Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1141

산업제어망 보안 컴플라이언스를 위한 패치 영향성 평가 방안에 관한 실증 연구

최 인 지[†‡]
한전 전력연구원 (선임 연구원)

A Empirical Study on the Patch Impact Assessment Method for Industrial Control Network Security Compliance

Inji Choi[†‡]
KEPCO Research Institute (Senior Researcher)

요 약

산업제어망은 대부분 독립된 폐쇄망으로 설치 이후 장기적으로 운영되면서 OS가 업데이트 되지 않아 보안 위협이 증가하고 보안 취약성이 존재한다. 제로 데이 공격 방어에는 최신 패치 적용이 필수로 이루어져야 하지만 대규모 산업망에서는 물리적인 장치를 직접 다루는 특성으로 더 높은 실시간성과 무중단 운영이 요구되기 때문에 실 운영 중인 시스템에 적용하기 어렵다. 이 문제를 해결하기 위해 신뢰로운 패치 적용을 위한 유틸리티사 고유의 패치 영향성 평가가 필요하다. 본 논문은 패치 시험에 대한 개념설계로부터 시스템 구현과 실증적용을 아우르고 있다. 패치 영향성 평가 방법론으로서 패치를 적용하기 전과 후의 시스템 고유 기능, 성능, 행위를 기반으로 시험 유형을 분류하고 반복 실험을 통해 패치의 안전성을 판정하는 최대 허용치를 제안하였다. 이후 산업제어망에 직접 적용한 결과 99.99% 가용성을 보장하면서 OS패치가 업데이트 되었다.

ABSTRACT

Most of the industrial control network is an independent closed network, which is operated for a long time after installation, and thus the OS is not updated, so security threats increase and security vulnerabilities exist. The zero-day attack defense must be applied with the latest patch, but in a large-scale industrial network, it requires a higher level of real-time and non-disruptive operation due to the direct handling of physical devices, so a step-by-step approach is required to apply it to a live system. In order to solve this problem, utility-specific patch impact assessment is required for reliable patch application. In this paper, we propose a method to test and safely install the patch using the regression analysis technique and show the proven results. As a patch impact evaluation methodology, the maximum allowance for determining the safety of a patch was derived by classifying test types based on system-specific functions, performance, and behavior before and after applying the patch. Finally, we report the results of case studies applied directly to industrial control networks, the OS patch has been updated while ensuring 99.99% availability.

Keywords: Security Compliance, Industrial Control System, Patch Impact Assessment, Patch Deployment

Received(08. 20. 2020), Modified(1st: 10. 15. 2020, 2nd: 11. 20. 2020), Accepted(11. 23. 2020)

† 주저자, inji.choi@kepco.co.kr
‡ 교신저자, inji.choi@kepco.co.kr(Corresponding author)

I. 서 론

산업제어망은 현장 설비 및 감시 장치와 연결되어 있고 중단 없는 서비스를 위해 주요 시스템이 한번 설치되면 운영 수명이 길다. 점차적으로 대규모 산업 제어망에서 운영 기술(OT : Operational Technology)을 위한 정보통신 기술(IT : Information Technology)의 도입이 확산되고 있는 상황 속에서 전력망 대상 사이버 보안 위협에 대한 우려와 관심이 증대되고 있다. 대규모 산업망은 네트워크 상에 존재하는 취약성이 존재하기 마련이고 이에 대한 최소한의 대응책으로서 시스템 및 소프트웨어 수준의 보안 패치 업데이트를 시행해야 한다. 미국의 NERC-CIP(North America Electric Reliability Corporation - Critical Infrastructure Protection)에서는 산업망의 중요 설비가 BES (Bulk Electric System)의 사이버 자산으로 분류된 경우, 매 35일 마다 새로운 패치에 대해 출처를 확인하고 적용 가능성을 평가할 것을 권고하고 있다[1]. 한국에서는 정보통신기반보호법에 의해 전력회사의 주요 설비는 보안성 관리 기반 시설로 지정되어 주요 OS, Software 패치 업그레이드를 권고하고 있다[2]. 이와 같은 법적 보안 규제에 대한 컴플라이언스를 위해 기업에서의 패치 관리는 필수임에도 불구하고 산업망에 적용한 사례는 부족한 실정이다[3][4]. 패치의 목적은 시스템의 보안을 향상시키거나 자원을 최적화 하는데 있으며 대부분 소프트웨어를 제공한 업체로부터 원작자 패치를 제공 받는다. 이때, 예상해 볼 수 있는 문제는 제어시스템과 호환성 문제, 백신 및 Anti-malware로 인한 오탐, 시스템 성능의 저하로 인한 안정성 및 신뢰성 저하가 있다. 따라서 해당 소프트웨어로 구동하는 시스템을 구축한 사용자는 내부적으로 패치를 시험하여 패치를 안정적으로 적용할 수 있는 방안뿐만 아니라 위와 같은 문제 발생 시 안전하게 제거할 수 있는 방안 등을 검토해야 한다. 본 논문에서 보이고자 하는 문제 해결 방안은 다음과 같다.

- 산업제어망에 신규 패치를 적용하기 전 영향성 평가를 위한 패치 시험 방법을 제안한다.
- 패치 시험 방법은 신뢰성, 안전성, 효율성 있는 절차와 도구를 사용한다.
- 실험 분석을 통해 안전성에 대한 합리적인 판정 기준을 도출한다.
- 현장 실증을 통해 이를 증명한다.

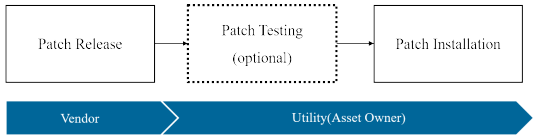

Fig. 1. Scope of roles according to patch life cycle

그림1에서 패치의 수명주기에 따른 패치 관리 범위와 역할을 개관하였다[5]. 제작사에서 패치가 업데이트되면 소유자 입장에서는 이를 자산 및 설비에 적용하기 전에 패치에 대한 시험, 평가를 수행할 필요가 있다. 현실은 모든 유틸리티(Asset Owner)가 구체적인 패치 평가 방법을 고안하지 못하고 있는 실정이며, 대부분 패치를 시스템에 적용하여 평가하는 데 수동으로 조작하고 있다. 또한 상용화 도구의 한계상 패치로 인한 유틸리티의 자산에 대한 시스템 영향성을 평가하기 위한 테스트 케이스가 충분하지 못하다. 본 연구에서 제시한 패치 시험 방법론은 유틸리티 시스템의 고유성과 평가 방법의 일반성을 고려하여 시험 시나리오와 평가 기준을 제안하고 있다. 아울러 한국전력공사의 대표 산업제어망을 선정하여 본 연구에서 제안한 패치 회귀분석 시험 방안을 영향성 평가로서 실증한 사례를 보이고자 한다.

II. 연구 개요

2.1 접근 방안

2.1.1 Compliance-driven approach

본 연구의 최초 접근은 기반시설 보호에 대한 규제준수(compliance)의 이슈에서 출발한다. 따라서 전력사에 적용하고 있는 패치 관리의 규제 항목을 점검할 필요성이 있다. 인터넷진흥원(KISA)에서는 주요정보통신기반시설의 취약점 분석 평가 상세 가이드라인에서 패치 관련 항목을 표 1과 같이 상세히 제시하고 있다. Unix(U-42), Windows(W31~33), HMI(PC-6~8), 보안장비(S-8), 네트워크 장비(N-6) 및 제어시스템(C-4) 분야에서 최신 패치를 적용하거나 최소한 안전하게 적용할 절차를 수립할 것을 권고하고 있다.

Table 1. Patch related vulnerability check item according to KISA guide

Code	Vulnerability Check Item
U-42	Apply the latest security patches and vendor recommendations
W-31	Apply the latest service pack
W-32	Apply the latest HOT FIX
W-33	Update an antivirus program
S-8	Apply the latest updates which vendor provides
N-6	Apply the latest security patches and vendor recommendations
C-4	Establish procedures such as the latest updates to the control system and test to safely apply security patches
PC-6	Apply the latest security patches such HOT FIX
PC-7	Apply the latest service pack
PC-8	Apply the latest security patches and vendor recommendations such as MS-OFFICE, Hangeul, Adobe Acrobat Reader etc.

2.1.2 Procedure-driven approach

OT 환경에 신규 패치 적용 시 최우선 고려사항은 가용성에 있다. 즉 새로운 패치는 현재 운영 중인 시스템에 오작동, 재부팅 오류, 과부하 등의 문제를 일으켜서는 안 된다. 그러한 패치는 사전 시험 통해 걸러져야 하고, 시스템은 전 상태로 회귀해야 한다. 이러한 사전 시험은 신뢰로운 패치 관리 프로세스 안에서 수행되어야 하며, 본 연구에서는 IEC 62443-2-3 규격에 따라 다음과 같은 절차대로 문제해결을 시도한다[5].

- Information Gathering : 패치 관리 대상 및 범위선정
- Monitoring & Evaluation : 패치 현황 및 수준 분석
- Patch Testing : 패치 파일의 진위 여부 확인부터 패치 후 변동사항까지 확인
- Patch Deployment : 패치 배포 절차 수립
- Verification & Reporting : 현장 적용 결과 검증 및 통합 관리시스템에 결과 전송

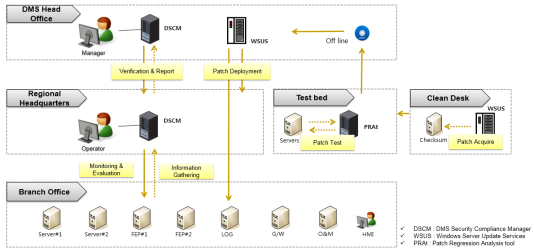

Fig. 2. Patch management practice in progress

그림 2는 한국전력공사의 대표적인 산업망을 대상으로 수행한 보안 컴플라이언스를 위한 패치 관리 시스템 및 절차를 개관한 그림이다.

2.2 연구 방법론

주요기반시설의 보안 프레임 워크에 의하면 제어시스템은 가용성의 요구사항을 충족시키는 방법으로 모든 보안적 조치를 취해야 한다[6]. 또한 즉각 패치가 어려운 제어시스템에 패치를 적용하기 위해서는 취약점을 통계적으로 평가하는 모델을 제시하고 있다[7]. 또한 보안 법규 기준에 만족(compliance)하기 위해서는 실 제어시스템에 적용하기 전 테스트 베드 검증이 필요하다[8].

본 논문에서는 패치의 안전성을 평가하고 판정해주는 기준을 세우기 위해 회귀분석 평가 모델을 참조하여 Patch Regression Analysis model을 세우고 이후 평가 기준을 Functionality, Availability, Security 세 부분으로 분류하였다.

이후 개발된 도구와 시험 시나리오를 통해 반복실험 후 초기 설정값을 세우고 통계적으로 뒷받침하기 위해 양적 연구를 수행하였다. 한편, 현장 적용 시범 실증을 통해 도출된 대표적인 케이스에 대해 테스트 베드에서 패치 회귀분석 평가 기준을 검증하였다. 아울러 이와 같은 검증 방법을 통해 안전한 패치를 획득한 후 한국전력공사의 대표적인 산업제어망인 Distribution Management System (DMS)를 대상으로 MS사의 OS Windows 패치를 업데이트 적용하였다. 이를 통해 산업망에 실적용을 위한 패치 회귀분석 사전영향평가 방법론을 확인 검증할 수 있었다. 이와 같은 연구 방법론은 미국전력연구소로부터 지원받아 수행한 연구 결과로 보고한 바 있으며 표 2에 정리한 바와 같이 본 논문에서는 추가적으로 실증 시험을 통한 개념확인을 하였다[9].

Table 2. Introduction of research methodology of this paper

Research methodology	Description
Patch Management Process	Reference to the IEC TR 62443-2-3 standard
Assessment model	Regression analysis through comparison before and after patch
Assessment method	Developed evaluation criteria and test case based on scenario
Implemented software tool	Patch Regression Analysis tool
Target system	Distribution Management System
Target patch	Windows OS patch from Microsoft
Proof of Concept	Field Trials applying to KEPCO DMS center

2.3 시험 유형

전력제어망 OT 시스템은 남한의 전력망을 종합 운영하는 시스템으로서 안전성, 가용성이 최우선시되고 있다. 전력 제어망의 OT 시스템은 용량 및 운영 목적에 따라 SCADA, DAS, HVDC 등으로 구분할 수 있지만 IT 시스템을 도입한 제어망이라는 공통점 하에 아래와 같이 4가지 시험 유형으로 분류할 수 있다.

- 메시지 기반 시험 : 운영 시스템 간 전송 메시지 상태를 확인
- UI(User Interface) 기반 시험 : 운영 시스템 화면에 표시된 상태를 확인
- 자원 사용량 시험 : 각 시스템 별 자원 사용량(CPU, 메모리)에 대한 변화량 확인
- Whitelist 기반 시험 : 각 시스템 별 허용되지 않은 프로세스 및 서비스 실행여부 확인

위의 4가지 유형의 시험은 각 OT 시스템별 환경에 적합한 시나리오에 따라 수행해야 한다. 시나리오는 4장에서 상세 논한다.

III. 패치 영향성 평가 기준

3.1 회귀분석 모델

회귀분석은 원래의 결과가 예상 결과와 어떻게 차이가 있는지 평가하고 독립 변수 중 하나가 변할 때 기준 변수의 값이 어떻게 변하는지를 분석한다. 회귀분석 모델에서 사용하는 평가 기준은 다음과 같은 것들이 있다.

- MAE(Mean Absolute Error) - 편차에 절대값을 씌운 결과의 평균(작은 에러에 민감)
- MSE(Mean Squared Error) - 편차 제곱의 평균(큰 에러를 최대한 줄이기)
- MedAE(Median Absolute Error) - 중간값에 절대값을 씌운 결과의 평균(이상치에 강함)
- R2 Score - 기존 생성 모델이 새로운 샘플에 얼마나 적합할지 판단해 주는 지표. Regression model의 성능을 mean value로 예측하는 모델과 상대적으로 비교하여 측정하기 위한 척도(0 ~ 1)

패치의 안전성 평가를 위해 Patch Regression Analysis Model은 패치 적용 전과 적용 후의 결과를 비교하여 변화량이 사전에 설정한 기준을 넘는지를 평가한다.

먼저 패치 적용 전에 시스템 간 통신 메시지, UI에 표시되는 특정 동작, 각 시스템 별 CPU, Memory usage에 관한 데이터는 각각 변수 'α'로 지정한다. 패치 적용 후 같은 시험 항목에 대하여 데이터를 각각 변수 'β'로 지정한다. 이 변수를 비교하여 절대값을 취한 뒤 다시 변수 'δ'로 지정한 뒤 허용치 'ε'와 비교하여 'fail'과 'success'로 나눈다. 변수 'δ'는 패치 전과 후의 값의 차이로서 물리적으로는 시스템 기능과 성능 면에서 변화량을 나타내는 척도이다.

Patch Regression Analysis Model에서 가장 중요한 것은 확률변수의 물리량 정의와 'fail'과 'success'를 결정하는 비교 변수, 즉 평가 기준의 정의이다. 이것은 Regression Analysis Model을 통해 비교, 분석하고자 하는 시스템의 특성을 얼마나 잘 대표하는지를 말한다.

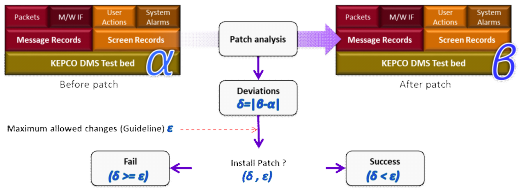

Fig. 3. Patch Regression Analysis Model

3.2 영향성 평가기준

보안 패치의 영향성 평가를 위해서는 시스템의 특성과 회귀분석 목적에 가장 잘 부합하는 기준치, 즉 'fail'과 'success'를 결정하는 평가 기준을 정의해야 한다. Patch Regression Analysis Model에서는 OT 시스템의 특징을 반영하여 Functionality, Availability, Security 영역으로 구분하여 제시하고자 한다.

Table 3. Evaluation Criteria Category

	Functionality	Availability	Security
Scope	- Application layer behavior	- System Performance	- System change based on security policy
Method	- Scenario Test case - Pass or Fail before and after patching	- Aging Test - comparison before and after patching	- Check security events or log files
Test case	- User Interface - Messages - Communication Protocol (ex. DNP)	- Usage of CPU - Usage of Memory - Usage of Disk	- Whitelist - Abnormal services - Port, Traffic Change
Criteria Value 'ε'	0	〈 5%	0

3.2.1 Functionality

OT 시스템이 사용하고 있는 응용 프로그램에 대한 기능을 테스트하기 위한 항목이다. OT 시스템 고유의 기능이 패치 전후로 잘 발휘되는지를 평가한다. 시험 방법은 UI기반 시험 시나리오와 메시지 기반 시험 시나리오는 각각 패치 전과 패치 후에 대해 반복 실행되며, 패치 전과 패치 후의 결과(즉, 전체 테스트 시나리오 중 성공한 시나리오의 개수)가 완벽하게 일치할 경우(ε=0)만을 성공으로 판정한다.

3.2.2 Availability

신규 패치 후에도 OT 시스템이 장시간 동안 지속적으로 정상 운영이 가능한지 확인하기 위해 시스템의 성능을 측정하는 항목이다. 시험 방법은 시스템을 15일 동안 가동하여 시스템 내에 사용되는 자원 변화량을 측정한다. 국내외 기준이 신규패치 발행 후 30~35일간의 관찰을 요하고 있으므로[1][2], 본 연구에서는 패치 전후 각각 15일 동안의 데이터를 수집, 분석한다. 즉 패치 설치 전 15일 동안의 시스템 자원과 패치 설치 후 15일 동안의 시스템 자원을 비교하여 사용량의 변화를 분석한다. 이때 자원 사용량은 CPU 사용률, 메모리 사용률, 디스크 사용률 등이 있다. Availability 영역의 안전성 판정 기준은 자원 사용률 변화량이 모두 5%를 넘지 않을 때 성공이라고 판정한다. Availability의 평가 기준 값인 5%는 도구 개발 시 기능 테스트 기간('16.12~'17.12) 동안 OT 시스템의 리소스를 측정하여 분석한 통계 데이터를 기준으로 선정한 값이고, 실험 설계자 및 관찰자, 제어시스템 담당자 및 설비 운영자, 보안담당자 등 본 산업설비 관련자들의 의견을 종합하여 설정하였다.

본 논문에서 제시한 판정 기준 허용치는 위의 기간 중 총 50회의 반복 실험에 의한 통계적 평균값을 적용하였고, 이때 시스템의 오작동 여부를 동시 관찰하였다. 그림 4는 신규 패치 적용 전(normal period)과 적용 후(comparison period) 자동화 시험 도구로 수집한 자원 사용량 비교 그래프 예제이다.

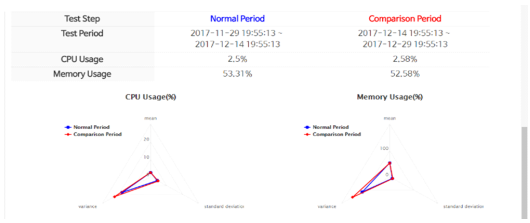

Fig. 4. Resource usage comparison graph

3.2.3 Security

시스템의 보안성을 확인하기 위한 항목으로 패치 전후로 동일한 서비스, 프로그램, 통신포트, 프로토콜이 운영되야 함을 전제한 시험이다. Security 시

험은 패치 전과 후에 Whitelist에 존재하는 서비스가 아닌 Abnormal 서비스나 프로그램의 실행을 검출하여 보안 문제를 확인한다. 단, Abnormal 서비스의 최종 판단은 담당자 검토를 통해 보안상 문제가 있는 서비스와 정상적인 서비스를 식별한다. 이외에도 허용되지 않는 통신 포트 스캔 및 통신프로토콜 검사 등이 이 범주의 시험 시나리오로 적합하다. Whitelist를 기반으로 허용 프로그램, 서비스 개수를 비교하여 패치 전후로 변화량이 없을 때($\varepsilon=0$) 성공으로 판단한다.

IV. 실증 시험

4.1 실증 환경

IEC 62443-2-3 패치 관리 규정 및 산업제어시스템 보안성 평가 방법론에 따르면 패치 시험은 대상 시스템과 동일 환경하에 동일 프로세스로 시험을 진행하는 것을 권고하고 있다[5][11]. 이에 따라 본 연구에서 한국전력공사에서 실제 운영 중인 DMS (Distribution Management System, 가칭)과 동일한 서버들로 구성된 테스트 베드를 구축하였다.

그림 5에서 WSUS(Windows Server Update Service)서버는 윈도우 업데이트를 관리하며 각 시스템에 패치를 배포한다. PRAt(Patch Regression Analysis tool) 서버는 패치의 영향성 평가를 위해 테스트 도구들을 실행시키고 시험 결과를 저장한다. 아울러 각 시스템별 시험 유형과 시나리오를 저장, 편집한다. DMS Security Compliance Manager는 각 시스템 별로 설치된 패치 현황과 신규 패치 정보를 저장한다. DMS는 SERVER#1, SERVER#2, LOG, HMI, FEP으로 구성되어 있으며 전력 계통망과 연결되어 필드 디바이스들과 통신한다.

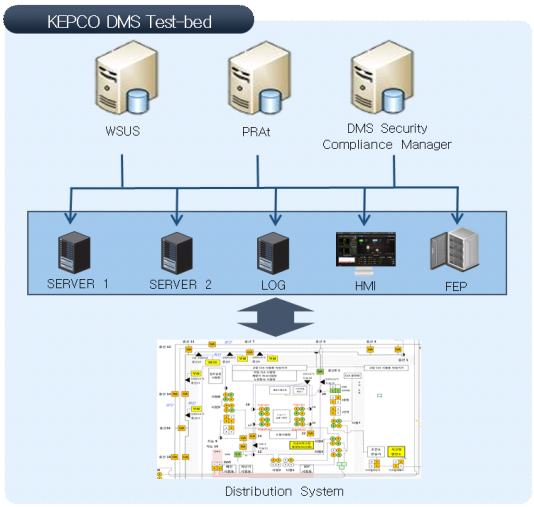

Fig. 5. Test-bed configuring map

4.2 시험 시나리오

산업제어시스템 보안을 위한 평가 방법론에 의하면 제어시스템 고유 특성을 반영해야 하는 것이 주요 고려사항이다[10][11]. 이에 따라 그림5의 DMS 각 시스템 별, 표2의 시험 유형별, 평가 범위별로 시험 시나리오를 구성한다. 시험 시나리오는 현장 계통 상황에 따라 가변적이며 표3은 DMS의 HMI 시스템을 대상으로 한 시나리오의 예제이다. 해당 시스템의 View(가칭) 응용프로그램의 UI 시험 7번 항목의 예제이다. 본 시험 항목은 공사용 개폐기를 추가하고 정상적으로 출력되는지 확인하고 있다. 응용프로그램 상의 UI화면 출력을 통해 시험 결과 값을 확인하고, PRAt 도구는 이를 자동화하여 비교분석 한다.

Table 4. Example of HMI Test Scenario

Test Case	Definition	Precondition
TC-View-UI-007	Check that the construction switch is displayed normally after add a construction switch	Exist the 'View' program on whitelist

4.3 실증 사례

4.3.1 시험 방법

시험은 실제 운영 중인 시스템의 H/W, S/W 및 프로그램 사양을 준수한 테스트 베드에서 수행하였다. 테스트 베드를 구성하고 있는 각 시스템은 전용 기능에 따라 시험 시나리오를 만들었고, 시험 유형별, 평가 기준별로 패치 전과 패치 후의 값을 비교하여, 패치의 안전성을 판정하였다. 표4는 DMS의 HMI 시스템을 대상으로 한 시험 방법(test case) 및 평가 기준(criteria)의 예제이다.

Table 5. Example of criteria for patch impact assessment (HMI case)

Category	Criteria	Setting value
Message test	Test result : success comparison counts	0
User Interface test	Test result : success comparison counts	0
Resource monitoring	Memory and CPU usage rate	〈5%
Whitelist check	Abnormal processes and services list comparison counts	0

4.3.2 실증 결과

실증은 DMS 테스트 베드에서 6개월('18.8~'19.1)에 걸쳐 매월 둘째 주 화요일마다 게시되는 Windows OS 패치를 활용하여 시험하였다. Patch Regression Analysis 시험은 DMS를 모사한 20 여종의 시스템을 대상으로 12종의 패치를 활용, 총 50회에 걸쳐 이뤄졌다. 표5는 DMS의 HMI 시스템을 대상으로 한 시험 결과의 예제이다.

시험 결과 다음의 결론을 도출할 수 있다.

- 메시지 시험은 패치 전/후 27개의 모든 시험 유형에 대하여 성공하였으며, 화면 시험은 패치 전/후 35개의 모든 시험 유형에 대해 성공하였다.
- 자원 모니터링에서 CPU 사용량은 1.36% 증가, 메모리 사용량은 1.12% 감소하여 각각 5% 미만의 증가량을 보였기 때문에 평가 기준을 만족한다.
- 비정상 프로그램은 패치 전/후 모두 검출된 비정상 프로그램이 없다. 패치 전과 후의 결과가 동일하므로 평가 기준을 만족한다.

Table 6. Example of result for patch impact assessment (HMI case)

Test		Pre-patch	Post-patch	Remarks	Result
Message test		Success: 27 Failure: 0	Success: 27 Failure: 0	-	Safe
UI test		Success: 35 Failure: 0	Success: 35 Failure: 0	-	Safe
Resource monitoring	CPU usage	0.58%	1.94%	1.36% increase	Safe
	Memory usage	48.27%	47.15%	1.12% decrease	Safe
Whitelist check		0	0	-	Safe

- 메시지, UI, 자원 모니터링, 비정상 프로그램의 결과가 모두 평가 기준을 만족하므로 이 패치는 안전하다고 판정한다.

이와 같은 과정을 통해 해당 보안패치의 안전성을 평가하고, 산업제어망 OT 시스템에 적합한 패치를 선정하는 시스템을 구축할 수 있다.

4.4 적용 결과

테스트 베드 실증을 통해 안정성을 검증 받은 패치를 한국전력공사 A본부 B센터의 DMS 시스템을 대상으로 업데이트 적용하였다. A본부의 경우 대부분 서버가 '14년, '16년 이후로 업데이트된 적이 없어서 누적 평균 131개, 2.27GB의 패치가 업데이트 대상이었다. OS 패치 이후에는 서버가 재부팅된다는 점을 고려하여 이중화 및 절체 작업을 병행하였다. 적용 결과 17대 서버 평균 46분의 재부팅 시간이 소요되었고 가용성 99.99%를 만족하였다.

V. 결 론

더 높은 실시간성과 무중단 운영이 요구되는 대규모 산업망에 패치를 적용하기 위해서는 가용성을 최우선으로 접근해야 한다. 보안패치 영향평가 기술은 주요 산업망에 최신의 소프트웨어로 패치 업데이트를 적용하기 전에 패치 파일의 안전성을 검증 및 평가하는 것을 의미한다. 이를 위해 제안한 평가 모델은 회귀분석(regression analysis)법으로써 패치를 적용하기 전과 적용 후의 비교 값의 차이를 통해 평가한다. 제안한 평가 기준에 따라 실 계통과 시스템을 모사한 테스트 베드에서 안전성을 검증한 패치는 실제 사업소에 적용함으로 패치의 시험에서 적용까지 실증하였다.

본 연구를 통해 안정성, 가용성 운전이 최우선인 산업제어망 운영시스템에서 시스템에 영향 없이 내부 시험평가 기준에 의해 안전성이 확보된 최신 패치를 적용 가능함을 보였다. 이는 폐쇄망으로 운영되는 기반시설을 대상으로 최초 적용하는 것으로서 상시 운영 가능한 점에서 실용적인 사례로 보고되고 있으며 당초 보안 규제 적용을 기술적으로 해결하고자 한 측면에서 국내외 법규의 패치 관련 항목을 대부분 만족하는 결과를 보였다.

References

[1] The North American Electric Reliability Corporation - Critical Infrastructure Protection-007-6, "Cyber Security - System Security Management," *North American Electric Reliability Corporation*, V6, Atlanta, GA, pp. 142-178, Jul. 2020.

[2] Korea Internet & Security Agency , "Guide of vulnerability analysis and assessment for information and communication infrastructure," *KISA*, Naju, Korea, 2017.

[3] Chee-Wooi Ten, Manimaran Govindarasu, Chen-Ching Liu, "Cybersecurity for Electric Power Control and Automation Systems", *2007 IEEE International Conference on Systems, Mand and Cybernetics,* Montreal, Que., pp. 29-34, Oct. 2007.

[4] J. Matt Cole, "Challenges of Implementing Substation Hardware Upgrades for NERC CIP Version 5 Compliance to Enhance Cybersecurity", *2016 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*, Dallas, TX, pp.1-5, 2016.

[5] IEC Technical Report 62443-2-3 " Security for Industrial Automation and Control Systems - Part 2-3: Patch Management in the IACS Environment. Ed. 1.0", *International Electrotechnical Commission*, June. 2015.

[6] Suyoen Lee, Jiyeon Yoo, Jongin Lim, "A Study on the Security Framework Design for Stable Operation of Critical Infrastructure Service", *Journal of Information Technology Services*, 15(4), pp.63-72, Dec. 2016.

[7] Ieck-Chae Euom, "A Study on the Prababilistic Vulnerability Assessment of COTS O/S based I&C System", *Journal of Convergence for Information Technology*, 9(8), pp.35-44, Dec. 2019.

[8] Kang Dong Joo, Kim Huy Kang "사이버 보안 관점에서의 전력시스템 신뢰도 기준 수립을 위한 NERC 규정 분석 및 국내 적용방안 연구", *Review of The Korea Institute of Information Security & Cryptology*, 25(5), pp.18-25, Oct. 2015.

[9] EPRI Technical Report 3002014137, " Patch Regression Testing Tool Analysis in Practice" , *Electric Power Research Institute,* Jan. 2019. https://www.epri.com/research/products/000000003002014137

[10] Yonghee Jeon, "Network Design and structure for industrial control system security", *Review of The Korea Institute of Information Security & Cryptology*, 19(5), pp.60-67, April. 2009.

[11] Myeonggil Choi, "A Study on Security Evaluation Methodology for Industrial Control Systems", *Journal of The Korea Institute of Information Security & Cryptology*, 23(2), pp.287-298, April. 2013.

〈저자소개〉

최 인 지 (Inji Choi) 정회원
2002년 2월: 충북대학교 전파공학과 졸업
2005년 2월: 충남대학교 정보통신공학과 석사
2005년 2월~현재: 한국전력공사 전력연구원
〈관심분야〉 산업제어시스템, 정보보호, 사이버보안