Journal of the Korean Institute of Illuminating and Electrical Installation Engineers (2012) 26(7) : 99~109
http://dx.doi.org/10.5207/JIEIE.2012.26.7.099
논문 26-7-14

이중화 자동복구 보안기능이 구비된 배전반의 보안성 평가를 위한 테스트베드 구성에 대한 고찰

(An Inquire into Test Bed Compositions in Assessing the Security of a Soft Redundancy Sub-Station System with Auto-Restoration)

최형석* · 진창기 · 배기덕**
(Hyeong-Seok Choi · Chang-Gi Jin · Gi-Deok Bae)

Abstract

Sub-station, key equipment in electric power infrastructure, are being exposed to increasing risk of hacking. For this, soft redundancy sub-station system needs to be formulated with automatic restoration mechanism. For this it is important to assess the reliability of the applicable range of data that are used in actual system operation, as well as the methods and findings of the tests. At the same time performance of soft redundancy system and total security mechanism, which are aligned for the protection of the sub-station, need to be tested. For testing the above-mentioned, this paper presented a viable formation of a soft redundancy practical VPN system within a panel to protect the latter from hacking or cracking incidences, and conducts a test to check if the considered system actually serves the protection function in the actual operation setting, gathering evidence from the data from the testing of the actual performance of the system as well as of emergency scenario simulation operations. Because tested soft-redundancy & restorative sub-station system is expected to be widely applicable for various cases such as Smart-grid or electricity IT system, where VPN with enhanced level of security is required.

Key Words : SCADA, Sub-Station, VPN, Soft Redundancy, Auto Restore

1. 서 론

1.1 연구의 배경

대다수 배전반 시스템 계통기기들이 SCADA (Supervisory Control and Data Acquisition) 시스템으로 관리와 운영이 이루어지고 있다. 이러한 시스템의 특성으로 인해 국가 주요핵심기반시설은 사이버

* 주저자 : CIO, Sam Deuk Elec Co., LTD.
** 교신저자 : CTO, XNSystems Co., LTD.
Tel : 031-984-0330, Fax : 031-984-1199
E-mail : d600183@hanmail.net
접수일자 : 2012년 6월 25일
1차심사 : 2012년 6월 27일, 2차심사 : 2012년 7월 20일
심사완료 : 2012년 7월 23일

테러 및 해킹, 바이러스 등의 표적으로서 공격당하게 되면 조작 및 통제 권한을 상실하거나, 기기의 오작동이 일어날 수 있으므로 심각한 위험에 빠질 가능성에 의하여 보안의 중요성이 부각되고 있다[1].

SCADA 시스템을 이용하는 국가 주요핵심기반시설 보안의 중요성을 보여주는 예로는 슬래머 웜(Slammer Worm)과 스텍스 넷(Stuxnet)이 있다. 이는 전 세계적으로 심각한 피해를 야기했고, 오하이오 원전, 이란 원전은 보고된 사례에 불과하다.

다양한 유·무선 통신방식의 도입으로 기존의 SCADA는 개방형 Open Protocol 시스템으로 확장되고 있는데 이는 시스템 운용의 효율 증대 측면에서는 바람직하나 시스템 보안은 취약하게 노출되는 단점도 동시에 수반한다. 이는 시스템의 유연성과 접근성 향상으로 운용상의 효율을 가져오는 반면 상대적으로 많은 연결과 접속지점의 허용으로 외부노출과 침입에 대한 약점이 발생된다.

SCADA 통신망 침입 그리고 정보유출과 특정정보에 대한 위·변조 등의 악의적 공격이 발생할 경우 이로 인한 피해와 파급효과는 매우 크다[2]. 시스템의 관리대상과 처리하는 정보의 중요성이 증가됨에 따라서 보안성 향상을 위한 취약성 분석 기법과 사이버공격이나 침입 그리고 정보유출과 같은 위협에 대비하기 위한 기술들이 요구된다.

통상 SCADA 상위의 고속통신망은 안정적인 정보관리와 처리를 위하여 침입탐지(Intrusion Detection System, IDS) 또는 방호시스템(Intrusion-Prevention System, IPS)과 같은 보안대책을 마련하고 있으나 현장에서 계측정보를 수집하거나 원격지의 명령을 수행하는 설비들은 상대적으로 보안성이 취약하다.

즉 출입과 같은 물리적 보안절차를 만족할 경우 하위의 단말장치들은 통신구간에서 외부의 침입이나 악의적인 정보의 위·변조 공격에 대응할 수 있는 기능이 부족한 실정이다.

SCADA 시스템을 대상으로 하는 잠재적 위협과 공격 가능성이 증가됨에 따라서 통신규약을 비롯한 기존 장치와 설비에 대한 보안성 향상 방안들 연구되고 있다[3]. SCADA 시스템의 보안성 향상은 기존설비를 개량·개선하는 방법과 차세대설비로 교체하여 사이버보안에 대비하는 것으로 구분되며, 암호화 장치나 인증시스템을 기존설비에 도입하는 방법과 현재 사용하고 있는 통신규약이나 운용프로그램의 취약성을 분석하여 개선하는 방법들이 검토되고 있다.

1.2 연구의 목적 및 방법

본 연구에서는 상대적으로 보안성이 취약한 RTU(Remote Terminal Unit) 및 IED(Intelligent Electronic Device) 또는 계전기류 같은 하위 현장설비들에 대한 보안 대책으로 해당설비의 통신포트에 직접 연계하거나[4-5], 보호 함체에 밀접 근거리 부착해서 직접 적용할 수 있는 프로토콜 변환기능을 구비한 전력기기 보호용 보안 입출력 장치에 I/O암호화 장치를 부가하도록 제안하였다.

상위의 제어명령을 직접 수행하고 계측정보를 원격지 서버로 전송하는 현장설비들은 직렬통신방식을 이용하여 정보를 교환한다. 하지만 공개된 통신규약과 침입탐지 또는 방지시스템이 없는 직렬통신구간에서는 탭핑(Tapping)과 같은 방법으로 현장설비들에 대한 접근이 가능하다. 따라서 악의적인 제어명령이나 계측정보의 위·변조를 방지하기 위한 직렬통신 구간 암호화 장치와 같은 대책이 필요하다.

더불어 악의적인 제어명령이나 계측정보의 위·변조를 방지하기 위한 직렬통신 구간 암호화 장치와 같은 대책과 함께 실부하 현장 적용에 이중화된 Power Hot-Swap과 Network Hot-Swap의 절체 기능이 반드시 필요하다.

제안된 장치는 제어대상의 중요도와 구성에 따라서 접근 권한의 레벨을 분류하고 통신선로의 침입이나 물리적 키유출의 대비책을 포함한 총 6단계의 관리권한 부여에 대한 보안절차를 구성함으로서 안전성을 확보한 효과적인 SCADA 통신을 구현할 수 있다[6]. 이때 구성되는 Transaction은 현장시설의 관리권한과 접속통제의 보다 강화된 수단이 요구되는 바, 짧은 주기의 Key 갱신 메커니즘에 의하여 장기간의 운전시에도 상시 접근이 허용된 내부 관리자 등에 의한 Key 유출 사고를 대비하도록 하였다.

제안된 장치는 임베디드 리눅스 기반으로서 내

장된 직렬통신 디바이스 드라이버 키교환 및 암·복호 처리 태스크 등은 MMI(Man Machine Interface, MMI ; 중앙관제소 운영 프로그램)연동으로 운전된다.

본 연구에서는 SCADA 통신규약으로 널리 사용되고 있는 IEC-60870 Modbus방식을 채용한 RS-485 구간과 VPN이 구축된 Ethernet 구간을 계층별로 구분하여 보안 클라이언트 구간, 보안 서버 구간, 보안 MMI 구간에서 기능 및 성능평가를 수행하였다.

또한 본 연구 제안의 신뢰성과 고가용성을 증대하기 위한 방안의 일환으로 배전반에서 발생할 수 있는 데이터 스푸핑, 스니핑을 방지하기 위한 물리적 기술적 복합 방호 방안을 제안하였고, 소프트웨어 또는 하드웨어, 통신 계통 장애, 중계 장치류의 결점 오류에 의한 시스템 무력화에 대비하기 위한 L2, L3~L7 계층을 지원하는 이중화 시스템을 개발하였다.

본 연구에서 설계한 이중화 자동복구 절체 시스템은 작은 시간 내에 시스템을 회복하고 사고나 고장 여부를 신속히 보고하게 함으로서 외부공격과 위협을 탐지 대응할 수 있으며, 내부 명령계통 지휘절차계통이 구비되지 아니하여 불확실한 사업장에도 전혀 종속되지 않는 운용기법을 제공하여 효율성과 신뢰성을 향상시키고자 하였다.

2. 본 론

2.1 배전반 해킹/크래킹 시나리오 개요

본 연구의 실제 적용된 장치는 표 1과 같이 전력계통기기 보안용 입출력 변환장치 [X-Cure_CKERI (TRD12S00426)]로서 사진 1과 같이 함체 내에 이중화 구성하였으며, 주요 내용은 표 1과 같이 IEC-60870을 지원하는 IEC-62053 계전기류의 전력계통기기 입출력 변환장치[X-Cure_PGB KERI(TRD 12S00427)]를 복층 1함체로 구성함을 특징으로 하는 바, Mux (다회로 교합 중계기능)를 통한 Serial 및 보안전용 I/O통신을 지원함을 주요 특장점으로 구성하여 접근, 개문, 조작 통제를 동시에 실시하였다.

표 1. 배전반 함체 장착 적용 장치 개요
Table 1. Specification of the equipment to be installed in the sub-station panel

<table>
<tr><td rowspan="3">제조사양</td><td>메이커</td><td>SDE</td></tr>
<tr><td>제조연월일</td><td>2012년 3월</td></tr>
<tr><td>NISS인증</td><td>2012년 1월</td></tr>
<tr><td>제품 및 규격</td><td>Test bed 구성 내용</td><td>주요기능</td></tr>
<tr><td>CC EAL 3
(VPN/IPS)</td><td>2중화 테스트 장비 베드 1식
연동장치 기구제작 및 회로수정 S/W 등</td><td>VPN, IPS F/W</td></tr>
<tr><td>X-Cure_C
KERI(TRD12S00426)</td><td rowspan="3">S/W, H/W, Net
검증 사양 및 방법 제시</td><td>Protocol 변환
I/O VPN</td></tr>
<tr><td>X-Cure_PGB
KERI(TRD12S00427)</td><td rowspan="2">Protocol 변환</td></tr>
<tr><td>KCC-REM-XCU-Xcure-PGB</td></tr>
</table>

사진 1. 함체내부에 장착된 VPN 이중화 시스템
Photo 1. Soft-redundant VPN system installed within the panel

사진 2의 SCADA 직렬 통신구간 암호화 장치 X-Cure_C는 기존 계전기 설비의 통신포트에 접속되어 정보를 송·수신하고 암호화 장치간의 암·복호 처리기능으로 암호 통신을 수행한다. 보다 상세한 기능은 2.5절에서 다시 설명한다.

사진 2. 전력계통기기 보안용 입출력 변환장치 X-Cure-C
Photo 2. X-Cure-C, In-out switch machine for security of the Power System

그림 1은 실현장에 장착된 VPN 이중화 자동복구시스템의 구성 개요도로서 함체 내부는 VPN Client, 함체외부는 VPN Master로 2중화 자동복구 기능이 구비된 상태로 자동복구 VPN Session을 맺는다.

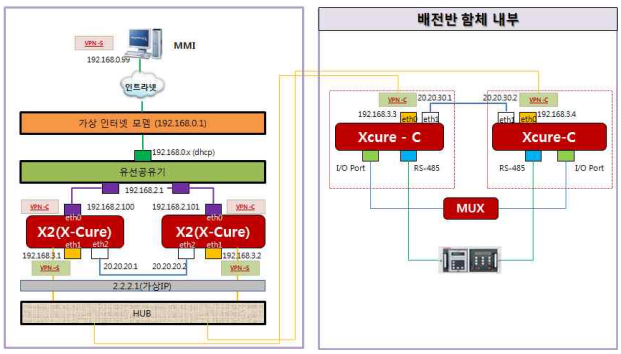

그림 1. 함체 내·외부 VPN이중화 시스템 구성 개요
Fig. 1. Structure of interior and exterior of Soft-redundant VPN system

또한 그림 2와 같이 장치간의 인증ID certification과 키 교환(key exchange), 총 6단계의 키 갱신 절차가 수행된다.

보다 구체적인 실험을 위해 내부의 물리적 침입 가로채기 제어 위변조 교란 TEST를 통한 Tamper 기능을 제공하고 배전반 함체 외부에 X-cure S2 VPN Master시스템 2Set를 주어 이중화 자동복구 절체와 VPN 무결성 Session 유지를 지원한다.

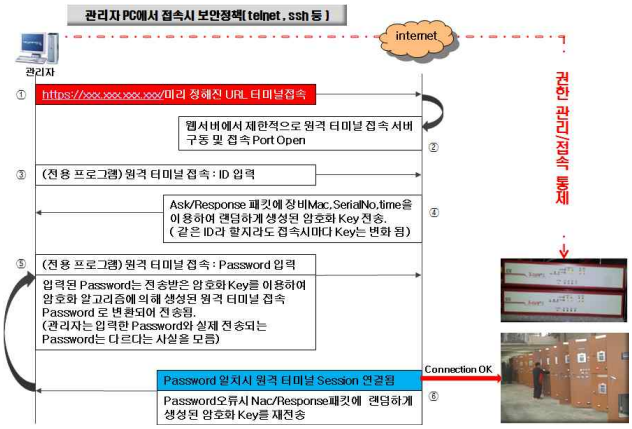

그림 2. 관리권한 확인을 위한 키 인증 교환절차
Fig. 2. Authentication process through key word for checking management authority

또한 통신규약과 접속방법 및 구조(Topology)를 고려하여 1 : 1(point-to-point), 1 : N 또는 다중접속(multi-drop)을 수용할 수 있도록 구성하였고 광역의 클라우드 ISP 서비스를 지원하기 위하여 그림 3과 같이 설계한 2중화 보안 Network Pipeline을 개발하였으며 이는 네트웍의 사용 대역폭과 IP Port를 지정하고, 사고 상황의 인지와 절체 자동복구, 우회 시도횟수 설정, VPN Session의 재구성을 포괄하는 복합적인 일련의 Procedure Process를 포함하며 운영의 신뢰성을 유지하는 핵심 기능이다.

이때 이중화 절체에 구현된 메커니즘은 표 2와 표 3과 같으며 표 2는 임의 데모 판넬에 설치된 장비의 Active - Stanby 절체 및 리세션 이중화 및 VPN 상태 분석 및 대응을 말하며 표 3은 표 2의 분석에 따른 Master<->Slave 절체 과정의 구조도이다.

실험에 사용된 장비에서 Master측 이중화를 위한 장비 와 Slave측 이중화를 구성하기 위한 장비 간에는 192 대역의 Data 통신 IP와 구별되는 20 대역의 IP로 Heart-bit Protocol 통신을 실시하고 Master <-->Slave 간의 내부는 ARP (Address Request Protocol)와 RIP (Routing Interior Protocol) Demon을 상주하게 하여 상호 Cross-Check 절체를 지원하게 하였다.

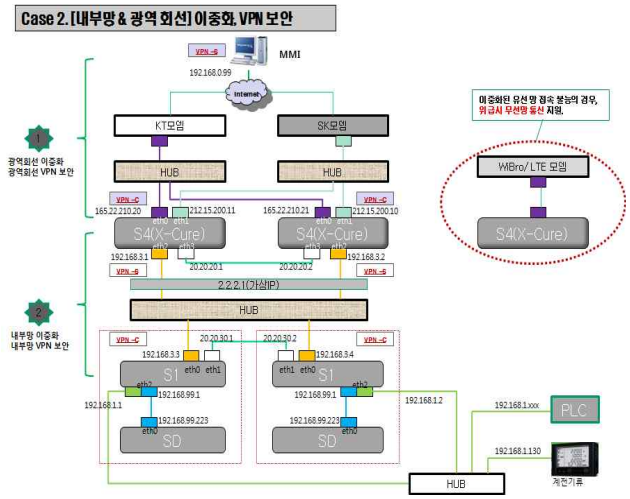

그림 3. 내부망과 외부 광역회선 이중화 및 VPN이 지원되는 Pipeline구성 계통
Fig. 3. Pipeline structure of the system supported by soft-redundancy mechanism of internal network and external broadband line and VPN

표 2. 장비의 이중화 및 VPN 상태 분석 및 대응
Table 2. Situation analyses and according responses of soft redundancy of equipment and VPN

VPN 이중화 절체 Procedure	Detection point
현재 장비의 이중화.VPN 상태 값을 분석	
현재 장비의 이중화 상태의 Master/Slave 상태 분석	
현재 장비의 VPN 상태의 이상 상태 분석	
현재 이중화 상태 Master 여부확인, 이상 현상 조치	VPN 네트웍 이상 상태 감지
	새로운 VPN의 연결실패 감지
	연결된 VPN에 이상상태 감지
Primary VPN 상태 이상으로 강제로 장비를 Slave 상태로 전환	
현재 장비의 VPN연결이 다른VPN 서버로 전환되었음을 감지	
끊어진 장비의 ProgotolGateway, I/O 세션 재 연결	

표 3. 표 2 분석에 따른 장비 이상 상태 발견 시, 장비 절체 모드 Master⟨->Slave 전환
Table 3. Switching mode between equipment transfer Master ⟨-⟩ Slave upon the discovery of emergency situation based on the analysis of Table 2 above

Master/Slave 절체 Procedure	Detection point
현재 장비의 이중화 상태가 Master 상태이면, 계속 Master 역할 수행	ALARM_MASTER
현재 장비의 이중화 상태가 Slave상태이면 Slave -> Master 역할 변환	
현재 장비의 ProgotolGateway,\ I/O 세션을 생성 및 연결	ALARM_SLAVE
현재 장비의 이중화 상태가 Slave 상태이면, 계속 Slave 역할 수행	
현재 장비의 이중화 상태가 Master 상태이면, Master -> Slave 역할 변환	
현재 장비의 ProgotolGateway, I/O 세션을 종료	PG_DestroySession IO_DestroySession

2.2 실제 해킹/크래킹 시스템 구성

정상 동작 중앙 감시반을 구성의 최상위 네트웍으로 설정하고 표 4와 같은 내용의 실험을 실시하여 각 동작에 대한 결과 Log Data 취득을 모색하였다.

표 4. 배전반 시험내용
Table 4. Testing areas of sub-station

구분			적용내용	Test Bed 구성내용
형식	내용	유형		
크래킹	가로채기	제어	고압반 VCB	▪ 시나리오 ▪ 프로그램 ▪ 컨버터설치 센서 무력화
		위변조(가공)	KVA값, CB상태	
	교란 (파괴)	시스템장애	계전기 무력화 MMI 무력화	
		시스템파괴	시험(xTR)	미실시
	악의적 (오)동작		VCB 트립	버튼류 확인
	기타		물리적 입출력	출입통제기기 연동
해킹	침입		VPN Server/Client Event Logger	VPN System 로그 분석 등

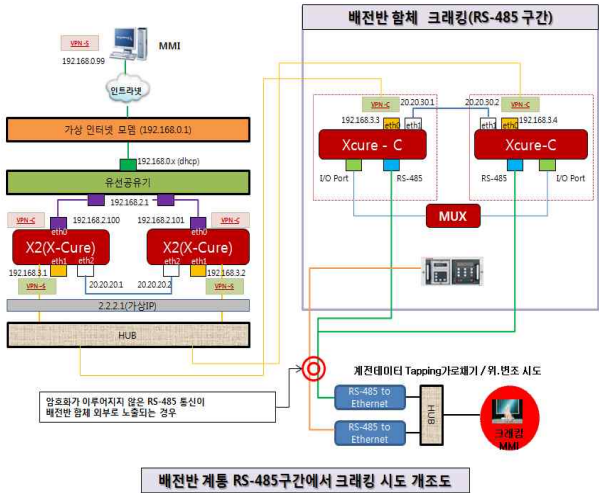

그림 4. RS-485 구간 해킹/크래킹 시스템 구성 개요
Fig. 4. Diagram of hacking/cracking system in RS-485 section

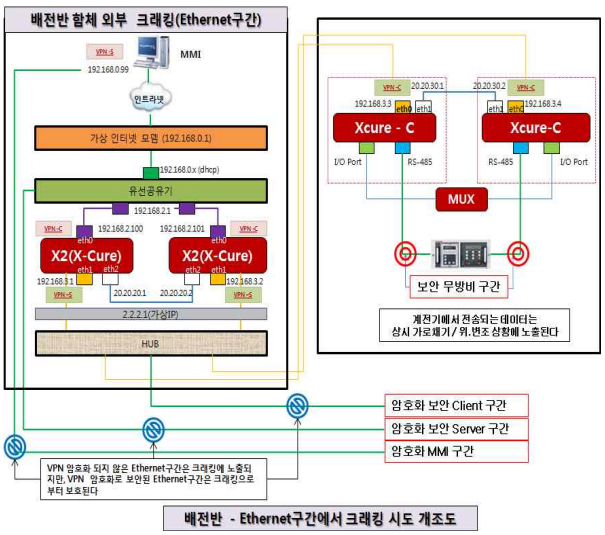

그림 5. Ethernet 구간 해킹/크래킹 시스템 구성 개요
Fig. 5. Diagram of hacking/cracking system in Ethernet section

이때 적용한 네트웍은 그림 4 및 그림 5와 같이 구성하였으며 함체를 기준으로 그림 4는 평문 RS-485 구간에서 표 4의 크래킹을 구현하였고, 그림 5는 함체 외부로 구성되는 모든 통신은 암호화된 Ethernet으로서, 암호문 VPN Ethernet 구간을 대상으로 해킹 침입시도를 통해 시스템 무력화를 시도한 실시 개요이다.

2.3 실제 배전반 크래킹 작업 개요

크래킹 코어 S/W와 MMI의 연동은 크래킹 코어 S/W의 역할로서 크래킹 MMI에서 하달되는 명령을 수행하는 역할로 "가로채기, 위·변조, 강제 CB제어" 등을 담당하는 S/W에 대한 구성으로 MMI에서는 register를 통한 인터페이스만 구성하였다.

악의적 크래킹 MMI 서버 S/W 및 UI(User Interface)화면 구성서버 S/W는 변경불가하며 UI화면 구성은 가상태그를 추가하여 태그상태에 따라 이벤트 화면표출로 데이터 신뢰성을 유지한다.

그림 6.은 악의적 크래킹 MMI 서버 관련한 구성화면 내용을 제시하였다.

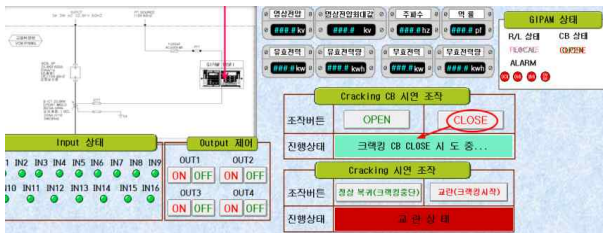

그림 6. 악의적 크래킹 MMI 서버 구성화면 내용
Fig. 6. Content of the composition screen of MMI Server under malevolent cracking

악의적 크래킹 코어 S/W 와 크래킹 MMI 서버 연동 테스트를 위한 구체적인 시나리오 스텝은 악의적 행동으로 현장 계전기 CB 출력을 제어하고 현장 알람 이벤트를 무력화시키고 사용자 MMI는 정상상태로 표출하는 단계로서, 계전기 CB를 제어하는 부분의 구현과 현장 알람 이벤트 무력화 및 MMI 화면상의 상태 표출은 크래킹(가로채기 - 위·변조) 내용을 도시한다.

현장 계전기 알람이벤트 발생에도 불구하고 가로채기 동작으로 MMI는 정상상태 표출하게 하여 크래킹(가로채기 - 위·변조)에 해당 하는 내용을 구현하였다.

이를 위하여 고압반을 대상으로 한 계전기 GIPAM 115FI 485 라인 크래킹을 위한 배전반 데모 통신선 작업은 그림 4와 같이 통상의 현장여건과 동일하게 함체

외부에 방기된 것으로 가정된 RS-485 통신을 대상으로 다음과 같이 구성하였다.

- Ethernet To 485 디바이스 2EA
- 크래킹 MMI용 물리적 PC/서버 준비 및 셋팅

이때 MMI서버 또는 MMI Viewer를 크래킹하거나 서버의 크래킹은 본 연구 제안 범위 초과이나 데모용 배전반의 판넬 PC가 정상적인 MMI 서버 및 MMI Viewer 를 겸하고 있으므로 악의적 크래킹 MMI 서버 및 MMI Viewer 역할을 수행할 수 있는 컴퓨터를 일반 업무용 수준 사양 PC 2대로 별도 구성하여 시리얼 구간 크랙용 PC, Ethernet구간 해킹용 PC로 준비했다.

2.4 함체 외부 경로에 대한 VPN 구간의 배전반 해킹의 공격경로

아래 그림 7의 번호가 부여된 주요 공격 대상 지점에 대하여 ①번은 중앙 감시반에 해당되는 곳이고, ②번은 함체 외부의 VPN Server및 Master 기능을 수행하는 구간이고 ③번은 함체 내부의 VPN Client 및 Slave로서 ④번에서 전송된 데이터 뿐만 아니라 본 연구에서 제안한 보안전용 입출력 신호도 함께 암호화와 함수화를 실시하는데 배전반 해킹의 공격경로에 대한 구성은

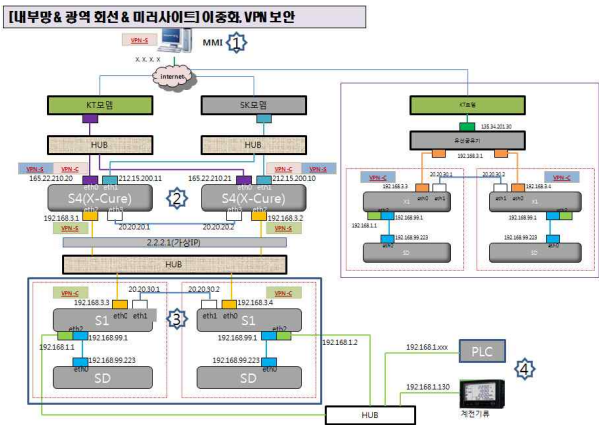

그림 7. 함체 외부 경로에 대한 배전반 SCADA 해킹 공격 예상지점(번호가 부여된 구간)
Fig. 7. Expected spots for hacking attacks at SCADA sub-station against the external route of the power system

- ① 보안 MMI구간
- ② 보안 Server구간
- ③ 보안 Slave구간
- ④ (비)보안 Source구간

으로 공격 경로를 축약하여 구성하였다.

2.5 내부 VPN 실제 장착 해킹/크래킹 공격경로

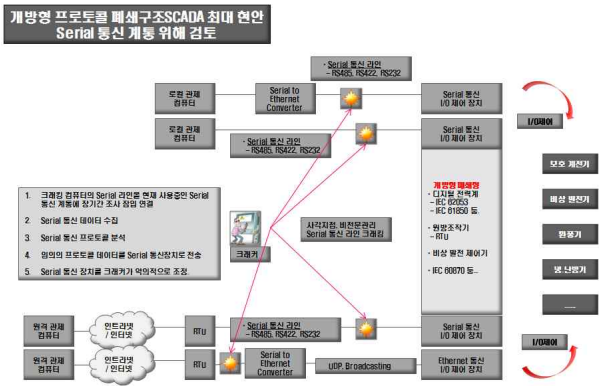

그림 8. 내부망 접속 침투 교란 시도 모식도
Fig. 8. A pattern diagram of attempted infiltration and disturbance through connection into the internal network

윗 그림 8은 임의의 지점에 Tapping Dump 또는 UDP Port를 통해 내부망에 접속하고 침투 교란, 크래킹이 이루어 질 수 있는 계통의 모식도로서 본 연구에서는 표 5의 내용과 같이 현장 여건에 최대한 부합되도록 구성하였다.

그림 9의 S1(VPN Part)과 SD(보안 I/O Part)는 X-cure-C로 구성되는 단일 장치로서 내부는 Ethernet으로 연결된 하나의 장치이고 전력기기 보호용 보안장치로서 Modbus Protocol 변환기와 Discrete I/O 단말기, Mips 계열의 32[Bit]Octeon Processor를 탑재하고 3DES 및 MD5 함수 알고리즘에 대한 VPN 암호화 엔진 기능을 단일 장치에서 저가의 가격으로 수행하기 위하여 특별히 고안하였다. 여기서 검은 점선 박스는 각각의 X-cure-C이고 사진 2의 장치이다.

통상 계전기류는 배전반 함체내에 구성되며 사진 1을 참조하면 함체 외부로 노출되는 상위의 네트웍은

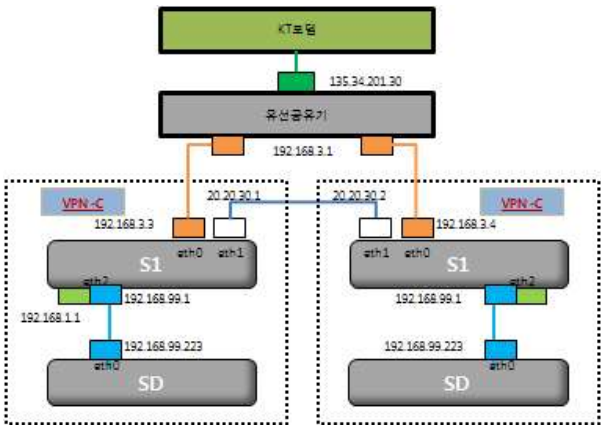

그림 9. 전력계통기기 보안용 입출력 변환장치 구성개요
Fig. 9. Structure of input/output switch machine for protection of power system equipment

표 5. 배전반 해킹/크래킹 시나리오
Table 5. Scenarios of hacking/cracking of sub-station

테모 시스템 구축			테모 시스템의 Transaction Procedure
PC 시연 MMI 구분			임의의 MMI 패널PC는 정상동작 시스템으로 구축 임의의 악의적 기능 MMI PC 2Set는 크래킹 시스템으로 구축
크래킹 시스템 구축	시스템 구성	RS-485	통신선로상 덤핑 절취(임의지점) 작업 - Ethernet To 485 디바이스 2EA - 크래킹 MMI용 물리적 PC / 서버 준비 및 셋팅
		Ethernet	통신선로상 임의포트 접속
	크래킹 실증 시연		악의적 크래킹 MMI 서버 S/W 및 UI 화면 구성 - 악의적 크래킹 MMI서버 S/W는 변경불가하며 UI화면구성은 가상태그를 추가하여 태그상태에 따라 이벤트 화면표출로 데이터 신뢰성 유지. - 악의적 크래킹 MMI 서버 관련 이벤트 화면 구성 정상동작 MMI 서버에서는 register를 통한 인터페이스만 구성하고 데이터 절취 등의 상황 표현
	시스템 크래킹 주요내용		잠입된 상태에서 정상동작 유지 기능 가로채기 - xCB 제어 상태값 표기 변조 계측값 가공 변조 교란 : MMI와 계전기 통신(IEC-60870) 무력화
	정상방어 확인		정상 회로상에서의 운전중 침입 탐지 가로채기시 VPN 암호화 동작구간 제어불능 시연
해킹 시스템 구축	해킹 실증 시연		임의의 네트웍 클라우드 지점에서 침입시도 임의의 네트웍 시스템에서의 Warm, DDoS 공격
	시스템 구성		Fig-1. 상에서의 다양한 가상공격 지점 설정
	시스템 해킹 주요내용		시스템 침입 (장기간의 잠입) 시스템 데이터 절취 제어
	정상방어 확인		VPN 구간 내에서의 이중화 기반 보안 정상기능 확인

오직 Ethernet으로서 VPN 암호화 무결성이 지원되는 구간이다.

표 6. 물리적 보안계통 구성 Step Process Programming
Table 6. Step Process Programming for composition of physical security system

정상 경로	접근	체류 시간	설정 범위내	관리자 확인		OK	녹색 LED(경광등)	허용
						NO	적색 LED(경광등)	
			설정 범위 초과	경보방송	관리자 재확인 1,2차	OK	녹색 LED(경광등)	허용
						NO	적색LED(경광등) 경보메시지 방송 경보문자	
					확인거부			
	횡보	횟수	설정 범위내	경보대기				
			설정 범위 초과	경보방송	관리자 확인	OK	녹색 LED(경광등)	허용
						NO	적색 LED(경광등) 경보메시지 방송 경보문자	
비 정상 경로	접근	속도	설정 범위내	관리자확인		OK	녹색 LED(경광등) 경보대기	허용
						NO	적색 LED(경광등) 경보메시지 방송 경보문자	
			설정 범위 초과	적색 LED(경광등) 경보메시지 방송 경보문자, 긴급 출동 명령, CCTV연계 경보 등				
	횡보	속도	설정 범위내	관리자확인		OK	녹색 LED(경광등) 경보대기	
						NO	적색 LED(경광등) 경보메시지, 경보음발신 경보문자	
			설정 범위 초과	적색 LED(경광등) 경보메시지 방송 경보문자, 긴급 출동 명령, CCTV연계 경보 등				

따라서 사진 1과 그림 1에 도시된 범주 내에서 배전반은 기본적으로 관리 권한 관리와 물리적 접근 개문 조작 통제에 실패하지 않는다고 전제할 경우 내부관

리자에 의한 고의적인 키 유출 사고를 방지할 수 있는 짧은 주기 Key갱신 알고리즘과 연계할 수 있을 때 고신뢰 이중화 시스템 보안시스템이 구성되므로 완성도 높은 안전을 확보할 수 있을 것으로 판단된다.

표 6는 배전반의 함체 내부에 VPN이 지원되지 않는 계전기기 IED's, RTU, PLC 등이 상위 SCADA 네트웍으로 구성되고 있는 일반적인 무방비 상황을 물리적으로 보완하기 위한 방호(Barrier) 개념으로서 시설 함체에 접근하는 부분에 대한 것으로서 SCADA 시스템의 기술적 보안과 물리적 방호 개념이 복합되는 내용을 Step Process Programming으로 추론하여 보다 효과 적인 시스템 구성을 이루기 위한 제안이다.

2.6 내부 VPN 실제 장착 사고실험 결과

캡션 1은 임의로 실시한 통신 및 전원 사고 실험에 대한 VPN Master측 DB에 저장된 Log기록의 일부이다.

본 연구에서는 발생한 사고에 대하여 무리한 재연결 시도 보다는 충분한 사고 상황 인지 시간을 두어 30초 내외의 시간 동안 Re-Session 체결이 그림 10과 같이 구성된 설정 Program을 통해 그림 11의 절체 복구를 위한 기초 데이터 설정 메커니즘을 통하여 구현되도록 프로그램하였다.

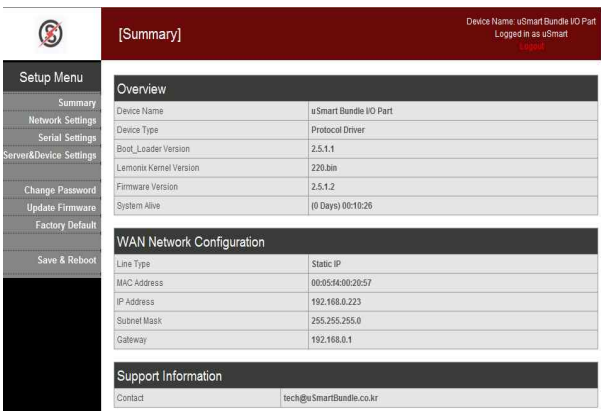

그림 10. 전력계통기기 보안용 입출력 변환장치 Setup Menu 구성
Fig. 10. Composition of a Setup Menu of in-out switch machine for protection of power system equipment

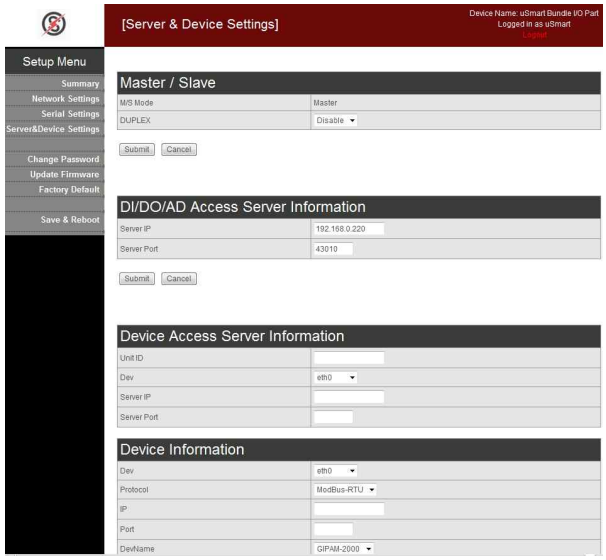

그림 11. 전력계통기기 보안용 입출력 변환장치 Sever 및 Device Setup 구성
Fig. 11. Composition of Server and Device Setup of in-out switch machine for protection of power system equipment

이와 같은 일련의 Processing을 통하여 시스템 자동복구(Auto-Restore) 기능이 수행됨과 동시에 VPN 보안 Session 구성이 계속 유지되는 아래와 같은 결과를 얻을 수 있었다.

- 전력계통기기 보호 보안장치 이중화
- 전력계통기기 보호 장치구성 내부망 이중화
- 전력계통기기 보호 장치구성 광역회선 이중화
- 하나의 I/O에 대한 교합중계(Mux) 이중화 지원

2012-05-19 12:32:51 XCUREGATEWAY NSM: xnid=0503510007 class=이벤트 subclass=HA level=notice subject=NSM result=성공 msg="NSM 서비스가 WAN 또는 LAN 회선들의 DEAD로 인한 VRRP 서비스 종료에 성공하였습니다. (인터페이스=eth0(WAN0) 회선상태=DEAD)"
2012-05-19 12:32:51 XCUREGATEWAY S_HA: xnid=0503220016 class=이벤트 subclass=HA level=crit subject=S_HA result=실패 msg="장비에 장애가 발생했습니다. 지금부터 Slave 모드로 동작 합니다."
2012-05-19 12:32:51 XCUREGATEWAY HAM:

xnid=0504510004 class=이벤트 subclass=ike-helper level=notice subject=HAM result=성공 msg="NSM 서비스로부터 인터페이스 상태 메시지를 수신하였습니다. (인터페이스이름=eth0 인터페이스상태=dead)"
2012-05-19 12:32:51 XCUREGATEWAY pluto[1245]: interface eth0 become dead (weight 0)
2012-05-19 12:32:52 XCUREGATEWAY pluto[1245]: update_iface_weight(eth0, 0)
2012-05-19 12:32:52 XCUREGATEWAY pluto[1245]: update_iface_weight(eth0, 0)
2012-05-19 12:32:52 XCUREGATEWAY HAM: xnid=0504510018 class=이벤트 subclass=ike-helper level=notice subject=HAM result=성공 msg="HAM 서비스가 인터페이스 상태 변경 요청에 성공하였습니다. (인터페이스이름=eth0 상태=dead)"
2012-05-19 12:32:52 XCUREGATEWAY NSM: xnid=0503510001 class=이벤트 subclass=HA level=notice subject=NSM result=성공 msg="NSM 서비스가 인터페이스의 회선상태 변경에 성공하였습니다. (회선상태확인방식=LINK_LED 인터페이스=eth0 회선상태=DEAD)"
2012-05-19 12:32:53 XCUREGATEWAY S_HA: xnid=0503220017 class=이벤트 subclass=HA level=crit subject=S_HA result=실패 msg="LLCF 기능이 사용중이지 않거나 WAN LAN 회선이 모두 ALIVE 상태가 아닙니다. Slave 모드로 동작합니다. (WAN:DEAD LAN:ALIVE)"
2012-05-19 12:32:53 XCUREGATEWAY pluto[1245]: received TERM signal
2012-05-19 12:32:53 XCUREGATEWAY pluto[1245]: forgetting secrets
2012-05-19 12:32:53 XCUREGATEWAY pluto[1245]: "to_192_168_3_4"[1,0]: deleting connection

캡션 1. VPN Master 측 DB에 저장된 Log기록
Caption 1. Recorded log saved in DB of the master part of the VPN

4. 결 론

본 연구의 목적을 달성하고 실제 도입하기 위해서는 각 배전반에 보안장치와 부대기기 및 MMI를 구성내용에 맞추어 설치해야 하기 때문에 기술적/경제적인 부분에 있어 저렴한 모듈 개발이 선행되어야 관련 산업에 쉽게 적용할 수 있다고 할 수 있으므로 본 연구는 이에 부합하기 위한 하나의 접근방법 제안이다.

반면 다수의 열반된 배전반에 시스템을 보다 용이하게 구성하기 위한 보다 확장성 있는 장치류와 관리시스템을 구현하기 위한 논리적 보안 요소 발굴 적용도 지속적인 연구가 필요할 것이다.

본 연구는 배전반 실제 장착 해킹, 크래킹 시스템의 구성과 실제 현장의 시설과 동일한 배전반을 제작하여 시스템을 구축 테스트하였다.

통상의 시스템이 확장은 물론 운용상 효율을 위하여 개방구조 통신규약을 채택함이 주류인 상황에서 시설구축 편의성은 증가하지만 상대적으로 많은 연결과 접속지점의 허용으로 외부노출과 침입에 대한 보안 취약성이 발생된다.

특히 계측・제어 명령을 직접 수행하는 하위장치들의 직렬통신구간은 중요성과 규모에 비하여 상대적으로 보안대책이 취약하다. 따라서 이에 대한 보안 대책과 취약성 대비가 필요하다.

본 연구에서는 직렬통신구간의 보안성 향상을 위하여 불편과 제약이 최소화 되면서 HA(High Availabilty, 연간 Down-Time 30분 이내의 고가용성)를 지원하는 임베디드 리눅스 기반의 전력계통기기 보호용 보안 입출력 변환 장치를 함체내에 저가 고기능으로 동시에 구현하고 SCADA 테스트베드에서 성능시험 및 사이버공격에 대한 암호화장치의 대응을 실부하 테스트하였다.

특히 적용된 장치는 국가정보원 보안인증 사무국(NISS)의 가상사설망 VPN과 침입방지 IPS 알고리즘에 대한 CC EAL-3등급을 획득한 신뢰성이 특징으로 자체 구성한 접근, 개문, 조작 통제 논리 알고리듬을 병용함으로서 다양한 사양의 직렬통신망이 적용된 배전반 시스템 계통 등에 즉시 적용할 수 있을 것으로 기대된다.

개발된 전력계통기기 보호용 보안 입출력 변환 장치는 다음의 기능들을 추가적으로 개선하여 스마트그리드 기술도입에 따른 다양한 통신방식과 규약에 효과적으로 대비할 수 있을 것이다.

- IEC 61850
- 허용 I/O 수의 증대
- 무선 및 Fiber I/F 채용
- 진동 소음 적외선 UF연계 배전반 보안 및 계통 기기 방호 모듈로 융합

또한 본 연구에서 제안된 장치의 부가적인 기능 개선과 대규모 현장 실증을 통하여 향후 SCADA 시스템의 주요설비 보호와 악의적인 침입 및 해킹공격에 대한 대응과 운영상의 보완 대책은 다음과 같다.

- RS-485 구간 공격 시도시 Sniffing 및 Spoofing 탐지방법 고도화 및 대응 메커니즘 탑재
- 다양한 물리적 접근 통제 기능과 연동

위와 같은 해킹/크래킹 방호 대책이 보강되면 유용성은 한층 증대될 것이다.

References

[1] Nicholson "SCADA security in the light of Cyber-Warfare Computers & security" / v.31 no.4, (2012), pp.418-436 North-Holland ; Elsevier Science Ltd 0167-4048.

[2] Jong-joo Lee "A Development of Cipher Device based on Embedded Linux for Serial Communication in SCADA" Journal of the Korean institute of illuminating and electrical installation engineers / v.24 no.4, (2010), pp.25-32.

[3] Rosslin John Robles " Importance of Supervisory Control and Data Acquisition Security in Critical Infrastructure Increase", Journal of Korean institute of information technology / v.7 no.4, (2009), pp.198-207 Korean Institute Of Information Technology.

[4] Jong-joo Lee "A SCADA Testbed Implementation Architecture for Security Assessment" Journal of the Korean Institute of Illuminating and Electrical Installation Engineers (2010), 24(4) : 50~56.

[5] Young-Jin Kim "A Study on the Secure Plan of Security in SCADA Systems" Journal of the Korean Institute of Information Security and Cryptology, (2009), pp.145-152.

[6] Hak-Man Kim "Security Technology for SCADA Communication Data" Journal of the Korean institute of illuminating and electrical installation engineers, (2008.10), page(s): 3-394.

◇ 저자소개 ◇

최형석 (崔亨碩)
1961년 11월 6일생. 현재 촉탁 CIO, Sam Deuk Elec Co., LTD.
E-mail : d600183@hanmail.net

진창기 (秦彰基)
1971년 8월 6일생. 2001년 강원대학교 제어계측 공학과 석사 졸업. 현재 촉탁 CTO, Sam Deuk Elec Co., LTD.
E-mail : jinchangki@gmail.com

배기덕 (裵起德)
1972년 9월 25일생. 1999년 경남대학교 전산통계학과. 현재 CTO, XNSystems Co., LTD.
E-mail : comsta@xnsystems.com