TCP/IP Multicast or Broadcast Storm	• The test case generates identical packets. • Each Packet contain a null payload and all flags are set to 'Zero' • The source address is set to the TD address and the destination address is set to the Multicast or Broadcast address.
TCP/IP Fragmented Storm	• The test does not send the final fragment, in an attempt to force the DUT to keep incomplete packets in memory(e.g. when an TCP/IP packet is larger than the maximum transmission unit(MTU) of a network segment over which it is to be sent, it must keep the fragments in memory until the final fragment is received) • The test case create a TCP/IP packet that is the maximum size(e.g. 65536 bytes) and fragment it to the maximum MTU size. • The test case then increments the packet ID and creates the next packet. • The Destination address is set to the DUT address.
TCP/IP Scan Robustness	• The test case generates identical packets. • Scan mode performed individually, such as SYN, ACK, FIN, connect, NULL, XMAS etc.
TCP/IP SYN Flood	• The test case should not be a new connection is set up because it does not transmit ACK message. • Setting Window size(e.g. 5000) and SYN flag • The source address of each packet is set to an unused address and the destination address is set to the DUT address.
TCP/IP LAND Attack	• The test case send LAND packets to all open TCP ports and adjacent TCP ports on the DUT(generate identical packets) • Setting Window size(e.g. 2048) and SYN flag • The source and destination addresses are set to the DUT address. The source and destination ports are equals.
DNP3 Serial Communication Storm	• The test case generates identical packets. • Each Packet contain a null payload and Sequence flags are set to 'Zero', Flag to determine whether the master is set to the master flag(e.g. flag value is '0') • The source address is set to the TD address and the destination address is set to the DUT address.
DNP3 Fragmented Storm	• The test does not send the final fragment, in an attempt to force the DUT to keep incomplete packets in memory(e.g. when an DNP3 packet is larger than the maximum transmission unit(MTU) of a network segment over which it is to be sent, it must keep the fragments in memory until the final fragment is received) • The test case create a DNP3 packet that is the maximum size(e.g. 292 bytes) • The test case then increments the packet ID and creates the next packet. • The Destination address is set to the DUT address.
DNP3 LAND Attack	• The test case send LAND packets to all open ports and adjacent ports on the DUT(generate identical packets) • The source and destination addresses are set to the DUT address. The source and destination ports are equals.
DNP3 Unsolicited Response Storm	• TD generate message storm of unsolicited response when using the change event between Binary input and analog input. • The source address is set to the TD address and the destination address is set to the DUT address.
Keep the Unused Connection Attack	• Continue to perform a TCP/IP connection(e.g. 3-way handshake) • TD generate a number of connection in each test packet repeatedly send invalid sequence number • TD generate a number of connection in each test packet repeatedly send FIN flag • The DUT continues to adequately maintain essential services

- 문법(Grammars) : 미리 정의된 목록(e.g. DNP-XML 도구 등)을 통하여 정상/비정상(Valid/Invalid) 패킷을 생성한다. 문법 기능으로 생성된 패킷을 통하여 악성 패킷 테스트를 수행한다.

- 퍼징(Fuzzing) : 랜덤(Random)한 헤더 값과 옵션 값으로 유효/비유효 한 패킷을 생성한다. 퍼징 기능을 통해 생성된 패킷을 통하여 악성 패킷 테스트를 수행한다. 각 요구사항은 아래 Table 3.에서 확인 할 수 있다.

측정 : 요구사항에서 제시한 요구사항 별 측정 기준을 마련한다. 모든 측정 방법은 시리얼 DNP3 및 TCP/IP 기반 DNP3를 고려하여 작성되었다. 또한 level 2 이상의 더 높은 보안 평가·인증이 필요한 경우 기울임 글씨체로 표현하였다. 모든 측정은 해당 DUT 제어 및 동작 기능의 필수 서비스 유지 불가 및 정지와 같은 기본 동작을 유지 못할 시 실패로 간주하며, 성공/실패로 점검을 진행한다. 일부 목록과 내용은 Achilles Certification에서 참고하였으며[12] 각 측정방법은 아래 Table 4.에서 확인 할 수 있다.

Table 3. Basic Requirement for Malicious Packet Test

Requirement Name	Requirement Description
TCP/IP Fuzzing	TCP/IP fuzzing generates valid/invalid packets using randomized header values. Target DUT examine for robustness to control and operation of feature while dealing with the fuzzing test(e.g. fragmented Invalid packet).
TCP/IP Grammar - Urgent Data	TD generate TCP/IP Grammar Urgent data. Urgent data examines how the DUT handles unauthorized packets containing an urgent flag.
TCP/IP Grammar - Fragmentation	Fragmentation generated Packets with invalid fragmentation and send them to the DUT. The grammar examines the DUT's ability to maintain control while processing or discarding invalidly fragmented packets.
TCP/IP Grammar - Port	TD generate TCP/IP Grammar port number. Implementations that do not defined the port number as an unsigned number are expected to malfunction.
DNP3 Fuzzing	DNP3 fuzzing generates valid/invalid packets using randomized header values. Target DUT examine for robustness to control and operation of feature while dealing with the fuzzing test(e.g. fragmented Invalid packet).
DNP3 Control Command	TD sends the invalid control command to the DUT.
DNP3 Initialization	TD sends the invalid initialization command to the DUT.
DNP3 Unsolicited Response Enable&Disable Command	TD sends the invalid unsolicited response command to the DUT.
DNP3 Assign Class Command	TD sends the invalid assign class command to the DUT.
DNP3 Write Command	TD sends the invalid write command to the DUT.
DNP3 Malformed Message Attack	TD generate messages that do not defined the protocol spec or erroneous message sequence. Target DUT examine for robustness to control and operation of feature while dealing with the test.

Table 4. Measurement Methods for Malicious Packet Test

Requirement Name	Measurement Methods
TCP/IP Fuzzing	• The test case generates invalid packets and fragmented packets using randomized values. • TD send invalid intial sequence number to the DUT. • TCP/IP packet generate larger than the MTU value or smaller than 20bytes which it is to be sent, • TD send invalid CRC value to the DUT. • TD includes non-null TCP/IP option fields in some of its TCP/IP option. some of these option fields are malformed or undefined options. • TD includes one or more of the TCP/IP options MSSN, WSN, SACKN, POCR and ACR, which it is to be sent. • The source and destination addresses are set to the DUT address.
TCP/IP Grammar - Urgent Data	• Packet flags are set to URG flag and Urgent Pointer. • Packet lengths is within the range[(DataOffset of Header * 4) ~ (DataOffset of Header * 4 + UrgentPointer)] which it is to be sent. • Transfer with normal packet and URG flag packet to the DUT(DUT continues to adequately maintain essential service).
TCP/IP Grammar - Fragmentation	• TD generates TCP/IP packets with invalid fragmentation and sends them to the DUT. • TD examines the DUT's ability to maintain both control and monitoring while processing or discarding invalidly fragmented packet.
TCP/IP Grammar - Port	• TD attempts to establish TCP/IP connections with the DUT on both port zero(0x0000) and port 65535(0xFFFF). • DUT is expected to respond to the connection establishment request TD. The expected another case response consists of a TCP/IP with the RST flag.
DNP3 Fuzzing	• The test case generates invalid packets and fragmented packets using randomized values. • DNP3 packet generate larger than the MTU value. • TD send invalid CRC value to the DUT. • TD includes non-null TCP/IP option fields in some of its TCP/IP option. some of these option fields are malformed or undefined options. • Signal transmission having more than 4 second time period(e.g. average transmission time = 4 second). • The header source and destination addresses are set to the DUT address.
DNP3 Control Command	• The control command signal to manipulate the command code 3,4(select and oprate) and 5(direct operate), and sent to the DUT..
DNP3 Initialization	• A signal to operate the command code 14(warm restart) to initialize the event queue, setting value. and sent to DUT.
DNP3 Unsolicited Response Enable&Disable Command	• A signal to operate the command code 20(Enable Unsolicited) to execute the Unsolicited Response function, and sent to DUT(Causing unnecessary traffic). • A signal to operate the command code 21(Disable Unsolicited) to stop the Unsolicited Response function, and sent to DUT(Interfering with the reporting of important event).
DNP3 Assign Class Command	• A signal to operate the command code 22(Assign class) to newly registered the data point. and sent to DUT.
DNP3 Write Command	• A signal to operate the command code 2(write) to implemented 'Time and Data' object, and sent to DUT.
DNP3 Malformed Message Attack	• A signal that CROB(Binary Output Command) object data of the request message is missing, and sent to the DUT. • A signal that Application payload of DNP3 message is missing, and sent to the DUT.

IV. EMS/SCADA 보안성 평가·인증 기술 비교

4장에서는 Achilles Certification와 ISASecure Certification 프로그램 그리고 본 논문에서 제시하는 EMS/SCADA 연계구간 보안성 평가·인증 기술을 비교하여 기존 평가·인증 방법과의 차별성에 대해서 분석하도록 한다. 비교 항목의 순서는 각 평가·인증 기술의 적용 범위와 EMS/SCADA 구간의 전용프로토콜인 DNP3 고려 여부, 실제로 평가를 수행하기 위한 요구사항 및 평가방법 제시 마지막으로 국내 환경에서의 적합성 순으로 진행한다.

Achilles Certification 통신 인증 (Communication Certification)의 평가 대상은 이미 전 세계 많은 산업제어시스템의 제조업체에서 사용되고 있으며 대표적 협력 기업으로 CISCO, SIEMENS, WIND RIVER 등이 있다. DNP3 고려 여부에 대해서 프로토콜 테스트 항목에는 존재하지만 구체적인 세부사항에 대한 언급이 부족하다. 또한 레벨 2 검사 강도는 ISASecure Certification 프로그램의 플랫폼을 통해서 통신 안전성을 평가하고 있기 때문에 아직 DNP3에 대한 고려가 부족한 것으로 판단된다. 평가·인증을 위한 요구사항은 존재하지만 보안성 평가 방법에 대한 제시가 구체적이지 못하고, 테스트 항목의 목록만 간단하게 작성되어 있다. 위와 같은 이유로 아직 국내 환경 적합성이 부족할 것이라 예측된다.

ISASecure Certification 프로그램의 인증 절차 중 통신 평가에 해당하는 CRT 기술에 대해서 살펴보도록 한다. CRT는 미국에서 시작되어 전 세계 산업제어 자동화 시스템 및 제품을 평가 대상으로 두고 있다. 하지만 인증 프로토콜 항목에 아직 DNP3와 같은 전용 프로토콜에 대한 내용이 없고 향후 연구 과제로 분류해 두었기 때문에 DNP3만의 특정 취약점 및 네트워크 공격을 테스트하였다고 보기 어렵다. 또한 CRT 인증기술은 각각의 테스트 요구사항에 대한 내용이 자세하게 구성되어있지만 측정 방법이 존재하지 않기 때문에 실제 환경에 맞추어 평가할 방법 마련이 모호하다. 즉 현재 CRT 인증 기술은 국내 EMS/SCADA 연계구간에 적용하기 어려울 것이라 판단된다.

Achilles Certification와 ISASecure Certification 프로그램 및 본 논문에서 제시하는 보안성 평가·인증 기술에 대해서 간략하게 비교분석한 내용을 아래 Table 5.에서 확인할 수 있다.

국내 EMS/SCADA의 연계구간에서 필드디바이스와 제어 센터 사이의 통신은 시리얼 기반 DNP3가 많이 사용되고 있고, 향후 설비 계획에도 주요하게 사용될 DNP3을 고려한 보안성 평가·인증기술의 제시는 본 논문의 차별화된 필요성을 강조한다고 볼 수 있다. 또한 각각의 요구사항을 실제 어떤 방식으로 점검해야하는지 평가방법을 제시함으로써 국내 환경에 대한 더 높은 적합성을 보일 수 있을 것이라 예측해 볼 수 있다.

V. 결 론

EMS/SCADA는 주요 기반 시설의 근간이 되기 때문에 보안 위협에 대한 보안성 평가·인증제도 및 기술이 필요하다. 하지만 현재까지 국내 보안성 평가·인증 기술은 아직 부족하고 잠재적 취약점과 위

Table 5. A Comparative Analysis of Security Certification and Accreditation

	Achilles Certification (Comm. certification)	ISASecure Certification (CRT)	Proposed technique (Comm. Evaluation)
Target of Evaluation	Industry Control System	Industry Control System	EMS/SCADA DNP3 comm. link
Consider of DNP3	△	X	O
Suggest a Requirement	O	O	O
Suggest a Measurement Methods	△	X	O
Domestic Compatibility	△	X	O

협에 대한 방어 대책을 마련하기 위해서 본 연구를 진행하게 되었다. 상대적으로 국외의 제어시스템 관련 보안성 평가·인증 제도는 활발히 진행되고 있는 추세이며 대표적인 Achilles Certification와 ISASecure Certification 프로그램은 이미 많은 산업제어시스템 개발업체들과 협력하여 보안 위협을 줄이고자 노력하고 있다. 또한 실제 인증을 받은 제품의 사용 여부는 매우 중요한 사항으로 여겨진다. 그러나 앞서 설명한 두 평가·인증 기술은 현재 국내 EMS/SCADA의 연계구간에서 주로 사용되는 DNP3 프로토콜에 대한 연구가 아직 진행 중이거나 미비한 상황이다. 또한 각각의 평가·인증을 위한 요구사항별 측정방법이 존재하지 않기 때문에 실제 국내 환경에 맞춘 연구가 필요하다.

이러한 점에서 본 논문은 'EMS/SCADA의 DNP3 연계구간 보안성 평가·인증기술'을 제시하였다. EMS/SCADA 연계구간에서 주로 사용되는 시리얼 DNP3와 TCP/IP기반 DNP3를 고려하였으며 제안하는 보안성 평가·인증 항목은 자원 안전성 테스트와 악성 패킷 테스트 2가지 세부 평가로 나누어 안전성을 점검한다. 또한 각각의 항목은 보안 요구사항에 대한 측정방법을 두어 기존의 평가·인증 기술들과 차별화된 내용을 제시한다. 향후 연구 방향은 국내 EMS/SCADA에서 사용되는 다른 프로토콜들(ICCP, OPC, Modbus 등)에 대해서 연구를 진행할 계획이다. 또한 보안기능과 초기 구성 상태에 대해서 보안 요구사항을 만족하는지 확인하는 '기능평가' 측면을 추가 보완할 예정이다.

본 논문은 전력망과 정보통신기술(ICT)*의 융합 및 발전하는 스마트그리드 시장에 의한 증가된 보안 위협을 분석하는 사전연구가 될 것이라 기대한다. 또한 향후 EMS/SCADA 연계구간의 안정적인 운영을 도모하고 최소한의 보안 조치 마련을 위한 국내 보안성 평가·인증제도 및 기술 개발에 기여할 수 있다고 생각한다.

References

〔1〕 ISA-SP99, "Security for Industrial Automation and Control System, Part 4:Technical Security Requirements for an Industrial Automation and Control Systems," Draft 1, Edit 2, Mar. 2008.

〔2〕 EDSA-406, http://www.isasecure.org/en-US/Documents/EDSA-406-TCP-robustness-test-spec(v1_41)

〔3〕 FORCE, JOINT TASK, and TRANSFORMATION INITIATIVE. "Security and privacy controls for federal information systems and organizations." NIST Special Publication 800 (2013): 53.

〔4〕 Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication (2011): 800-82.

〔5〕 NERC CIP-008, Cyber Security-Incident Reporting and Response Planning, NERC, Jun. 2006

〔6〕 IEEE, "IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)," IEEE Std. 1815-2012 (Revision of IEEE Std. 1815-2010), 2012.

〔7〕 Erfan Ibrahim, "Overview of DNP3-SA," IEC 62351, Dec. 2013.

〔8〕 Moon-su Jang, Gun-hee Lee, Sin-Kyu Kim, Byung-gil Min, Woo-nyon Kim, Jun-taek Seo, "Testing Vulnerabilities of DNP3," Journal of Security Engineering, 7(1), pp. 15-28, Feb. 2010.

〔9〕 C.C. Michael, Ken van Wyk, and Radosevich, "Black Box Security Testing Tools," Cigital, Dec. 2005.

〔10〕 Hyosang Lee, Wanhong Kim, Minryung Park, Yeojun Yoon, "A Study of SCADA Function Specific Design in Korean EMS," Proceeding of The Transactions of Korean Institute of Electrical Engineers Summer Conference, pp.402-403, Jul. 2007.

〔11〕 Tsutomu Yamada, Tadashi Kaji, Dr.Info, "Trends and Development in Security Standards for Secure Social Infrastructure Systems," Hitachi Review, Vol.63, No.5, 2014

〔12〕 The Achilles Certification Program, http://www.wurldtech.com/product_services/certifications/achilles_communications

_certification/
〔13〕 Andre Teixeira, Gyorgy Dan, Henrik Sandberg, Karl H. Johansson, "A Cyber Security Study of a SCADA Energy Management System: Stealthy Deception Attacks on the State Estimator," in Proc. of IFAC World Congress, Aug. 2011.
〔14〕 Giani, Annarita, et al. "The VIKING project: an initiative on resilient control of power networks." ISRCS 2009-2nd International Symposium on Resilient Control Systems; Idaho Falls, ID; 11 Aug. 2009.
〔15〕 Falliere, Nicolas. "Stuxnet introduces the first known rootkit for industrial control systems," Published online at http://www. symantec. com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices. Last accessed on Feb. 2011.
〔16〕 Tae-sik Kim, Dong-joo Kang, "A Study on Identification and Classification of Cyber Security Threats on Electric Power System," Journal of Security Engineering, 9(1), Feb. 2012.

〈저자소개〉

김 종 완 (Jongwan Kim) 학생회원
2013년 7월: 아주대학교 정보컴퓨터공학부 졸업
2013년 8월~현재: 아주대학교 대학원 석사과정
〈관심분야〉 전력제어시스템 보안, 스마트그리드, 디지털 포렌식, 비정상행위탐지

손 태 식 (Taeshik Shon) 정회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월: 아주대학교 정보통신전문대학원 공학석사
2005년 8월: 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월: Research Scholar, University of Minnesota
2005년 8월~2011년 2월: 삼전전자 DMC 연구소 책임연구원
2011년 3월~현재: 아주대학교 정보통신대학 정보컴퓨터공학과 조교수
〈관심분야〉 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지, ICT융합보안