Journal of the Korean Institute of Illuminating and Electrical Installation Engineers (2010) 24(4) : 50~56
DOI 10.5207/JIEIE.2010.24.4.050

논문 24-4-7

SCADA 시스템의 보안성 평가를 위한 테스트베드 구성

(A SCADA Testbed Implementation Architecture for Security Assessment)

이종주* · 김석주 · 강동주**
(Jong-Joo Lee · Seog-Joo Kim · Dong-Joo Kang)

요 약

집중 원격감시 제어 또는 감시제어 데이터 수집 시스템인 SCADA(Supervisory Control And Data Acquisition) 는 기존의 국지적인 산업용 네트워크 기반의 제어시스템이 정보통신 기술의 발전으로 광역화 되면서 전력, 가스, 상하수도, 교통시스템 등 주요 기반시설에 적용되어 분산제어와 공정제어 시스템으로 사용되고 있다.

SCADA 시스템의 중요성과 사고시 미치는 파급효과를 고려하여 구성 장치 및 통신 설비들에 대한 사이버 보안(cyber security) 인식이 점차 높아지고 있으며, SCADA 시스템의 취약성 분석과 보안성 확보에 대한 연구가 이루어지고 있다.

본 논문에서는 현장에서 운용중인 상용 SCADA 시스템의 계층구조와 통신 사양 및 규약을 고려하여 보안성 평가를 위한 테스트베드를 제안하고자 한다. 특히 계측·제어 명령을 수행하는 RTU, IED와 같은 단말 장치의 직렬통신 구간에서 보안성 평가를 수행하기 위한 물리적 접속과 평가 절차를 제시하였다.

Abstract

Supervisory Control and Data Acquisition Systems (SCADAs) is real-time monitor and control systems. SCADA systems are used to monitor or control chemical and transportation processes, in municipal water supply systems, electric power generation, transmission and distribution, gas and oil pipelines, and other distributed processes. SCADA refers to a large-scale distributed system. The supervisory control system is placed on top of a real time control system to control external processes.

Emerging security technologies and security devices are decreasing the vulnerability of the power system against cyber threats. Dealing with these threats and analyzing vulnerabilities is an important task for equipment such as RTU, IED and FEP.

To reduce such risks, we develop such a SCADA testbed. This paper presents the development of a testbed designed to assess the vulnerabilities SCADA networks(including serial communication).

Key Words : SCADA Security, SCADA Testbed, Security Assessment, SCADA Testbed Structure

* 주저자 : 한국전기연구원 위촉선임연구원
** 교신저자 : 한국전기연구원 선임연구원
Tel : 031-420-6188, Fax : 031-420-6189, E-mail : jongjoo@keri.re.kr
접수일자 : 2010년 11월 3일, 1차심사 : 2010년 11월 6일, 심사완료 : 2010년 1월 26일

1. 서 론

집중 원격 감시 · 제어 또는 감시 · 제어 데이터 수집 시스템인 SCADA(Supervisory Control And Data Acquisition)는 기존의 국지적인 산업용 네트워크 기반의 제어시스템이 정보통신 기술의 발전으로 광역화되면서 전력, 가스, 상하수도, 교통시스템 등 주요 기반시설에 적용되고 있다. 이러한 SCADA 시스템은 분산제어(Distributed Control)와 공정제어(Process Control) 형태로 활용되고 있다. 기반시설을 구성하는 SCADA 기기들은 짧게는 수 [km], 멀리는 수백 [km]의 원거리에 위치하고 있으며, 전용선, 인터넷, 전화선, 무선통신 등과 같은 다양한 형태의 통신 방식과 경로를 이용하여 중앙 제어시스템과 연계된다[1-2].

SCADA 시스템의 중앙 계측 · 제어 서버는 원격 단말 통신 장치인 RTU(Remote Terminal Unit) 또는 IED(Intelligent Electronic Device)와 연결된다.

SCADA 통신에 사용되는 규약은 DNP(Distributed Network Protocol), Modbus, Harris, TCP/IP, ICCP(Intercontrol Center Communications Protocol) 등 다양한 방식들을 채용하며, 각 규약들은 시스템의 구조와 제어 등급 그리고 계측 · 제어 대상에 따라서 결정되며 다수의 규약들이 혼용되기도 한다[1-2].

SCADA 통신 규약들은 통신환경에 최적화된 것으로 안정성(stability)과 효율성(efficiency) 그리고 유연성(flexibility)을 제공한다. 하지만, 개방된 상용 규약은 일반 사용자나 조작자가 해당 통신 규약의 사양서나 제작사의 설명서를 이용하여 장치들을 구비하거나 통신 프레임을 분석할 수 있다. 이는 해당 통신 규약이 갖는 여러 가지 장점에도 불구하고 공개된 정보를 활용하여 SCADA 시스템에 불필요한 접근이나 악의적 수단으로 사용될 수 있다는 단점을 갖는다.

전력망 및 교통망과 같은 중요 사회 인프라에 사용되는 SCADA 시스템에 예기치 않은 사고나 통신망 침입으로 정보 유출과 특정 정보에 대한 위조 · 변조 등의 악의적 공격이 발생할 경우 이로 인한 피해와 파급효과는 상상할 수 없을 정도이다. 실제로 외국의 경우 이러한 피해 사례와 위협들이 보고되고 있다[3-6]. 이처럼 SCADA 시스템을 구성하는 장치 및 통신 설비들에 대한 사이버 보안(cyber security) 인식이 점차 높아지고 있다. 특히, 유럽과 미국의 경우 국가적 차원에서 에너지 관련 분야와 주요 설비들을 시작으로 SCADA 보안성 확보를 위한 연구가 이루어지고 있으며, 관련 장비 제작사와 연구소의 협력을 통한 표준화 기구의 구성과 공동연구가 진행 중이다[6-12].

본 논문에서는 SCADA 통신 규약으로 널리 사용되고 있는 Modbus와 DNP 방식을 채용한 시스템의 보안성 평가를 위한 테스트베드 구성과 주요 장비들의 보안성 평가 항목들을 제안한다. 특히 계측 · 제어를 수행하는 하위 계층의 RTU, IED, MTU(Master Terminal Unit), FEP(Front End Processor) 등과 같은 장치들의 직렬(RS232, RS485) 통신 구간에 접속하여 사이버 보안성 평가를 위한 모의 해킹 방법을 제안한다.

2. SCADA 테스트베드의 구성

2.1 SCADA 시스템 구조

SCADA 시스템은 계측 · 제어 장치와 RTU 또는 IED 등 단말 장치의 취득 데이터를 FEP를 통하여 상위 계층으로 전송하거나 상위의 제어 명령을 전달하는 다중 통신장치로 구성된다.

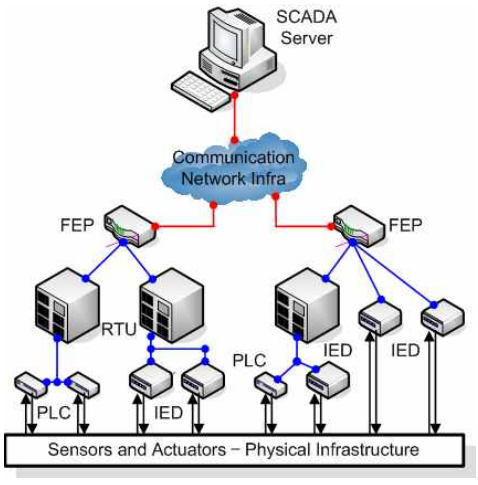

그림 1. SCADA 시스템의 구조
Fig. 1. Network Structure of a SCADA System

그림 1은 일반적인 SCADA 시스템 구조를 나타낸 것이다. FEP를 기준으로 상위 계층은 고속, 하위 계층은 저속 통신 구간으로 구분된다. RTU는 하위에 PLC(Programmable Logic Controller)나 IED 장치를 연계하고, IED의 경우 직접 FEP를 연계하거나 수용하는 구조를 갖는다[1-2]. 각 장치의 통신 포트와 통신 선로는 중요도와 우선순위에 따라서 2회선 이상의 예비(backup/redundant) 선로를 갖는다. SCADA 네트워크와 일반적인 정보통신 네트워크와의 차이점은 다음의 표 1에 나타난 바와 같다[1-5].

표 1. SCADA 네트워크 특징 비교
Table 1. Feature of SCADA Network

	SCADA	정보통신
실시간	실시간 처리	빠른 처리
처리방식	분산 제어	중앙 집중 제어
규약/표준	다양한 규약 이기종 수용	전체 구조가 표준화된 규약
운용	연속적인 운용 주기적	비 정기(비 주기)적 운용
정책	무결성>가용성>보안성	보안성>무결성>가용성
오류/복구	결함/오류 처리	데이터 무결성
용도	계측·제어	정보 전송
대상	전력, 교통제어, 생산(제조) 등	전산 업무, 금융, 전자결제 등

SCADA 시스템에서는 상위 서버의 요청이나 하위에서 발생한 이벤트 전송 및 서버 요청에 대한 응답 속도와 임계 시간 내(deadline) 처리가 중요한 요소이다. 즉, 정해진 시간 내에 처리된 정보를 정확히 전달하는 무결성이 SCADA 통신 정책의 최우선 순위이며, 오류 또는 결함 발생시 이를 허용하고 처리하기 위한 방안이 필요하다. SCADA 네트워크를 구성하는 각 장치 노드(node)들은 계층 구조와 지역 및 환경적 요인에 따라서 복수개의 통신 규약을 수용하거나 이 기종 장치의 접속을 허용한다.

2.2 SCADA 테스트베드 구성 조건

SCADA 테스트베드는 현장에서 사용되는 장치들의 사양과 기능 그리고 통신 규약 및 계층 구조를 반영하여 구성된다[13-14]. 다음 사항들은 보안성 평가를 위한 테스트베드의 구성 조건을 나열한 것이다.

- 표준화된 SCADA 통신 규약 채용
- 이 기종간의 접속 허용
- 분산 처리를 위한 계층 구조
- 보안성 평가를 위한 모의 공격 가능
- 외부 공격에 대한 방어 툴 제공
- 진단 및 평가 툴 제공
- 장치의 개별 조작 및 동작 방법 제공
- 사용자 정의 모의 정보 프레임 전송 제공

SCADA 테스트베드 구성 조건을 수용하기 위하여, 고속 통신을 수행하는 FEP 상위 계층에서는 침입탐지시스템(IDS, Intrusion Detection System), 침입방지시스템(IPS, Intrusion Prevention System) 그리고 저속 통신 구간인 하위 계층에서는 프로토콜 분석 도구가 필요하다. 네트워크 분석 도구의 접속과 분석 대상 구간을 평가자가 선택하기 위하여 SCADA 테스트베드를 구성하는 장치들의 통신 포트는 예비 포트와 지역적 또는 계층별 절체(차단)와 (재)연결이 가능한 이중(다중)화 통신 선로를 갖도록 한다. 서버측에서는 요청에 대한 응답속도 및 오류 발생빈도 측정과 최상위에서 말단 장치간에 전달되는 송·수신 프레임의 비교 기능이 필요하다.

따라서 이상의 보안성 평가를 위한 구성 조건과 기능들을 수용하고 기존 SCADA 네트워크와 통신흐름에 영향을 주지 않는 통신부 인터페이스와 연계방안이 구비되어야 한다.

2.3 보안성 평가 방법

SCADA 시스템의 보안성 평가는 서버 프로그램과 MTU, RTU. IED 등 각 설비들의 운영 프로그램(OS 포함)에 대한 분석이 선행되어야 한다.

선행 분석 후 SCADA 구성 장치들의 입·출력 단자, 통신 포트 그리고 각 구간에 대한 보안성 평가와 취약성 진단을 수행한다. 또한 이 기종 기기 연동을 위한 변환 장치와 네트워크 연계 장치에 대한 취약성 분석으로 전체 SCADA 시스템의 보안성을 점검할 수 있다[6,10-11,15-16]. 다음의 항목들은 기본적인 보안성 평가 대상과 항목을 나열한 것이다.

- 네트워크 구조

· 원격지 접속 및 통신회선 관리
· 바이러스 대비책
· 고장 복구 및 사고 대비 능력
· 물리적 보안
· 시스템 감시 기능
· 무선 통신 및 네트워크 침입 경로 취약성 관리
· 보안 패치 및 절차
· 운전원/관리자 보안성 검토 및 교육
· 암호 및 계정 관리
· 엄격한 접근 · 제어 관리 정책
· 장비 접속 절차 및 인증

보안성 평가를 위한 SCADA 테스트베드는 여러 가지 형태의 통신장애와 침입 및 교란 공격 등에 대한 모의가 가능하도록 설계되며, 보안성 평가 수행을 위하여 다음에 나열한 해킹(hacking) 방법들의 모의가 가능하여야 한다.

· 위장하기(spoofing)
· 재생공격(replay attack)
· 서비스거부(DoS, denial of service)
· 세션 하이재킹(session hijacking)
· 스니핑(sniffing)

위장하기(spoofing)는 다른 시스템의 신뢰 관계를 속여서 침입하는 해킹 기법으로 비교적 상위 수준의 기술적 요소가 필요하며 다음과 같은 종류들로 구분된다.

· IP spoofing : 목표로 하는 호스트(target host)와 신뢰관계를 맺고 있는 다른 호스트로 공격자의 IP 주소를 속여서 패킷을 보내는 기법
· DNS spoofing : 목표로 하는 호스트가 이용하는 도메인 네임서버(Domain Name Server)에 가짜 DNS 레코드를 전달함으로써 목표로 하는 호스트가 잘못된 주소 정보를 이용하게 하는 기법
· login spoofing : 목표로 하는 호스트에서 가짜 login 프로그램 실행으로 비밀 번호를 파악하는 기법

위장하기 공격은 먼저 네트워크 프로토콜에 대한 분석이 완료된 후 공격이 가능하며, 계층별로 운용되는 장치들을 구분하여 해킹함으로서 단계적 또는 계층별 보안 성능을 확인할 수 있다.

재생공격(replay attack)은 네트워크상의 정보 프레임을 수집한 뒤 해당 메시지를 재전송함으로서 갱신되지 않은 정보의 전달이나, 대상 설비에게 정당한 정보 전송으로 인식시켜 오류를 유도하는 기법이다. 수집된 정보의 재전송으로 공격대상 장치의 오류 발생 빈도를 측정함으로서 취약성을 평가한다.

서비스거부(DoS)는 시스템의 정상적인 동작을 방해하는 공격으로 대량의 데이터 패킷을 통신망으로 보냄으로 통신 회선을 선점하고, 서버의 자원을 고갈시키는 방법이다. 비정상적으로 많은 자원 요구를 받게 된 서버 시스템은 정상적인 서비스를 제공할 수 없게 된다. 이러한 서비스거부 공격은 현재 분산서비스거부(DDoS, distributed DoS) 공격이나 분산반사서비스거부(DRDoS, distributed reflection DoS) 공격으로 발전하고 있다. 서비스거부 공격에서는 회선 점유 시간과 데이터 패킷의 크기를 제어함으로 해당 설비의 통신 불능 한계와 대처 방안을 평가할 수 있다.

세션 하이재킹(session hijacking)은 정당한 사용자 또는 인증 받은 접속 수행 이후의 세션을 가로채는 보안 공격 기법으로 해당 네트워크상에서 인증 이후의 접근 가능한 모든 정보를 획득한다.

스니핑(sniffing)은 통신 네트워크에 송 · 수신되는 정보(traffic)을 감시하고 장시간 수집된 정보와 전송되는 정보들의 패턴을 분석함으로서 필요한 정보를 획득하는 기법을 말한다. 스니핑으로 수집된 정보는 통신 프레임의 패턴과 유사성 또는 반복성을 계산하여, 해당 시스템의 취약성을 평가한다.

상기 나열한 보안성 평가 방법들은 SCADA 네트워크를 구성하는 통신 모듈과 방화벽, 침입탐지시스템(IDS), 침입방지시스템(IPS) 뿐만 아니라 RTU, IED, FEP 등 단말 장치들의 장애극복(Fail-over), 결함 허용(fault-tolerance), 이중화(replication) 처리 능력과 운용상의 안정성 평가에도 활용한다.

2.4 통신부 결선 및 연계방법

SCADA 구성 장치들의 통신부 연계방법은 상위 계층의 고속 통신부와 하위 계층의 저속 통신부로 구분되며, 기존 통신 흐름에 영향을 미치지 않는 방법을 채택한다. FEP 통신 장치를 기준으로 상위 계층은 다중

접속이 가능한 Ethernet급 이상의 고속 통신망으로 구성된다. 상위 계층의 고속망은 공중망을 이용하거나 감시·제어 대상의 중요도와 신뢰도에 따라서 타 시스템이나 네트워크의 간섭이 없는 별도의 전용회선이나 임대 회선을 이용한 단독 또는 독립 네트워크로 구성된다. 상용 공중망을 이용하는 경우 VPN(Virtual Private Network) 장치를 이용하는 가상사설망 형태를 갖는다. SCADA 고속 통신망을 구성하는 장치들은 대부분 통신 규약을 고려하여 제작된 전용 장비보다는 대부분 일반 정보통신망에 사용되는 설비와 장치들이 사용된다[1-2,7]. 일부 RTU나 IED 장치는 FEP를 사용하지 않고 모뎀(modem)을 이용하여 상위 계층과 네트워크 연결을 시도한다. 따라서 테스트베드 상에서 고속 통신부 결선 및 연계방법은 게이트웨이(Gateway), 리피터(Repeater), 브리지(Bridge), 라우터(Router)와 같은 통신 중계 장치들의 예비 포트 접속이나 서버와 공중전화망(PSTN, public switched telephone network)등의 우회 경로를 통한 접속으로 가능하다.

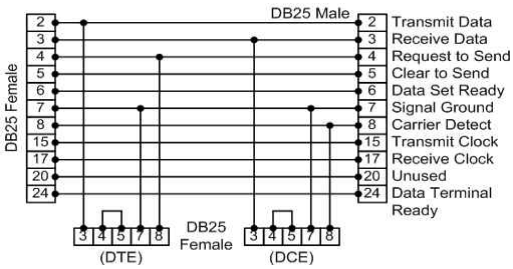

그림 2. DB25 직렬통신 선로 연계 결선도
Fig. 2. Tapping Connection for DB25 of Serial Communication

반면 FEP 하위 계층은 저속 통신 구간으로 RS232 또는 RS485 방식의 직렬통신을 사용한다. 직렬통신 구간에서는 장치가 할당하는 예비(echo) 포트가 없는 경우 통신선의 물리적인 탭핑(tapping)으로 SCADA 통신 구간에 접근할 수 있다. 단일 지점에서의 탭핑으로 간단한 통신 정보의 유출이 가능하며, 두 지점 이상의 탭핑으로는 계측·제어 값들의 위조나 변조 그리고 우회(bypass) 경로 형성과 특정 경로(방향) 차단 제어가 가능하다. 다음의 그림 2는 직렬통신 구간에서 SCADA 통신 프레임의 감시(sniffing)와 우회 경로 및 데이터 방향 제어가 가능한 탭핑 결선을 나타낸 것이다.

위의 그림 2에 나타난 결선은 물리적 접속 시점의 잡음 현상을 제외하면, 통신에 영향을 주지 않고 지속적인 정보 수집을 수행할 수 있다. 상향 서버측은 DTE(Data Terminal Equipment) 포트, RTU를 비롯한 하향 장비측은 DCE(Data Communication Equipment) 포트로 할당하여 해당 통신 정보를 모의하거나 감시한다.

우회 경로는 그림 2에서 서버와 RTU측의 통신 포트를 선택적으로 개방(open)함으로서 구성할 수 있다. 또한, DTE와 DCE 포트를 이용하여 RTU 계측정보 및 서버 제어 명령들을 다양한 형태로 변형한 공격을 수행할 수 있다.

3. 보안성 평가 테스트베드 구현

보안성 평가를 위하여 구현된 SCADA 테스트베드는 다음의 그림 3에 나타난 구조로 구성하였다. 각 RTU와 IED 장치들은 통신 포트의 물리적 접속방식에 따라서 직렬 통신(RS232/RS485)과 고속 Ethernet 통신을 선택적으로 사용할 수 있도록 하였으며, 테스트베드에서 사용하는 표준 통신 규약은 DNP와 Modbus로 설정하였다.

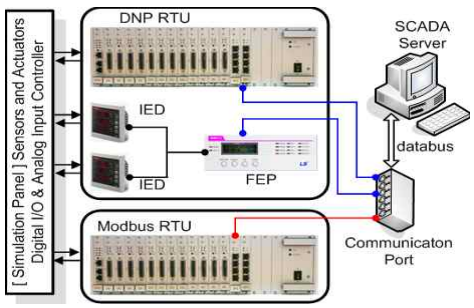

그림 3. SCADA 테스트베드의 구조
Fig. 3. Network Structure of SCADA Testbed

각 통신 구간은 앞서 제시한 보안성 평가 방법들을 시험하기 위하여, FEP 상위 계층은 통신장치의 예비 포트를 할당하고 저속 직렬통신 구간은 그림 2에 나타난 결선으로 각 분석 장치들을 접속할 수 있도록 하였

다. 보안성 평가를 위하여 마련된 접속 포트들은 기존 통신 흐름에 영향을 주지 않으며, 상향과 하향 포트로 각 구분된다. 각 구간에 설정된 상 · 하향 포트를 이용하여 해당 장치의 입 · 출력 정보뿐만 아니라 사용자가 원하는 구간을 선정하고 해당 구간이나 계층에서 여러 장치를 거쳐서 송 · 수신되는 통신 보안성 평가도 가능하다.

다음의 그림 4는 상기 나열한 기능과 보안성 평가를 위하여 구성된 테스트베드로 SCADA 서버, RTU 및 IED와 FEP 그리고 계측 · 제어 기능 수행을 위하여 제작된 시뮬레이션 판넬을 나타낸 것이다.

그림 4. 구현된 SCADA 테스트베드
Fig. 4. SCADA Testbed Equipments

SCADA 서버 HMI 조작으로 시뮬레이션 판넬의 디지털 출력을 제어하고 시뮬레이션 판넬의 디지털 입력과 아날로그 입력 그리고 FEP에서 전송되는 IED 계측값을 서버 프로그램에 표시한다. 다음의 그림 5는 서버 프로그램의 실행 화면을 나타낸 것이다.

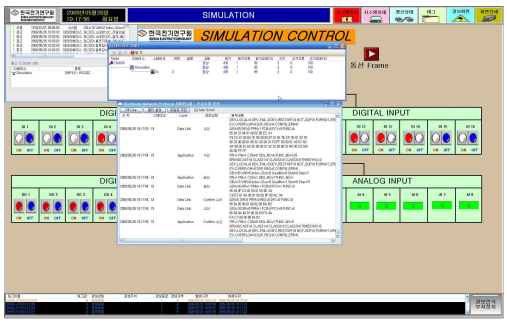

그림 5. 서버 프로그램 실행 화면
Fig. 5. SCADA Program Monitor

서버 프로그램에서는 선택된 규약에 대한 데이터 프레임과 송 · 수신 오류 그리고 통신 환경에 대한 정보를 실시간으로 표시한다. 이상의 기능을 활용하여 테스트베드를 구성하는 장치 및 구간에서 통신 규약과 전송매체 그리고 속도 특성에 따른 다양한 보안성 평가시험을 수행할 수 있다.

테스트베드의 직렬통신 구간에서 그림 2에서 제시한 연계 결선도를 활용하여 스니핑, 재생공격, 위장하기, 서비스거부의 순서로 해킹방법을 수행하였다.

RTU와 서버간에 통신 프레임은 DTE와 DCE 포트로 할당 후 각각 송신과 수신 프레임으로 구분하여 저장한다. 또한 각 포트로 수집되는 정보들은 프로토콜 분석 툴을 이용하여 해당 정보값이나 명령어로 해석하는 스니핑을 수행하였다. 스니핑 결과는 RTU의 계측정보와 서버측 제어명령을 시간 단위로 대조함으로서 성공률을 확인한다.

스니핑 수행으로 분류된 프레임을 호출하여 서버측에는 RTU 계측정보를 RTU에는 서버의 제어명령 프레임을 재사용함으로서 재생공격을 수행하였다. 재생공격의 경우 해당 시점의 실제 계측정보나 제어명령이 전달되지 않고 재전송된 이전 정보들의 송 · 수신 여부로 공격의 성공을 확인한다. 단, 우회경로 설정과 스니핑을 제외한 해킹 수행 시 모의 송신측 통신 포트는 개방한다.

위장하기 공격은 앞서 분석된 RTU 송신 프레임에서 RTU의 ID 번호를 변경하여 서버로 전송한다. 서버가 해당 정보의 수신 후 변경된 ID로 관련 정보를 갱신하는 것으로 공격의 성공을 확인한다.

서비스거부 공격은 DTE 또는 DCE 포트 중 하나의 포트에 연속적으로 대량의 데이터 프레임을 전송함으로서 서버와 RTU 사이의 통신 회선을 선점하여 정상적인 통신이 방해되는 것을 확인하여 공격의 성공을 확인한다. 구현된 SCADA 테스트베드상에서 상기 나열한 방식과 절차로 보안성 평가와 취약성 분석을 수행하였다.

4. 결 론

SCADA 네트워크는 적용 분야와 대상이 확대되고 있으며, 다양한 형식의 설비와 통신 장치들이 연계되

고 있다. 이는 운용적인 측면에서 유연하고 효율적인 장점이 있으나, 잠재적으로 외부의 침입으로 인한 사고와 오동작 발생 가능성을 갖는다.

또한 Smart Grid 기술의 도입으로 유·무선 융합 통신망 구성과 확대로 인하여 정보 보호와 사이버 공격을 대비하기 위한 보안성 향상 기술들이 요구된다. 따라서 SCADA 시스템 보안성 향상을 위한 평가 방안과 기술 개발이 필요하다.

본 논문에서는 현장에서 운용중인 상용 SCADA 시스템의 계층구조와 통신 사양(DNP, Modbus 규약)을 고려하여 보안성 평가 수행을 위한 테스트베드를 구성하였다. 특히 계측·제어 명령을 수행하는 RTU, IED와 같은 단말 장치의 직렬통신 구간 평가를 위하여 물리적 접속 방법과 해킹 방법 및 절차를 제시하였다. 제안된 테스트베드와 평가 절차 및 방법들은 향후 SCADA 주요설비 보호와 악의적인 침입이나 해킹에 대한 보안성 검토와 취약성 분석 그리고 단말 장치 제조사들의 보안 장비 개발에 활용할 수 있을 것으로 기대된다.

References

[1] Gordon Clarke, Deon Reynders, "PRACTICAL MODERN SCADA PROTOCOLS", Newnes, 1 edition, September 2004.

[2] Krutz, R., "Securing SCADA Systems", Wiley Publishing, Indianapolis, Indiana, 2006.

[3] National Infrastructure Security Coordination Centre, "The electronic Attack (eA) Threat to Supervisory Control and Data Acquisition(SCADA) Control & Automation Systems", "NISCC Briefing 02/04, 2004.

[4] Hugh Njemanze, "SCADA Security Protections Are On The Increase", Pipeline & Gas Journal, February 2007.

[5] 이철원, "주요 제어시설의 사이버 보안 동향", 국가보안기술연구소, 2007년 4월.

[6] 이철수, "원방감시제어자료수집(SCADA) 시스템 보안성 강화 방안", 국가사이버안전센터, 사이버 시큐리티, pp.8-17, 2005년 12월호.

[7] Erik Johansson, Teodor Sommestad, Mathias Ekstedt, "SECURITY ISSUES FOR SCADA SYSTEMS. WITHIN POWER DISTRIBUTION",.

[8] U.S. Separtment of Energy, Office of Energy Assurance, "21 Steps to Improve Cyber Security of SCADA Networks", 2003.

[9] Information of Tenable Network Security, Inc., "Protecting Critical Infrastructure SCADA Network Security Monitoring", August 1, 2008.

[10] Idaho National Engineering and Environmental Laboratory, Control Systems Security and Test Center, "A Comparison of Oil and Gas Segment Cyber Security Standards", U.S. Department of Homeland Security, November 3, 2004.

[11] Centre for the Protection of National Infrastructure, PA Consulting Group, "PROCESS CONTROL AND SCADA SECURITY - GUIDE 2. IMPLEMENT SECURE ARCHITECTURE".

[12] Julio Rodriguez, "SCADA-EMS Test Bed - INL Case Study on Current Vendor Partnerships", Idaho National Laboratory, May 23, 2007.

[13] Annarita Giani, Gabor Karsai, Tanya Roosta, Aakash Shah, Bruno Sinopoli, Jon Wiley, "A Testbed for Secure and Robust SCADA Systems", Special issue on the the 14th IEEE real-time and embedded technology and applications symposium (RTAS'08), Volume 5, Issue 2, Article No. 4, July 2008.

[14] C. M. Davis, J. E. Tate, H. Okhravi, C. Grier, T. J. Overbye, and D. Nicol, "SCADA Cyber Security Testbed Development", Power Symposium, 2006. NAPS 2006. 38th North American, pp 483-488, Sept. 2006.

[15] P.A.S. Ralston, J.H. Graham, J.L. Hieb, "Cyber security risk assessment for SCADA and DCS networks", ISA Trans. Volume 46, Issue 4, pp 583-594, October 2007.

[16] Ray Parks, Jason Hills, Sammy Smith, Tom Davis, Ana Baros, Patricia Cordeiro, "Network Security Infrastructure Testing", Sandia National Laboratories' Center for SCADA Security, October 12, 2005.

◇ 저자소개 ◇

이종주(李種柱)
1975년 11월 27일생. 1999년 수원대학교 전기공학 졸업. 2001년 성균관대학교 정보통신공학부 대학원 졸업(석사). 2008년 동대학원 정보통신공학부(박사). 2001~2004년 새턴정보통신(주) 개발팀장. 2005~2007년 성균관대학교 정보통신용신기능성소재및공정연구소 연구원. 2008년~현재 한국전기연구원 전력시스템 연구본부 Smart Grid 연구센터 위촉선임연구원.

김석주(金碩柱)
1961년 12월 8일생. 1984년 연세대학교 전기공학과 졸업. 1986년 동대학원 전기공학과(석사). 2007년 동대학원 전기전자공학과(박사). 1987년~현재 한국전기연구원 전력시스템 연구본부 Smart Grid 연구센터 책임연구원.

강동주(姜東周)
1975년 9월 9일생. 1999년 홍익대학교 전자전기제어공학과 졸업. 2001년 동대학원 전기정보제어공학과 졸업(석사). 2001년~현재 한국전기연구원 전력시스템 연구본부 Smart Grid 연구센터 선임연구원.