情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

보안측면에서의 산업제어시스템 비정상 행위 분류*

나 중 찬,† 조 현 숙‡
한국전자통신연구원

Classification of ICS abnormal behavior in terms of security*

Jung-Chan Na,† Hyun-Sook Cho‡
Electronics and Communications Research Institute

요 약

산업제어시스템의 사이버위협 특징은 의도하지 않았다고 하더라도 피해범위가 특정 시스템뿐만 아니라 네트워크의 서비스 제공을 위협하는 수준에 도달했다는 점이다. '보안'의 일부 범위는 단지 테러리스트나 사이버 해커의 고의적인 공격에 대한 시스템의 보호를 포함하지만, 종종 더 큰 피해는 의도적인 공격보다 부주의에 의한 설정 오류 또는 장비 고장 등의 비고의적인 행위로 이루어 진다. 본 논문은 고의적 공격, 실수, 장비 고장 및 소프트웨어 문제를 포함한 ICS의 모든 비정상 행위에 대한 분류를 제안하였다. ICS의 비정상 행위 분류 기준은 고의적인 공격뿐만 아니라 부주의한 행동의 공통점과 중요한 특징을 강조하기 위해 선정되었다.

ABSTRACT

Cyber threats of the ICS(Industrial Control System) has been researched on the level to the threat to the network service as well as a specific system, even if the extent of damage was not intended. Although some range of “security” just include the protection of systems against the deliberate attacks of terrorists or cyber hackers, often more damage is done by carelessness, and equipment failures than by those deliberate attacks. This paper presented a taxonomy for classifying all abnormal behaviors of ICS, including deliberate attacks, inadvertent mistakes, equipment failures, and software problems. The classification criteria of ICS abnormal behaviors was selected to highlight commonalities and important features of deliberate attacks as well as inadvertent actions.

Keywords: SCADA, Industrial Control System, Deliberate Attack, Inadvertent Actions

I. 서 론

산업제어시스템(Industrial Control System, ICS)은 가스/오일 파이프라인, 전력 전송시스템이나 물 분배시스템과 같은 대규모 지역에 걸쳐 시스템을 원거리 감시 제어할 수 있는 SCADA(Supervisory Control And Data Acquisition) 시스템과 제어시스템의 하부설비를 단위그룹으로 분산시켜 제어하는 분산제어시스템(Distributed Control System, DCS) 등을 포함하는 모든 종류의 산업자동화시스템을 일컫는다. 최근 ICS는 관리의 효율성과 호환성을 위해 IT 기술을 접목하고 있는 추세이며, 이에 따라 IT 기술의 보안 취약점과 더불어 ICS 운영환경에서 나타나는 취약점이 더해지고 있으며, 사이버 침해사고 사례와 인적 및 물적 피해에 따른 국가적 혼란을 야기시킬 수 있는 가능성에 대한 우려가 점차 높아지고 있

접수일(2013년 2월 20일), 수정일(2013년 4월 18일), 게재확정일(2013년 4월 18일)
* 본 연구는 지식경제부의 재원으로 한국산업기술평가관리원(KEIT)의 지원을 받아 수행한 산업융합원천기술개발사업(No. 10041560)입니다.
† 주저자, njc@etri.re.kr
‡ 교신저자, hscho@etri.re.kr

다[27].

ICS는 외부 네트워크로부터 단절되어 있는 관계로 로그인 기능을 제외하고 사이버보안 측면의 비정상 행위에 대한 고려를 거의 하지 않았으나, 최근 ICS를 표적으로 하여 이미 잘 알려진 일련의 침해사고들이 이것을 매우 중요하게 만들었다[7, 8, 24, 25]. 더욱 심각한 사항은 복잡하게 스턱스넷과 같은 악성코드를 이용해 ICS를 공격하는 것이 아니라 제어 프로토콜의 취약점을 직접 공격한다는데 그 위험성은 더 크다고 할 수 있다. 즉, ICS가 사용하고 있는 시스템 정보를 수집하여 스턱스넷과 같은 제로데이 공격보다 패킷 조작만으로 공격이 가능한 프로토콜 자체의 문제가 크다고 할 수 있다.

현재 국내·외적으로 ICS의 사이버 위협 또는 취약점을 찾기 위한 노력이 지속되고 있으며, 이와 관련된 침해사고 특징 패턴과 보안취약 점검 도구 활용 방안에 대한 관심이 높아지고 있다[10, 11, 12, 13, 14]. 특히 ICS 비정상 행위는 IT 시스템의 비정상 행위와 비슷하지만, 기존의 IT 사이버보안 기술을 배제하면서 ICS 환경을 위한 새로운 솔루션을 출시하였다[15]. 하지만 고의적 공격만을 고려하는 것은 자칫 가용성 보장에 한계를 가질 수 있다. 따라서 ICS 운영에 있어 높은 수준의 가용성과 보안성을 제공하기 위해서는 고의적 공격뿐만 아니라 비고의적인 ICS 구성요소의 설정 오류 및 ICS 장비 고장 등의 비정상 행위까지 포함한 ICS 보안상황 분류에 대한 연구가 필요하다.

본 논문은 보안 측면에서의 ICS 비정상 행위 분류에 관한 것이다. 본 논문의 구성은 2장에서 산업제어시스템 구조 및 비정상 행위의 범위와 함께 기존 관련 연구를 소개하고, 3장에서는 ICS 비정상 행위를 분류하며, 4장 결론을 끝으로 마친다.

II. 산업제어시스템 비정상 행위 개요

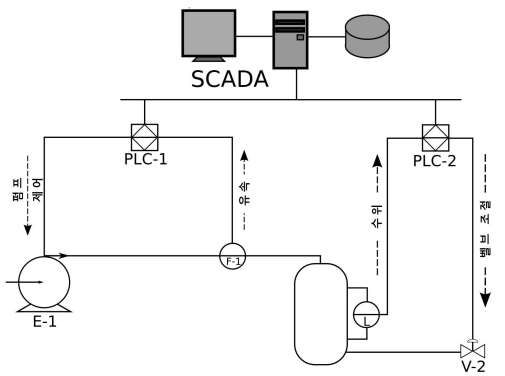
본 장은 ICS 비정상 행위를 분류하기에 앞서 ICS 구조, 비정상 행위의 범위 및 기존의 분류 방법에 대해 기술한다.

2.1 산업제어시스템 구조

ICS는 사용되는 대상과 목적에 따라 구조가 다르지만 일반적으로 사용자에게 운용 인터페이스를 제공하는 인터페이스부, 통신 기능을 수행하는 통신부, 실제 데이터를 생성, 제어, 관리하는 단말장치부 등의 구성요소를 갖는다.

인터페이스부는 필드장치로부터 수집한 상태정보를 운영자에게 제공하며, 운영자가 정보를 분석·판단하여 내린 제어명령을 단말장치에 전달하는 HMI (Human-Machine Interface), 콘솔 등으로 구성된다. 통신부는 필드장치와 서버간의 정보전송을 제공하기 위해 광, 구리선 등의 매체와 RS232 (Recommend Standard number. 232), RS485, Modbus, DNP3(Distribution Network Protocol 3.0) 등의 프로토콜을 이용한 유무선 통신 기능을 제공한다. 단말장치부는 대상 시스템의 다양한 상태 정보를 수집하는 센서, 수집 정보를 계측제어 서버로 전송하고, 계측제어 서버에서 전달된 제어명령을 해석하여 실제 제어대상 기기에 적합한 명령 신호를 보내는 기능을 수행하는 PLC(Programmable Logic Controller), DCS, 필드장치로부터 전송되는 계측 정보를 수집·분석하는 SCADA 서버와 수집 데이터와 로그정보 등을 저장하는 데이터 저장 서버로 구성된다.

[그림 1]은 ICS 구성요소를 포함하는 SCADA 시스템의 구성 예를 보인다.



[그림 1] 두 개의 PLC가 사용된 SCADA 시스템의 예

그림에서 SCADA 시스템(상단)은 유속과 수위를 읽고, 제어 및 설정값을 PLC에 내려보낸다. PLC-1(좌하단)은 측정된 유속을 설정값과 비교하고, 설정값에 근접하도록 펌프를 제어해 유속을 조절한다. PLC-2(우하단)도 측정된 수위를 설정값과 비교하고 밸브를 조절하여 설정값에 맞추는 작업을 한다[9].

SCADA 시스템 구조는 DCS를 하위 구성요소로 포함하고 있는 경우도 있다. 최근에는 중앙컴퓨터의 개입없이 일정 수준의 논리연산을 자동으로 수행할 수 있을 정도로 발전한 RTU(Remote Terminal Unit)

나 PLC를 사용하는 일이 점점 늘어나고 있으며, 제어 유형에 따른 ICS 구성요소는 〔표 1〕과 같다.

〔표 1〕 ICS와 SCADA

제어유형	제어장비
Process Conrol	DCS(Distributed Control System)
Discrete Control	PLC (Programmable Logic Controller)
Wide Area Control	MTU(Master Terminal Unit) / RTU(Remote Terminal Unit)

SCADA 시스템은 작업 공정을 조직화하는 쪽이며, 실시간으로 공정을 제어하지는 않는다. DCS는 하나의 현장에서 이루어지는 공정 기반 작업들을 처리하는 데에 주로 사용되고, SCADA 시스템은 지리적으로 널게 분산되는 형태의 이벤트 데이터 취합 기반 응용분야에서 선호된다〔9〕.

2.2 산업제어시스템의 비정상행위 범위

ICS의 운영자는 비용이 많이 드는 침해사고를 경험할 때까지는 ICS 사이버보안에 적절한 관심을 기울이지 않을 것이다. 그러나 ICS의 제어 프로토콜은 클라이언트의 요청에 대한 서버의 응답에 대한 인증, 인가에 대한 보안사항을 고려하지 않았기 때문에 프로토콜 자체의 보안 취약점에 의한 여러 공격 시도들이 가능하다. 이러한 보안 취약점 이외에도 가용성 관점의 서비스거부 공격들에 의한 ICS 비정상 행위유도가 가능하다. 제어 프로토콜은 태생적으로 사이버보안을 고려하지 않은 프로토콜로서 암호와 인증, 인가 기능을 추가한 프로토콜 상의 보안을 고려하더라도, 가용성 관점의 서비스거부 공격에 있어 여전히 보안 취약점과 함께 손쉽게 비정상행위로 이어질 수 있다〔4, 5, 6〕.

최근 들어서는 보안 측면의 ICS 비정상 행위는 고의적 공격뿐만 아니라 부주의 행동까지 강화하고 있다〔6〕. 즉, 산업제어시스템의 보안 범위는 테러리스트나 사이버해커의 고의적인 공격에 대한 시스템의 보호를 포함하고 있으나, 종종 더 많은 피해는 고의적인 공격보다는 부주의, 장비고장 및 자연재해에 의해 더 많이 이루어지고 있다〔2, 3〕.

따라서 본 논문에서는 고의적 공격뿐만 아니라 부주의에 의한 ICS 구성요소의 설정 오류 및 ICS 장비의 고장 등 비고의적인 상황까지 ICS 비정상 행위 범위를 확대하여 높은 수준의 가용성 및 보안성을 제공하는 기반을 갖고자 한다.

2.3 비정상 행위의 기존 분류방법

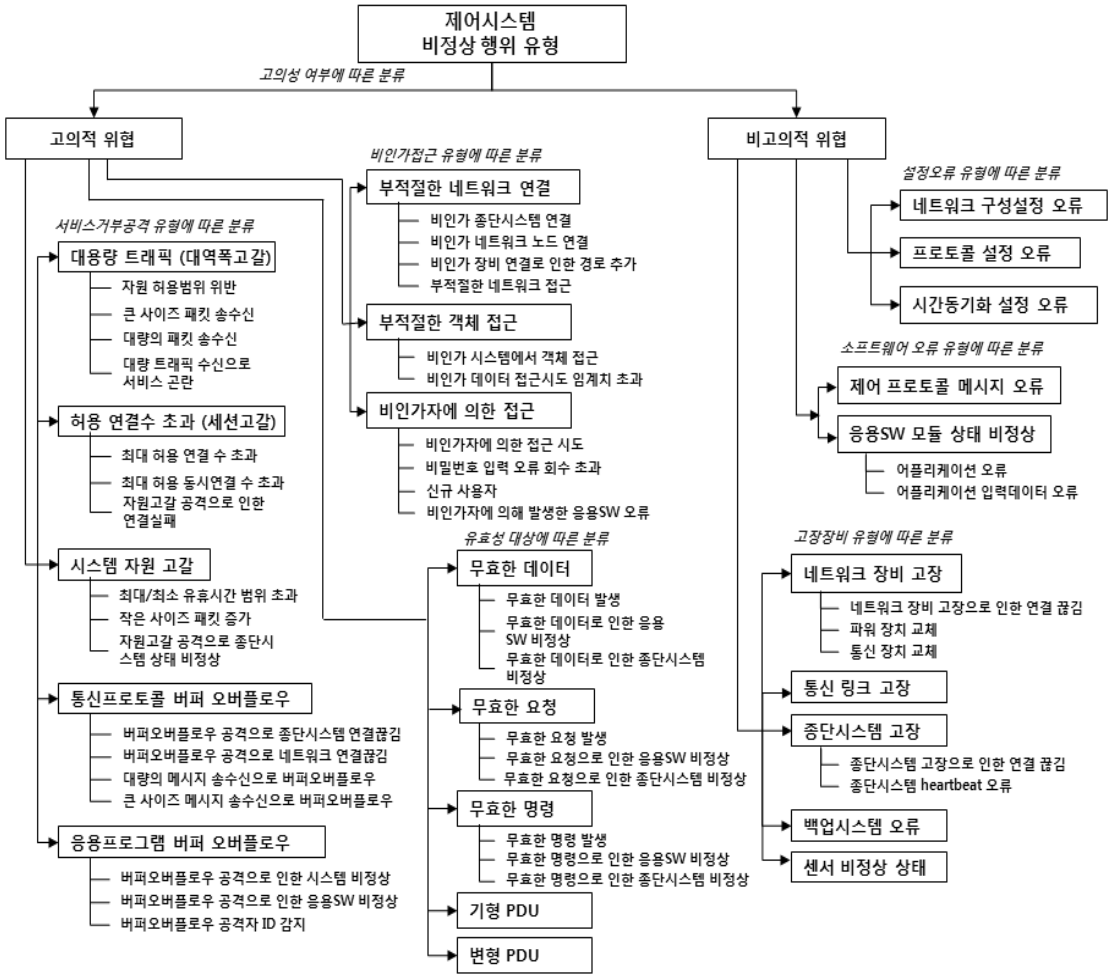
사이버공격 또는 비정상 행위와 관련하여 대부분의 기존 관련 연구는 통신 표준 또는 프로토콜, 통신 장치와 같은 IT 시스템에 대한 공격 또는 비정상 행위 분류에 초점을 맞추고 있다〔16, 17, 18, 19〕.

최근들어 ICS 제어 프로토콜 상의 서비스 거부 공격 등의 보안 취약점을 이용한 공격목표(제어 마스터 장치, 필드 장치, 통신 링크, 메시지 등)와 공격형태(차단, 가로채기, 변조, 위조 등)를 기준으로 하여 ICS 환경에서 발생하는 공격을 통신계층 단위로 나누어 분류하고, 이에 대한 방어를 위한 다양한 연구를 수행하였다〔20, 21〕. 또한 Bonnie Zhu〔22〕 등은 ICS 구성요소 중 하드웨어, 소프트웨어, 통신 스택으로 나누어 사이버공격을 분류하였으며, Terry Fleury〔23〕 등은 ICS의 공격, 취약점, 그리고 피해를 포함한 포괄적인 모델에 관하여 연구를 진행하였다. 국내에서는 정보의 기밀성, 무결성, 가용성 범주에 따라 제어시스템의 사이버 위협을 분류한 연구도 진행한 바 있다〔28〕.

기존 ICS 비정상행위 분류방법은 고의적인 행위에 기반하여 분류하였으며, 의도하지 않은 비정상 행위에 대해서는 고려하지 않는 단점이 있다. 본 논문은 최근 ICS 사이버보안 취약성 검증을 위한 도구〔10, 11, 12, 13, 14〕, ICS 침해사고 패턴 특징〔26〕, ICS에 특화된 사이버보안 상용제품〔15〕, ICS 관련 표준〔6〕 등을 기반으로 ICS에서 보안측면의 비정상 행위를 분류하고자 한다. 이는 네트워크 및 시스템 상태 감시, 사이버보안 침입탐지, 인프라의 성능 및 구성 관리정보 등을 기반으로하는 특징을 가지고 있으므로 ICS 제어 프로세스에 적합한 결과를 나타낼 것으로 예상한다.

III. 산업제어시스템의 비정상행위 분류

〔그림 2〕는 보안측면에서 ICS의 비정상행위 유형에 대한 포괄적인 분류표를 나타낸 것이다. 그림에서와 같이, ICS의 비정상행위는 고의성 여부에 따라 서비스 거부 공격, 비인가 접근, 데이터 유효성 등의 고의적인 비정상행위와 실수에 의한 설정 오류, 장비 고장, 소프트웨어 오류 등의 비고의적 비정상행위로 나뉘어진다.



〔그림 2〕 산업제어시스템의 비정상행위 유형

3.1 고의적인 행위에 따른 분류

ICS 비정상행위 중 고의적인 행위에 따른 분류는 크게 서비스 거부 공격, 비인가접근, 유효하지 않은 데이터 유형으로 분류할 수 있으며, 세부 내용은 아래와 같다.

3.1.1 서비스 거부 공격 유형에 따른 분류

서비스 거부 공격 유형에 따라 분류하면 대역폭 고갈 등을 야기하는 대용량 트래픽, 세션 고갈을 야기하는 허용 연결수 초과, 시스템 자원 고갈, 통신 프로토콜 상의 버퍼 오버플로우 및 응용 프로그램의 버퍼 오버플로우로 나눌 수 있다.

3.1.1.1 대용량 트래픽 발생에 의한 대역폭 고갈

자원 허용 범위 위반 유형이 발생하는 경우, 최소/최대 메시지 전송 시간, 최소/최대 메시지 크기, 전송 메시지 수 등이 허용된 값을 초과하는 현상이 나타난다. 또한 큰 사이즈 패킷 송수신이 발생할 때는 트래픽 볼륨은 설정값을 초과하고 트래픽 주기는 증가하지 않는 현상이 나타나고, 대량의 패킷 송수신이 발생할 때는 트래픽 주기와 트래픽 볼륨이 동시에 설정값을 초과하게 된다. 이러한 현상으로 인해 종단시스템의 비정상적인 상태가 발생할 수 있다. 특히 무의미한 제어 프로토콜 명령어를 반복시킴으로써 서비스 거부 현상이 발생할 수 있다.

3.1.1.2 허용 연결수 초과에 의한 세션 고갈

세션 고갈이 발생하면 연결 수와 동시 연결 수가 설정된 값을 초과함으로써 네트워크 연결이 끊기거나 종단 시스템 또는 응용 서비스의 비정상적 상태가 발생하기도 한다.

3.1.1.3 시스템 자원 고갈

시스템 자원 고갈에 의한 서비스 거부 공격은 최대/최소 유휴시간 범위 초과, 작은 사이즈 패킷 증가 등에 의해 발생할 수 있다. 또한 종단시스템의 최대/최소 유휴시간 범위가 초과하면 어플리케이션이 종료되거나 종단시스템의 비정상 상태가 발생하게 되며, 작은 사이즈 패킷이 증가하면 종단시스템의 네트워크 연결이 끊기거나 종단시스템의 "keep-alive" 메시지가 정상적으로 전달되지 못하는 등의 현상이 발생한다.

3.1.1.4 통신 프로토콜 버퍼 오버플로우

통신 프로토콜 버퍼 오버플로우에 의한 서비스 거부 공격이 발생하면 종단시스템의 네트워크 연결이 실패하거나, 네트워크 장비에서 접속 장애가 발생하기도 한다. 또한 메시지 수나 메시지 크기가 설정된 값을 초과함으로써 버퍼 오버플로우가 발생하기도 한다.

3.1.1.5 응용 프로그램 버퍼 오버플로우

응용 프로그램의 버퍼 오버플로우 발생으로 종단시스템의 비정상적 상태를 유발하여 종단시스템의 네트워크 연결이 끊기거나 종단시스템의 "keep-alive" 메시지 송수신이 불가능하게 되기도 하고, 응용 프로그램의 비정상 상태가 발생하거나 응용 프로그램이 종료되기도 한다.

3.1.2 비인가 접근 유형에 따른 분류

비인가 접근 유형은 부적절한 네트워크 연결, 접근 권한 대상에 따라 부적절한 객체 접근, 비인가자 또는 비인가 시스템으로부터의 접근 및 비인가 서비스 사용, 비인가 명령어 사용 등으로 구분할 수 있으며, 세부 분류는 다음과 같다.

3.1.2.1 부적절한 네트워크 연결

부적절한 네트워크 연결 유형으로는 비인가 종단시스템이 연결되거나 비인가 네트워크 노드가 연결되는 경우 및 비인가 네트워크 경로 추가 등이 있다. 부적절한 네트워크 연결이 발생하면 접근 제어 리스트에 포함되지 않은 시스템이나 시간 동기화가 되지 않은 시스템으로부터 메시지가 전송되거나 이용할 수 없는 링크를 통한 접근 시도가 발생하기도 하며, 비정상적인 프로토콜의 접근이 발생할 수도 있다.

3.1.2.2 부적절한 객체 접근

부적절한 객체 접근이 발생하면 인가되지 않은 데이터 접근 횟수 또는 인가되지 않은 접속 시도 횟수가 증가하게 되고 어플리케이션의 비정상 상태가 발생하기도 한다.

3.1.2.3 비인가자에 의한 접근

비인가자 접근이 발생하면 비정상적 프로토콜 접근 발생이나 비밀번호 입력 오류 횟수 증가, 응용 프로그램의 오류나 응용 프로그램 입력 데이터의 오류가 발생하기도 한다. 또한 관리자의 부주의로 인해 신규 사용자를 등록하지 않은 경우도 비인가자에 의한 접근과 동일한 현상이 나타날 것이다.

3.1.3 데이터 유효성 대상에 따른 분류

제어 프로토콜 상의 메시지 위·변조를 통한 시스템의 오작동을 유발하는 비정상 행위 유형은 제어 프로토콜 규칙에 어긋나는 유효하지 않은 데이터/요청/명령, 기형 PDU(Protocol Data Unit), 변형 PDU로 분류할 수 있다.

3.1.3.1 유효하지 않은 데이터/요청/명령

유효하지 않은 데이터, 요청, 제어명령은 비인가자 접근이나 비인가 데이터 접근에 의해 발생하거나, 종단시스템의 오류 또는 응용 프로그램의 오류로 인해 발생할 수 있다. 또한 유효하지 않은 데이터, 요청, 제어명령이 발생하면 응용 프로그램 자체 또는 응용 프로그램의 입력 데이터의 오류가 발생하거나 종단시스템의 비정상 상태가 발생하기도 한다.

3.1.3.2 기형 PDU

기형 PDU가 발생하면 어플리케이션이나 어플리케이션 입력 데이터의 비정상 상태가 나타난다. 기형 PDU는 각 통신계층마다 고려할 수 있는데, 데이터링크 계층와 TCP/IP(Transmission Control Protocol/Internet Protocol) 계층보다는 ICS ADU(Application Data Unit) 단위의 기형을 고려할 수 있다.

3.1.3.3 변형 PDU

변조 PDU가 발생하면 어플리케이션이나 어플리케이션 입력 데이터의 비정상 상태가 나타난다. 예를 들면, 제어 프로토콜 규격 상의 최대 길이를 초과하는 패킷이나 제어 프로토콜 헤더 상에 표기된 패킷 크기와 다른 크기를 갖는 패킷은 시스템의 비정상행위를 초래할 수 있다.

3.2 비고의적 행위에 따른 분류

ICS 비정상 행위 중 비고의적인 행위에 따른 분류는 크게 부주의에 의한 설정 오류, 소프트웨어 오류, 장비 고장 등으로 구분할 수 있다.

3.2.1 설정 오류 유형에 따른 분류

설정오류 유형에 따라 네트워크 구성 설정 오류, 프로토콜 설정 오류, 시간동기화 설정 오류로 구분할 수 있다.

3.2.1.1 네트워크 구성설정 오류

네트워크 구성설정 오류가 발생하면 접근 제어 리스트에 포함되지 않은 장비가 네트워크에 연결되거나, 인가된 장비의 네트워크 연결이 지속적으로 실패하는 현상이 나타난다. 일반적으로 제어 네트워크에서는 백업 장비와 백업 링크를 구성하고 있지만 지속적인 네트워크 연결 오류가 발생하면 네트워크의 가용성에 문제를 일으킬 수 있다.

3.2.1.2 프로토콜 설정 오류

프로토콜 설정 오류는 메시지 송수신 시스템 간의 프로토콜 ID나 프로토콜 버전 등 미리 지정된 프로토콜의 정보가 일치하지 않아서 발생한다. 프로토콜 불일치로 인해 전달되어야 하는 메시지가 전달되지 못하면 제어시스템의 가용성에 문제가 발생한다.

3.2.1.3 시간동기화 설정 오류

시간동기화 설정 오류는 메시지 송수신 시스템 간의 요구되는 수준의 시간 정확도 이상의 오프셋을 갖는 경우 발생한다.

3.2.2 소프트웨어 오류 유형에 따른 분류

소프트웨어 오류 유형에 따라서는 제어 프로토콜 메시지 오류와 응용 소프트웨어 모듈 상태 비정상으로 분류할 수 있다. 시간 동기화 오류 발생 시 제어 명령에 따른 대응이 실시간으로 이루어지지 않아 제어시스템의 운용에 문제가 될 수 있다.

3.2.2.1 제어 프로토콜 메시지 오류

비인가 시스템에 의한 제어 프로토콜 메시지 변조 및 기형에 의해 비정상적인 응용 소프트웨어 현상이 나타난다. 소프트웨어 모듈의 오류로 인해 비정상적인 프로토콜 메시지가 생성할 수 있으며 이러한 메시지는 제어 시스템이 정상적으로 동작할 수 없게 만들 수 있다.

3.2.2.2 응용 소프트웨어 모듈 상태 비정상

내재한 오류 또는 입력데이터 오류 및 무효한 요청/제어명령 등에 의해 비정상적인 응용 소프트웨어 현상이 나타난다. 응용 소프트웨어의 비정상 종료 등 오류가 발생하면 제어 시스템의 운용에 심각한 영향을 끼칠 수 있다.

3.2.3 고장 장비 유형에 따른 분류

고장 장비 유형에 따라 분류하면 네트워크 장비 고장, 통신 링크 고장, 종단시스템 고장, 백업시스템 고장, 센서 비정상 상태로 나눌 수 있다.

3.2.3.1 네트워크 장비 고장

네트워크 장비 고장이 발생하면 네트워크에 종단시스템의 비연결 상태가 검출되고, 네트워크 연결 실패 회수가 임계값을 초과하고, 연결-비연결 상태가 비정상적으로 반복되는 현상이 발생한다. 또한 파워 장치 교체가 발생하면 전원 손실 회수가 임계값을 초과하거나 전원 손실 시간이 전원 공급 시간보다 임계값 이하로 작아지는 비정상 상태가 발생된다. 통신 장치 교체가 발생하면 통신 매체 손실 회수가 임계값을 초과하거나 통신 매체 손실 시간이 통신 매체 연결 시간보다 임계값 이하로 작아지는 비정상상태가 발생한다. 일반적으로 제어 시스템에서는 백업 장비를 구축하고 있으나 메인 장비의 고장으로 인한 오류가 자주 발생할 경우 제어 시스템 가용성을 저하시키지 않도록 관리해야 한다.

3.2.3.2 통신 링크 고장

통신 링크 고장이 발생하면 정상 동작하고 있는 종

단시스템의 네트워크 연결이 끊기거나 메시지 전달 속도가 저하되어 백업 링크로의 전환이 발생하게 된다.

3.2.3.3 종단시스템 고장

IED, RTU 등의 종단시스템 고장이 발생하면 네트워크 연결이 끊기거나 연결-복구 과정이 비정상적으로 반복되며, "keep-alive" 메시지 전송이 중단되는 현상이 발생한다. 또한 종단 시스템 고장으로 인해 응용 소프트웨어도 실행되지 못하므로 제어 시스템의 가용성에 영향을 미치게 된다.

3.2.3.4 백업시스템 오류

백업시스템 오류가 발생하면 백업 디바이스, 백업 법 시스템, 백업 어플리케이션의 비정상 상태가 발생한다. 백업 시스템이 정상 동작하지 않으면 메인 시스템의 오류 시 제어 시스템의 운용에 심각한 문제가 된다.

3.2.3.5 센서 비정상 상태

센서 비정상 상태가 발생하면 센서로부터 발생하는 신호가 제한값을 초과하거나 신호 발생 주기가 설정값을 초과하는 현상이 나타난다.

기존의 비정상 행위 분류 방법에서는 비고의적 위협을 사람의 실수 등으로 간략히 설명하는 반면, 본 논문에서는 제어시스템에 위협이 되는 여러 요인을 고의적으로 발생하는 공격과 비고의적으로 발생하는 위협으로 분류함으로써 제어 시스템의 가용성 보장 범위를 확대하는 분류 방법을 제시하였다.

IV. 결 론

ICS의 많은 비정상 행위는 이론적으로 정리하기가 쉽지 않다. 그럼에도 불구하고 본 논문에서는 기존의 고의적인 비정상행위 분류 방법에서 부주의에 의한 설정 오류 및 장비 고장 등의 비고의적인 비정상행위까지 확장하여 상세한 보안상황 분석을 하여 가용성 및 보안성 수준을 향상시킬 수 있는 ICS 비정상 행위 분류를 제안하였다. ICS 비정상 행위 분류 결과는 위험 분석 및 완화 전략 수립과 신뢰성을 갖는 ICS 제어 프로토콜 설계에 도움을 줄 것이다.

본 논문에서 분류한 ICS 비정상 행위에 대하여 사전방지 및 탐지 방법은 추후 연구로 남겨둔다.

참고문헌

〔1〕 Repository for Industrial Security Incidents(RISI), "Report on Cyber Security Incidents and Trends Affecting Petroleum Industrial Control Systems," Annual Summary 2010, Dec. 2010.

〔2〕 Stewart Baker, Natalia Filipiak, and Katrina Timlin, "In the Dark, Crucial Industries Confront Cyberattacks," http://www.mcafee.com/us/resources/reports/rp-criticalinfrastructure-protection.pdf, Apr. 2011.

〔3〕 BCIT, "Industrial Security Incident Database(ISID)," http://www.bcit.ca/appliedresearch/security/services.shtml, 2008.

〔4〕 IEC, "Power Systems Management and assoicated Information Exchange - Data and communications security - Part 5: Security for any profiles including IEC 60870-5," IEC/TS 62351-5, May 2007.

〔5〕 Igor Nai Fovino, Andrea Carcano, Marcelo Masera and Alberto Trombetta, "Design and Implementation of a Secure Modbus Protocol," Critical Infrastructure Protection III, Springer, 2009.

〔6〕 IEC, "Power Systems Management and assoicated information exchange - Data and communications security - Part 7: Network and system management (NSM) data object models," IEC/TS 62351-7 Edition 1.0, Oct. 2010.

〔7〕 Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32. Stuxnet Dossier, Symantec Security Response, Version 1.4," http://ww w.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32 stuxnet dossier.pdf, Feb. 2011.

〔8〕 Phil Muncaster, "Stuxnet-like attacks beckon as 50 new Scada threats discovered," http://www.v3.co.uk/v3-uk/ news/2045556/stuxnet-attacks-beckon-scada-thre

atsdiscovered, Apr. 2011.
[9] Wikipedia, "SCADA," http://en.wikipedia.org/wiki/SCADA, 2013.
[10] NMAP.ORG, "Nmap - Free Security Scanner For Network Exploration & Security Audits," http://www.insecure.org/nmap, Apr. 2005.
[11] TENABLE Network Security, "Nessus Professional," July 24, 2012.
[12] Digital Bond Inc., "Basecamp," http://www.digital-bond.com/tools/basecamp, 2013.
[13] RAPID7, "Metasploit Pro User Guide Release 4.3," Dec. 2012.
[14] SCADAhacker.com, "Hacking using Nmap, Nessus and Metasploit," http:// scadahacker.com/howto/howto-hacking_tools1.html, 2011.
[15] Byres Security Inc., "Tofino Argon Security Appliance," Data Sheet DS-TSA-ARGON Ver. 5.0, 2010
[16] Simon Hansman and Ray Hunt, "A taxonomy of network and computer attacks," Computers & Security, DTD5, 2004.
[17] John D. Howard, "An Analysis Of Security Incidents On The Internet 1989 - 1995," Carnegie Mellon University, April 1997.
[18] Kevin S. Killourhy, Roy A. Maxion and Kymie M. C. Tan, "A Defense-Centric Taxonomy Based on Attack Manifestations," Proceedings of International Conference on Dependable Systems & Networks: Florence, Italy, 28 June - 01 July 2004.
[19] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communications Review, Volume 34, Number 2, April 2004.
[20] Samuel East, Jonathan Butts, Mauricio Papa, and Sujeet Shenoi, "A Taxonomy of Attacks on the DNP3 Protocol," Critical Infrastructure Protection III, Springer, 2009.
[21] Peter Huitsing, Rodrigo Chandia, Mauricio Papa, and Sujeet Shenoi, "Attack taxonomies for the Modbus protocols," International Journal of Critical Infrastructure Protection, Dec. 2008.
[22] Bonnie Zhu, Anthony Joseph and Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems," in Proc. Internet of Things (iThings/CPSCom), 2011.
[23] Terry Fleury, Himanshu Khurana, and Von Welch, "Towards A Taxonomy of Attacks against Energy Control Systems," Critical Infrastructure Protection II, The International Federation for Information Processing Volume 290, pp 71-85, 2009.
[24] Jayne Caswell, "Survey of Industrial Control Systems Security," http://www.cse.wustl.edu/~jain/cse571-11/ftp/ics/index.html, 2011.
[25] Bill Miller and Dale C. Rowe, "A Survey of SCADA and Critical Infrastructure Incidents," RIIT'12, Oct. 11 - 13, 2012.
[26] Digital Bond Inc., "SCADA Protocol IDS Signature," http://www.digitalbond.com/tools/quickdraw, 2013.
[27] 전용희, "산업제어시스템 정보보호 : 개요," 정보보호학회지, 제 19권 제 5호, 한국정보보호학회, pp. 52-59, 2009년 10월.
[28] 김태식, 강동주, "전력시스템의 사이버보안 위협 규명 및 분류에 대한 연구," 보안공학논문지, 제 9권 제 1호, pp. 53-65, 2012년 9월.

〈著者紹介〉

나 중 찬 (Jung-chan Na) 종신회원
1986년 2월: 충남대학교 계산통계학과 학사
1989년 2월: 숭실대학교 전자계산학과 석사
2004년 2월: 충남대학교 컴퓨터과학과 박사
1989년 2월~현재: 한국전자통신연구원 융합보안연구실 실장
〈관심분야〉 제어시스템 보안, 네트워크 보안

조 현 숙 (Hyun-Sook Cho) 종신회원
1979년 2월: 전남대학교 수학교육학과 학사
1989년 2월: 전남대학교 컴퓨터공학과 석사
2001년 2월: 충북대학교 컴퓨터공학과 박사
1982년 6월~현재: 한국전자통신연구원 사이버보안연구단 단장
〈관심분야〉 모바일 보안, 제어시스템 보안, 네트워크 보안