Chapter 06

제어시스템

1. 계정 관리 ····· 472
2. 서비스 관리 ····· 484
3. 패치 관리 ····· 501
4. 네트워크 접근통제 ····· 507
5. 물리적 접근통제 ····· 519
6. 보안위협 탐지 ····· 522
7. 복구 대응 ····· 525
8. 보안 관리 ····· 539
9. 교육 훈련 ····· 551

01 제어시스템 장비 취약점 분석 · 평가 항목

1. 계정 관리

점검항목	항목 중요도	항목코드
계정 기능이 있는 제어시스템 구성요소에 대해 계정을 안전하게 설정하여 사용	상	C-01
제어시스템 계정의 로그인/로그아웃, 사용 명령 등 사용기록을 저장	상	C-02
제어시스템 계정입력 시 비밀번호 마스킹 처리, 입력값 에러 발생 시 제공 정보 제한 수행	상	C-03
제어시스템 계정을 관리, 운영, 유지보수 등 용도에 따라 분리하고 운용	중	C-04
제어시스템 계정에 대해 관리, 운영, 유지보수 등 용도에 맞는 최소 권한 부여	중	C-05
제어시스템 운전원별 유일 계정 부여 또는 시간별 사용자 기록 유지	중	C-06

2. 서비스 관리

점검항목	항목 중요도	항목코드
제어시스템 구성요소에 대한 시간 동기화 수행	상	C-07
제어시스템에 불필요한 서비스 및 취약한 서비스 제거 또는 보완대책 수행	상	C-08
제어시스템 구성요소에 대한 관리자 페이지 운영 시 이에 대한 접근통제(사전인가 접근만 허용) 수행	중	C-09
제어시스템 내 파일/디렉터리 접근 권한 및 신뢰 관계를 적절히 부여	중	C-10
제어시스템 내 제어와 직접적인 관련이 없는 불필요 프로그램 삭제	중	C-11
제어시스템 운영 정보, 제어 명령 등 중요 정보에 대한 위변조 및 replay 공격 방지 대책 적용	중	C-12
제어시스템 내 전달되는 제어 명령 및 파라미터의 정상 범위를 식별하고 관리	하	C-13
제어시스템 내 사용자 통신 세션에 대해 세션 타임아웃 적용	하	C-14
GPS 스푸핑/재밍 공격 등 시각 동기화 서비스를 교란하기 위한 공격에 대비한 보안 조치 수행	하	C-15

3. 패치 관리

점검항목	항목 중요도	항목코드
제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 제조사 협력방안, 테스트 방안 등의 절차 수립	상	C-16
외부 업체, 인터넷을 통한 다운로드 등의 경로로 반입된 각종 패치·업데이트 파일에 대해 무결성 검증 및 클린 PC를 통한 악성코드 존재 여부 검사 수행	상	C-17
제어시스템 구성요소의 알려진 취약점에 대해 보안패치 적용 또는 상응하는 대응책 적용	상	C-18
운영체제, 응용프로그램, 펌웨어 등에 대한 안정성이 확인된 최신 버전의 소프트웨어 사용 및 기술지원이 종료된 제품 미사용	중	C-19
제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축	하	C-20

4. 네트워크 접근통제

점검항목	항목 중요도	항목코드
제어 네트워크는 업무망, 인터넷, CCTV망 등 외부망과 물리적으로 분리하여 사용	상	C-21
제어 네트워크 외부로 자료전달 시 물리적 일방향 자료전달 환경을 구축하여 외부에서 제어 네트워크로의 침입을 차단	상	C-22
제어 네트워크에 무선인터넷, 테더링, 외부 유선망 등의 외부망 연결을 제한하고 주기적으로 점검	상	C-23
제어 네트워크에 비인가된 시스템/기기에 대한 연결 및 접속을 차단	상	C-24
물리적 일방향 자료전달 환경의 올바른 동작 및 운용에 대한 주기적인 점검 수행	상	C-25
제어 네트워크를 용도에 따라 세분화하고, 접근제어를 수행하여 제어시스템 운영에 필요한 네트워크, 시스템 간의 통신만 허용	하	C-26

5. 물리적 접근통제

점검항목	항목 중요도	항목코드
제어시스템에 대해 네트워크 포트, USB 포트 등 외부 연결 접점에 대해 허가받은 사항을 제외하고 모두 물리적 또는 논리적으로 차단	상	C-27
제어시스템 구성요소를 물리적으로 보호할 수 있는 조치 적용(잠금장치가 있는 함체, 랙, 수납 책상 등)	중	C-28

6. 보안위협 탐지

점검항목	항목 중요도	항목코드
백신 프로그램 설치가 가능한 제어시스템 구성요소에 대해 악성코드 감염 및 차단을 위한 백신 프로그램 설치	상	C-29
이상 트래픽 발생 탐지 등 제어시스템 내의 보안 관리를 위해 적합한 침입탐지시스템 등을 구축 및 운용하고, 구축된 보안 솔루션 및 보안 장비에서 탐지한 보안 이벤트에 대해 모니터링 수행	하	C-30

7. 복구 대응

점검항목	항목 중요도	항목코드
제어시스템 대상 사이버 위기대응 매뉴얼을 수립	상	C-31
제어시스템 대상 사이버 위기대응 훈련을 정기적으로 시행	상	C-32
제어시스템 침해사고 대응을 위한 제어시스템 설정, 중요 데이터 등을 백업 및 관리	상	C-33
제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 수립	중	C-34
제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행	중	C-35
제어시스템 조작 불능에 대비하여 수작업 운전 매뉴얼 작성 및 교육훈련 시행	중	C-36
제어시스템의 각종 이벤트에 대한 로그를 관리하기 위한 중앙집중식 로그 관리 수행	하	C-37

점검항목	항목 중요도	항목코드
제어시스템 구성요소의 기준 형상을 설정하고 변경 및 업데이트 시 형상관리 수행	하	C-38
제어시스템 주요 장비 및 제어 네트워크 장비에 대해 이중화	하	C-39
제어시스템 보호를 위한 화재탐지 설비 및 화재 진압설비를 구비	하	C-40
제어시스템 보호를 위한 누수탐지 설비 및 침수 대응 장비 구비	하	C-41
제어시스템에 대하여 정기적으로 사이버 위험 시나리오를 식별하고, 완화방안 수립	하	C-42

8. 보안 관리

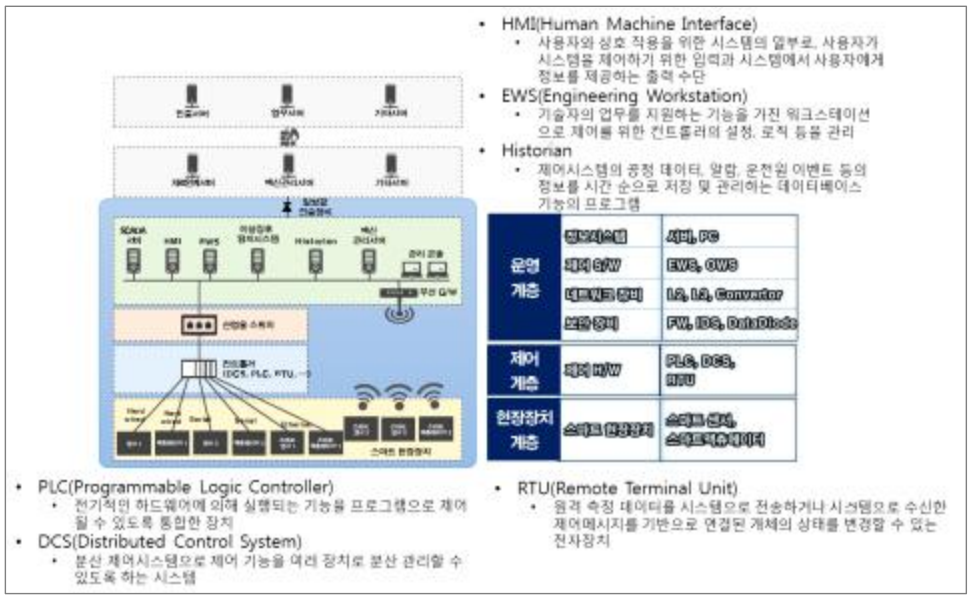
점검항목	항목 중요도	항목코드
제어시스템 구성요소에 대한 자산정보(담당자, 펌웨어 버전, 설치 SW 등)를 항상 최신으로 유지관리	상	C-43
제어시스템 중요 구성요소가 설치된 장소를 보호구역으로 설정	상	C-44
제어시스템에서 USB 등 이동형 저장 매체를 사용해야 하는 경우, 사전정의된 정책에 따라 사용	상	C-45
제어 네트워크에 연결되는 외부 정보통신기기 반·출입 시 클린존 통과, 관리대장 작성 등 관리절차 마련	상	C-46
제어시스템의 특성을 반영한 정보보안 정책, 지침을 수립	중	C-47
제어시스템 운영 업무에 대해 표준 업무 절차서를 작성하고 적용	중	C-48
제어시스템 유지보수를 위한 전용 장비(노트북 등)를 마련하고 관련 정책을 시행	하	C-49
허가에 의한 로직 변경 정책 수립	상	C-50

9. 교육 훈련

점검항목	항목 중요도	항목코드
제어시스템 운전원, 관리자, 유지보수인력, 보안 인력에 대해 직무별 직무교육을 정기적으로 실시	하	C-51

C-01 (상)	제어시스템 〉 1. 계정 관리
	계정 기능이 있는 제어시스템 구성요소에 대해 계정을 안전하게 설정하여 사용

개요	
점검 내용	제어시스템의 계정 기능이 존재하는 모든 설비에 대해 계정을 안전하게 설정하여 인가되지 않은 사용자의 접근 차단 여부 점검
점검 목적	제어시스템 구성요소의 계정 기능을 활성화하고 안전하게 설정하여 제어시스템이 인가되지 않은 접근으로부터 보호할 수 있도록 함
보안 위협	제어시스템 구성요소에 계정을 안전하게 설정하지 않는 경우 비인가자가 구성요소에 접근하여 이를 장악하여 구성요소 내 정보 획득 및 악의적으로 조작할 수 있음
참고	※ **제어시스템의 기본 구성도 및 각 구성요소** 제어시스템의 구성요소로는 크게 제어 H/W, 제어 S/W, 네트워크 장비, 정보시스템, 보안 장비로 이루어져 있으며, 이러한 구성요소에 대한 예시 및 일반적인 구성도는 다음 그림과 같음



[제어시스템의 기본 구성도 및 각 구성요소 예시]

※ **HMI 및 PLC 예시**

[HMI 화면 예시]

[PLC 기기 예시]

점검 대상 및 판단 기준	
대상	제어시스템 구성요소 전체
판단 기준	**양호 :** 계정 기능을 활성화하고 안전하게 설정하여 인가된 사용자만 접근이 가능한 경우
	취약 : 계정 기능을 비활성화하거나 안전하지 않게 설정하여 비인가 된 사용자가 접근이 가능한 경우
조치 방법	제어시스템 구성요소의 계정 기능을 활성화하고 안전하게 설정
조치 시 영향	일부 제어시스템 설정에 따라 접속 오류 발생 가능

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소 전체 중 계정 기능이 있는 구성요소를 식별

- 계정 기능이 존재하지 않은 기기에 대해서는 자체적으로 보안대책을 수립할 것을 권고

[Windows OS]

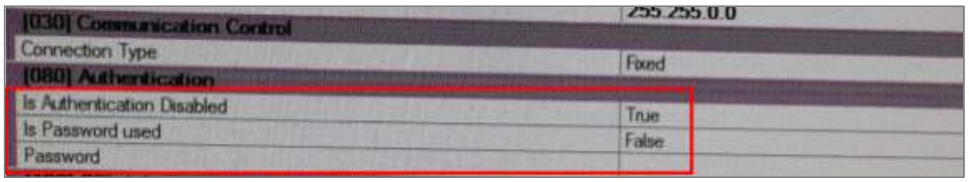
- 운영자, 관리자별 계정 발급 확인
  - 시작 > 제어판 > 사용자 계정
- (개선조치 시) 제어시스템 운영자, 관리자별 계정 추가
  - 시작 > 제어판 > 사용자 계정 > 추가

[Unix OS]

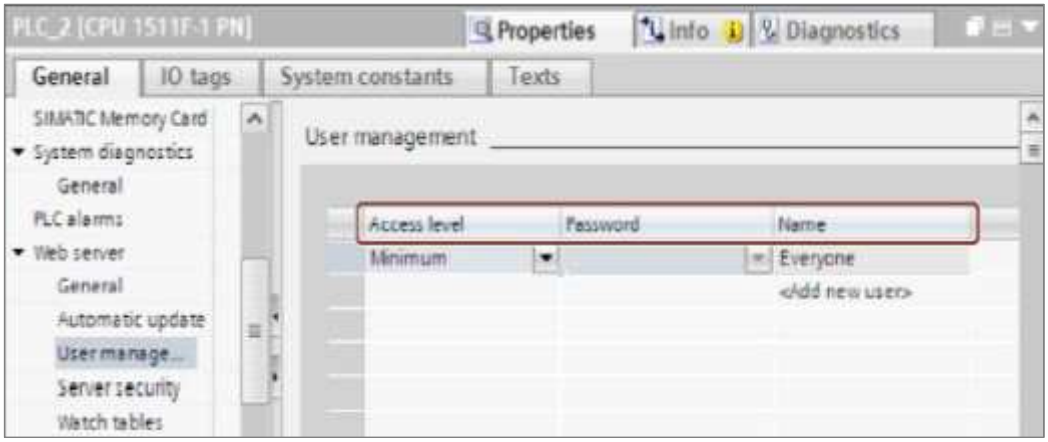
- 운영자, 관리자별 계정 발급 확인
  - #cat /etc/passwd
- (개선조치 시) 제어시스템 운영자, 관리자별 계정 추가
  - #useradd 계정명

Step 2) 식별된 구성요소를 대상으로 계정 기능의 활성화 여부 확인

- PLC, DCS 등의 제어 H/W와 이를 운영하는 EWS, OWS와 같은 제어 S/W의 경우 제조사별로 계정 기능의 관리, 확인 과정이 상이하므로 해당 제품의 매뉴얼을 통해 확인하거나 개발사에 문의하여 확인



[제어 H/W 제품 중 식별기능 설정 화면 예시]



[제어 H/W 제품 중 사용자 계정 관리 화면 예시]

Step 3) 계정 이름 및 비밀번호를 안전하게 설정했는지 여부 확인

- 기본 계정 및 비밀번호를 변경했는지 확인
- 비밀번호는 문자, 숫자, 특수문자를 조합한 8자리 이상으로 설정되어 있는지 확인

C-02 (상)	제어시스템 〉 1. 계정 관리
	제어시스템 계정의 로그인/로그아웃, 사용 명령 등 사용기록을 저장
개요	
점검 내용	운영자, 관리자 등의 계정 접근을 허용하는 제어시스템의 계정 접속 로그인 및 사용 기록(Log) 저장 여부 점검
점검 목적	제어시스템(운영체제, HMI 등)의 계정 접속 로그인 및 사용 기록(Log)이 저장되도록 하여 계정 사용에 대한 책임 추적성(Accountability)을 높일 수 있도록 함
보안 위협	계정 접속 로그인 및 사용내역 등의 접속기록(Log)이 생성되지 않거나 접속기록의 내용이 미흡(예시: 사용내역 누락)하여 책임 추적이 어려울 수 있음
참고	※ **접속기록(Log):** 시스템(운영체제) 또는 응용 프로그램의 접속기록은 접속자(예시: ID), 접속일시, 접속자의 위치(예시: IP주소), 사용내역(예시: 운영체제의 명령 실행 또는 제어설비에 밸브 조작 명령 실행) 등 4가지 유형의 정보를 포함하는 데이터
점검 대상 및 판단 기준	
대상	대상 시스템에 접속하기 위해 계정(ID) 접근이 요구되는 제어시스템 구성요소
판단 기준	**양호 :** 대상 기기에 로그인/로그아웃, 사용 명령 등의 사용기록을 저장하고 있는 경우
	취약 : 대상 기기에 로그인/로그아웃, 사용 명령 등의 사용기록이 저장되지 않아 확인할 수 없는 경우
조치 방법	대상 구성요소에 사용기록이 저장되도록 설정을 적용하거나, 다른 기기를 이용하여 대상 구성요소의 사용기록이 저장되도록 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 로그인/로그아웃, 사용 명령 등의 사용기록이 저장되도록 설정되어 있는지 확인

- 생성된 사용기록(별도 파일 또는 DB)의 내용에 사용자의 로그인, 로그아웃, 사용 명령의 내용을 포함하고 있는지 확인

15	02:28:35.182	2012-01-31	수신 이벤트	Logon denied for Web server user 2 -
16	02:28:32.256	2012-01-31	수신 이벤트	Logon denied for Web server user 2 -
17	02:28:29.146	2012-01-31	수신 이벤트	Logon denied for Web server user 2 -
18	02:28:05.202	2012-01-31	수신 이벤트	Logon denied for Web server user 2 -
19	02:27:39.368	2012-01-31	수신 이벤트	Logon denied for Web server user 2 -
20	02:23:23.618	2012-01-31	수신 이벤트	Communication initiated request: WARM RESTART - CPU changes from STARTUP to RUN mode
21	02:23:23.549	2012-01-31	수신 이벤트	Communication initiated request: WARM RESTART - CPU changes from STOP to STARTUP mode
22	02:21:03.415	2012-01-31	수신 이벤트	PLC project backup successfully created -
23	02:21:02.461	2012-01-31	수신 이벤트	PLC project backup via ES started -
24	02:20:02.694	2012-01-31	수신 이벤트	Communication initiated request: STOP - CPU changes from RUN to STOP mode
25	02:09:39.639	2012-01-31	수신 이벤트	Communication initiated request: WARM RESTART - CPU changes from STARTUP to RUN mode
26	02:09:39.568	2012-01-31	수신 이벤트	Communication initiated request: WARM RESTART - CPU changes from STOP to STARTUP mode
27	02:08:20.253	2012-01-31	수신 이벤트	Communication initiated request: STOP - CPU changes from RUN to STOP mode
28	00:41:09.227	2012-01-31	수신 이벤트	Follow-on operating mode change - CPU changes from STARTUP to RUN mode
29	00:41:09.165	2012-01-31	수신 이벤트	Follow-on operating mode change - CPU changes from STOP to STARTUP mode

세부사항: 15
Security event: Logon denied for Web server user 2

PLC_1
IPAddr: 192.168.22.201

[제어 H/W의 사용기록 저장 화면 확인 예시]

[Windows OS]

- 로깅 설정 및 로그 파일의 로깅 정보 확인
  - 제어판 > 관리 도구 > 로컬 보안 정책 > 보안 설정 > 로컬 정책 > 감사 정책
  - 계정 로그온 이벤트 감사 > “성공”, “실패” 설정
  - 권한 사용 감사 > “성공”, “실패” 설정

[Unix OS]

- #cat /etc/syslog.conf 파일에서 로그 설정 확인
  - #cat /var/adm/loginlog, authlog, sulog의 파일을 열어 로깅 정보 확인
- #vi /etc/syslog.conf 파일 설정 변경
- Unix 계열 운영체제의 생성 로그 종류
  - auth : 로그인 등의 인증 프로그램 유형이 발생한 메시지
  - authpriv : 개인인증을 요구하는 프로그램 유형이 발생한 메시지
  - cron : cron이나 at과 같은 프로그램이 발생하는 메시지
  - daemon : telnetd, ftpd 등과 같은 데몬이 발생한 메시지
  - kern : 커널이 발생한 메시지
  - lpr : 프린터 유형의 프로그램이 발생한 메시지
  - mail : 메일시스템에서 발생한 메시지
  - news : 유즈넷 뉴스 프로그램 유형이 발생한 메시지
  - syslog : syslog 프로그램 유형이 발생한 메시지
  - user : 사용자 프로세스
  - uucp : 시스템이 발생한 메시지
  - local0 : 여분으로 남겨둔 유형

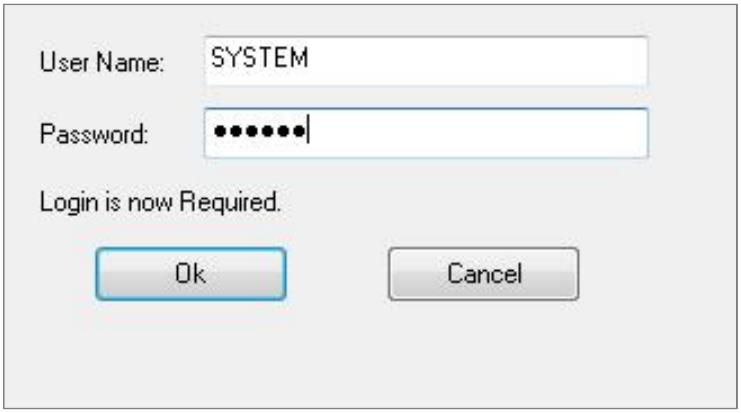
※ 조치 시, 시스템 운영 특성상 사용기록을 남기도록 변경할 수 없는 경우, 기기 운영기관에서 자체적으로 이에 대한 보완대책 수립

C-03 (상)	제어시스템 〉 1. 계정 관리
	제어시스템 계정입력 시 비밀번호 마스킹 처리, 입력값 에러 발생 시 제공 정보 제한 수행
개요	
점검 내용	인증과정에서 사용자가 입력하는 비밀번호의 노출을 방지하도록 마스킹 처리를 하고, 그 외 HMI 등의 제어시스템 입력창 중 문자열 입력이 가능한 경우 허용된 범위(예시: 문자 유형, 길이 등)의 값만 입력되도록 하고, 허용된 범위를 초과하는 비정상적인 값이 입력 시 오류 화면 등 발생 여부 점검
점검 목적	제어시스템 운영 중에 의도치 않은 실수로 비밀번호가 노출될 수 있으며 이를 방지하기 위해서 사용자가 입력하는 비밀번호가 노출되지 않도록 하고, 사용자의 입력에 대한 응답으로 제공되는 오류 메시지로 인해 공격자에게 제어시스템의 정보가 노출될 수 있어 이를 차단하기 위함
보안 위협	• 내부자가 자신보다 많은 권한을 가진 사용자가 입력하는 비밀번호를 획득하여 이를 이용하여 악의적인 목적으로 제어시스템 전체를 장악할 위험이 존재함 • 내부자가 HMI 등의 제어시스템 입력창에 비정상적인 값을 입력하여 그 결과 화면에 노출된 민감한 정보를 수집하여 악의적인 목적으로 사용할 위험이 존재함 • 해당 취약점이 알려져 있는 경우 이를 악용한 악성코드 감염을 통해 HMI 등의 제어시스템 권한을 이용한 제어설비 오동작 등의 피해가 발생할 위험이 존재함
참고	※ 본 취약점은 제어시스템을 개발, 납품하는 업체가 개발단계에서부터 보안 취약점이 최소화되도록 해야 하고, 운영단계에서 확인된 취약점이 있다면 제품을 이용하는 회사, 기관 등에 해당 취약점이 조치된 업데이트 및 보안패치를 배포되도록 하는 것이 바람직함
점검 대상 및 판단 기준	
대상	제어시스템 구성요소 전체
판단 기준	**양호** : 비밀번호 입력 시 마스킹 처리를 하고 있으며, 허용된 범위를 초과하는 값을 입력해도 불필요한 민감 정보 등이 노출되지 않는 경우
	취약 : 비밀번호 입력 시 비밀번호가 노출되고 있거나, 허용된 범위를 초과하는 값을 입력하는 경우 불필요한 정보가 노출되는 오류 화면이 나타나는 경우
조치 방법	비밀번호 입력 시 반드시 마스킹 처리를 하도록 하고, 모든 사용자 입력과정에서 허용된 범위의 값만이 입력되도록 하고 비정상적인 값이 입력되더라도 불필요한 정보가 노출되는 오류 화면 등이 나타나지 않도록 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 비밀번호 입력이 필요한 모든 제어시스템 구성요소에서 비밀번호 입력 시, 비밀번호가 마스킹 처리되고 있는지 확인



[비밀번호 마스킹 처리 예시]

Step 2) HMI 등의 소프트웨어에 운영자가 입력 가능한 입력창이 있는 경우, 해당 입력창에 다음 각 호와 같은 유형의 비정상적인 값을 입력했을 때 사전 정의된 결과(예시: 정상적인 값을 입력하도록 하는 경고 메시지 출력)가 나타나는지 확인

- 허용되는 문자 유형이 아닌 다른 문자 유형을 입력
  (예시: 숫자만 입력해야 하는 입력창에 문자나 특수문자를 입력)
- 허용되는 문자 길이를 초과하여 입력
  (예시: 보통 4개 문자만 입력하면 되나 8개 문자를 입력)
- DB 서버와 연동된 경우, DB Query 수준에 해당하는 문자열을 입력

Step 3) Step 2의 결과와 달리 비정상적인 에러 페이지가 나타나고 특히 해당 에러 페이지에 제어시스템에 관련된 주요 시스템 정보가 노출된다면 해당 소프트웨어의 설정을 변경하거나, 불가능한 경우 해당 구성요소의 개발업체와 협의하여 보완대책 마련

C-04 (중)	제어시스템 〉 1. 계정 관리
	제어시스템 계정을 관리, 운영, 유지보수 등 용도에 따라 분리하고 운용
개요	
점검 내용	제어시스템(HMI, DCS 등)에서 사용하고 있는 계정의 업무에 따른(관리, 운영, 유지보수 등) 분리 운용 여부 점검
점검 목적	제어시스템(HMI, DCS 등)에서 사용하고 있는 계정을 용도 별로 분리 사용하도록 하여 인가되지 않은 접근을 차단하고 책임추적이 가능하도록 하기 위함
보안 위협	용도에 따라 계정을 분리, 관리하지 않는 경우, 용도별 권한 분리가 불가능하여 권한 남용, 실수로 인한 기기의 오작동 발생할 수 있으며 사고 발생 시 사고 원인 파악 및 향후 예방 활동에 필수적인 사고 분석 제한의 위험이 존재함
참고	※ 본 점검항목은 제어시스템 계정은 관리 업무, 운영 업무, 유지보수 업무에 따라 서로 다른 계정을 사용하고 있는지 점검하는 것으로, 이는 용도별 권한을 분리하여 부여하기 위한 필수 항목임
점검 대상 및 판단 기준	
대상	제어시스템 운영 환경에서 계정 접근이 요구되는 전체 구성요소
판단 기준	**양호 :** 계정 기능을 사용하는 제어시스템 구성요소 전체에서 용도별로 계정을 분리하여 사용하고 있는 경우
	취약 : 계정 기능을 사용하는 제어시스템 구성요소 전체에서 용도별로 계정을 분리하지 않고 사용하고 있는 경우
조치 방법	계정 기능을 사용하는 제어시스템 구성요소에서 용도별로 계정을 분리하여 운영하도록 설정
조치 시 영향	일부 제어시스템 설정에 따라 접속 오류 발생 가능

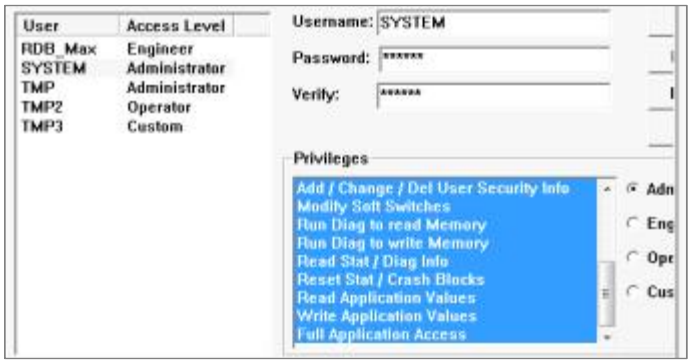
점검 및 조치 사례

● 공통

Step 1) 제어시스템 전체의 계정 목록을 확인하여 용도에 맞게 계정이 각각 분리되어 운영되고 있는지 확인

- 하나의 계정으로 서로 다른 업무를 가진 사용자가 동시에 사용하고 있는 경우, 서로 다른 계정을 사용하도록 조치
- 관리 용도, 운영 용도, 유지보수 용도에 따라 각각 계정을 다르게 부여하고 있어야 하며, 다만 점검 대상의 필요성, 또는 환경에 따라 해당 용도별 사용자가 없는 경우 분리되지 않은 경우도 예외로 허용 가능

※ PLC, DCS 등의 제어 H/W와 이를 운영하는 EWS, OWS와 같은 제어 S/W의 경우 제조사 별로 계정 기능의 관리, 확인 과정이 상이하므로 해당 제품의 매뉴얼을 통해 확인하거나 개발사에 문의하여 확인

C-05 (중)	제어시스템 〉 1. 계정 관리
	제어시스템 계정에 대해 관리, 운영, 유지보수 등 용도에 맞는 최소 권한 부여
개요	
점검 내용	제어시스템(HMI, DCS 등)에서 사용하고 있는 계정에 대해 용도에 맞는 최소 권한 부여 여부 점검
점검 목적	제어시스템(HMI, DCS 등)에서 사용하고 있는 계정을 용도별로 권한을 부여하여 불필요한 권한으로 발생하는 업무 사고를 차단할 수 있는지 점검하기 위함
보안 위협	용도에 따라 계정을 관리하지 않는 경우, 이를 통해 불필요한 권한을 할당받은 사용자가 악의적인 목적으로 제어시스템을 공격하거나, 잘못된 운전 조작 사고 등이 발생할 위험이 존재함
참고	※ 본 점검항목은 용도별 최소 권한 부여 여부를 점검하는 것으로, 용도별 계정을 분리 사용하고 있어야 함 ※ 제어시스템 기기에서는 계정 관리 기능에서 계정별 권한을 분리하여 할당할 수 있는 기능을 제공하고 있으며 이를 활용하여 용도별 권한을 분리하여 사용 가능함  [PLC의 계정 관리 화면 예시]
점검 대상 및 판단 기준	
대상	제어시스템 운영 환경에서 계정 접근이 요구되는 전체 구성요소
판단 기준	**양호 :** 계정에 따라 각 용도에 맞는 최소한의 권한을 부여하여 사용하고 있는 경우
	취약 : 계정에 따라 각 용도에 맞지 않는 권한이 부여되어 사용하고 있는 경우
조치 방법	계정의 용도에 따른 별도 권한 부여 설정
조치 시 영향	일부 제어시스템 설정에 따라 접속 오류 발생 가능

점검 및 조치 사례

● 공통

Step 1) 용도별 계정으로 기기에 접근하는 경우, 용도에 맞도록 권한이 분리되고 있는지 확인

- 관리 용도의 계정, 운영 용도의 계정, 유지보수 용도의 계정에 따라 각각 권한을 다르게 부여하고 있어야 하며, 다만 점검 대상의 필요성, 또는 환경에 따라 용도별 구분이 없는 경우 예외로 허용 가능

(예시: 관리자 1명이 운영을 동시에 하며 다른 사용자가 없는 경우)

C-06 (중)	제어시스템 〉 1. 계정 관리
	제어시스템 운전원별 유일 계정 부여 또는 시간별 사용자 기록 유지
개요	
점검 내용	제어시스템 운전원별로 다른 계정을 사용하거나 운전 시간에 따른 사용자(운전원) 기록 유지 여부 점검
점검 목적	제어시스템 운전원별로 다른 계정을 사용하거나 운전 시간에 따른 기록을 유지하도록 하여 계정 사용에 대한 책임 추적성(Accountability)을 높일 수 있도록 하기 위함
보안 위협	편의를 위해 다수의 운전원이 공용 계정을 사용하고, 시간별 사용자 기록이 존재하지 않는 경우 비밀번호 노출, 권한 남용, 사용자 책임추적 어려움 등의 우려가 있으며, 사고 발생 시 이에 대한 분석이 제한될 위험이 존재함
참고	※ **책임 추적성(Accountability)** : 정보시스템의 접속자, 접속시간, 접속 위치, 업무내역 등을 식별하여 장애 원인, 침해사고 경위 등을 조사하는 과정에서 책임을 규명할 수 있도록 하는 것을 의미
점검 대상 및 판단 기준	
대상	운전원이 접근하는 모든 제어시스템 구성요소
판단 기준	**양호** : 모든 운전원별로 다른 계정을 사용하거나 시간별 사용자 기록을 유지하고 있는 경우
	취약 : 운전원이 공용 계정을 사용하고 시간별 사용자 기록이 존재하지 않는 경우
조치 방법	모든 운전원별로 다른 계정을 사용하도록 계정 관리 또는 시간별 사용자 기록을 작성하도록 정책 변경 설정
조치 시 영향	일부 제어시스템 설정에 따라 접속 오류 발생 가능

점검 및 조치 사례

● 공통

Step 1) HMI, PLC 등의 제어 H/W, 제어 S/W에서 각 시스템 및 기기에 접근하기 위하여 사용하는 계정(ID) 목록과 각 계정을 사용하는 운영자 및 관리자 명단을 확인하여 유일한 계정을 사용하고 있는지 확인

※ PLC, DCS 등의 제어 H/W와 이를 운영하는 EWS, OWS와 같은 제어 S/W의 경우 제조사 별로 계정 기능의 관리, 확인 과정이 상이하므로 해당 제품의 매뉴얼을 통해 확인하거나 개발사에 문의하여 확인

[제어 S/W의 계정 관리 기능 예시]

Step 2) 제어시스템 내 정보시스템의 운영체제 계정(ID) 목록과 각 계정을 사용하는 인원의 명단을 확인(이 경우 다음 사항을 포함하여 점검)

- 공용 계정을 사용하는지 확인

[Windows OS]

- 운영자, 관리자별 계정 발급 확인
  - 시작 > 제어판 > 사용자 계정
- (개선조치 시) 제어시스템 운영자, 관리자별 계정 추가
  - 시작 > 제어판 > 사용자 계정 > 추가

[Unix OS]

- 운영자, 관리자별 계정 발급 확인
  - #cat /etc/passwd
- (개선조치 시) 제어시스템 운영자, 관리자별 계정 추가
  - #useradd 계정명

Step 3) Step 1, Step 2에서 공용 계정을 사용하고 있는 경우, 제어시스템을 운영하는 사용자의 시간별 사용기록을 남기는지 확인

Step 4) 사용기록은 사용자의 신원을 식별할 수 있는 방안을 포함하는지 확인
(예시: 근무자 표 작성 및 근무자 접근 단말 기록 등)

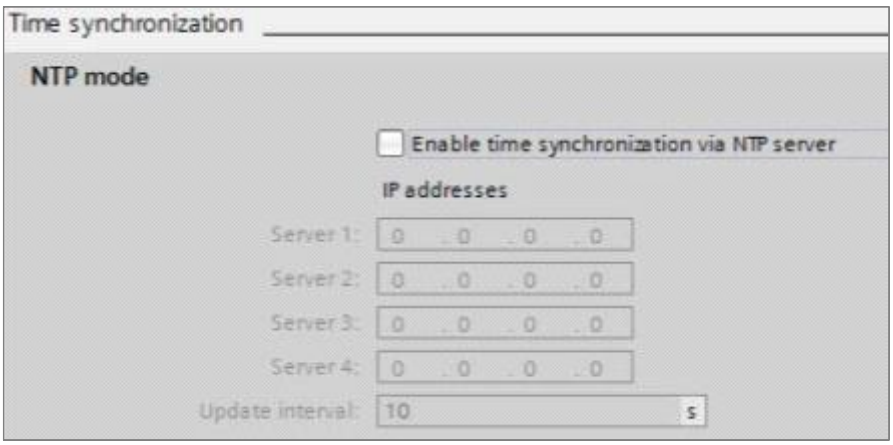
C-07 (상)	제어시스템 〉 2. 서비스 관리
	제어시스템 구성요소에 대한 시각 동기화 수행
개요	
점검 내용	제어시스템 구성요소들이 같은 시간을 유지할 수 있도록 하는 시각 동기화 기능의 제공 여부 점검
점검 목적	제어시스템에서 시각 동기화 기능을 제공하여 제어시스템 서비스의 안정성 유지와 사고 발생 시 이에 대한 로그 분석, 원인 파악 등이 가능한지 확인하기 위함
보안 위협	시각 동기화가 이루어지지 않는 경우, 구성요소 간 주고받는 제어 명령의 안정성에 문제가 발생할 수 있으며 제어시스템의 로그 분석이 어려워 이로 인해 공격자가 발각되지 않고 공격 기법을 숨기는 등의 위험이 존재함
참고	※ 제어 H/W 등의 일부 구성요소에서 시간 동기화 기능이 NTP 또는 PTP와 같은 프로토콜을 이용하지 않으나 상시 연결되어있는 EWS 또는 OWS 등의 다른 구성요소와 시간 동기화를 수행하고 있고, 해당 구성요소가 운영체제 등을 통해 정상적으로 시간 동기화를 수행하고 있는 경우 정상적으로 시간 동기화를 수행하는 것으로 볼 수 있음 ※ 정확한 시간 동기화를 위해서는 GPS 서버를 구축하여 시간 동기화에 활용할 수 있으며 이를 권장 [시각 동기화를 위한 GPS 서버 구축 예시]
점검 대상 및 판단 기준	
대상	모든 제어시스템 구성요소
판단 기준	**양호** : 모든 제어시스템 구성요소에서 NTP 또는 PTP 등의 시각 동기화 기능을 제공하고 있고, 설정되어 운용되고 있는 경우
	취약 : 제어시스템 구성요소 중에서 시각 동기화 기능이 존재하지 않거나, 시각 동기화 설정이 정상적으로 이루어지지 않은 경우
조치 방법	시각 동기화 기능이 존재하지 않는 경우 이에 대한 보완대책을 마련하고, 모든 제어시스템 구성요소들이 같은 시간 정보를 이용할 수 있도록 시간 동기화 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

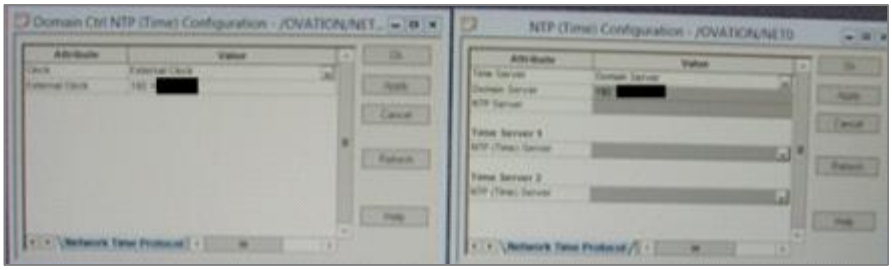
● 공통

Step 1) 제어시스템 구성요소에서 시각 동기화 기능을 제공하고 있는지 확인

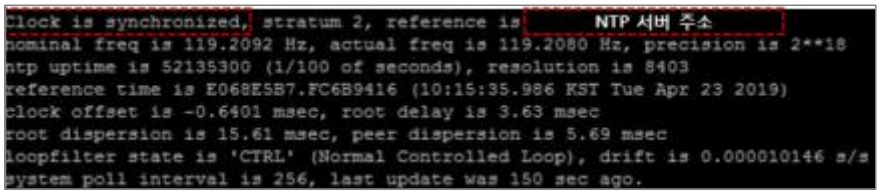
(예시: 제어 H/W, 제어 S/W, 네트워크 장비, 정보시스템의 NTP 서버 설정 화면)



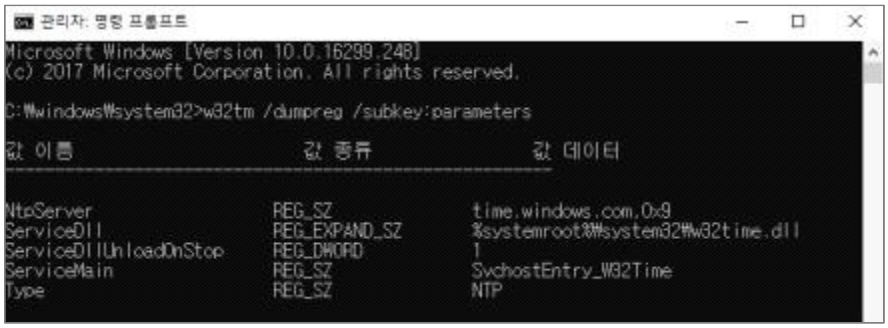
[제어 H/W의 NTP 서버 설정 화면 예시]



[제어 S/W의 NTP 서버 설정 화면 예시]



[네트워크 장비의 NTP 서버 설정 화면 예시]



[정보시스템의 NTP 서버 설정 화면 예시]

※ Cisco 스위치의 경우 'sh ntp status' 명령어로 확인 가능

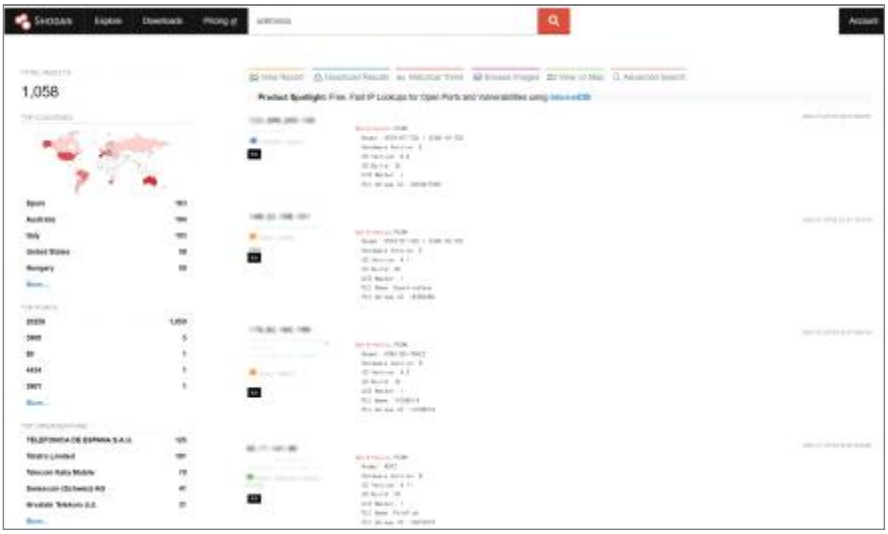
※ Microsoft Windows 제품의 경우 명령 프롬프트에서 ‘w32tm /dumpreg /subkey:parameters’ 명령어로 확인 가능

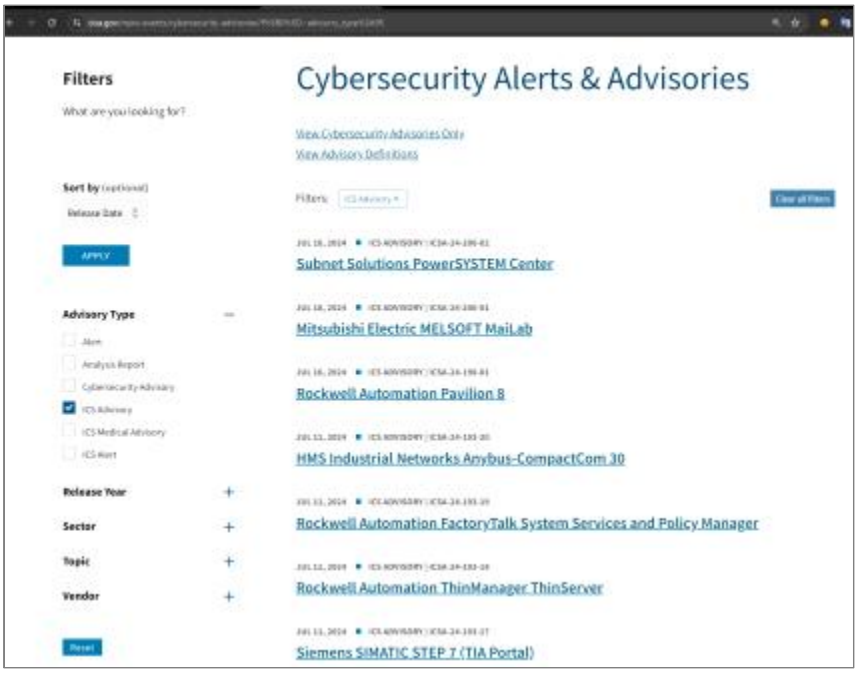
Step 2) 확인된 시각 동기화 기능에서 설정이 정상적으로 적용되어 실제 시간 동기화가 수행되고 있는지 확인

- Step 1)의 설정 화면에서 제어시스템 구성요소들이 같은 NTP 서버를 설정하고 있는지 확인
- 실제 복수의 제어시스템 구성요소의 시각 정보를 확인하여 같은지 확인

※ 제어시스템 구성 특성상 독립적으로 분리된 여러 네트워크를 운용 중인 경우, 네트워크별 GPS 서버를 구축하여 시각 동기화를 수행할 것을 권장하며, 제한될 경우, 일방향 전송 장치 등을 통해 네트워크 독립성을 유지한 상태에서 시간 동기화를 수행할 것을 권장

※ 제어시스템 구성요소에서 시간 동기화 기능을 제공하지 않는 경우, 이에 대한 보완대책의 예시로 주기적인 수동 시각 점검 및 설정하도록 하는 정책 수립 등의 방안이 있으며 이 경우 해당 정책 및 시행 여부에 대한 점검도 수행할 것을 권고

C-08 (상)	제어시스템 〉 2. 서비스 관리
	제어시스템에 불필요한 서비스 및 취약한 서비스 제거 또는 보완대책 수행
개요	
점검 내용	제어시스템 구성요소에서 불필요한 서비스와 취약한 서비스를 제거하거나 이용할 수 없도록 비활성화 여부 점검
점검 목적	제어시스템(운영체제)에 관련 소프트웨어를 위해 필요한 최소한의 서비스만 활성화하고 취약한 서비스를 제거 또는 비활성화하여 비인가자 및 악성코드에 의해 취약한 서비스 악용이 일어나지 않도록 하기 위함
보안 위협	• 불필요하거나 취약한 서비스가 활성화되어 있는 경우 공격자가 네트워크 스캐닝을 통해 취약한 서비스를 찾아내, 비인가자 접근, 악성코드 유포 등 해당 서비스를 악용한 해킹의 위험이 존재함 • **위협 사례:** SMB Redirect(Redirect To SMB) 공격의 경우, Windows PC 간에 파일 공유를 위해 사용하는 SMB(Server Message Block) 프로토콜을 악용하여, 해당 네트워크 트래픽을 해커가 장악한 SMB 서버 또는 악성 웹사이트로 우회시킬 수 있는 취약점을 이용함. 이를 통해 해커는 Windows PC 사용자들의 해당 로그인 정보를 탈취할 수 있으며 이와 같은 공격에 대한 최선의 보안대책은 TCP 139와 445 포트를 차단하여 SMB 프로토콜 자체를 이용하지 못하도록 함
참고	※ **제어시스템 취약점 검색엔진:** 쇼단(https://www.shodan.io)과 같은 웹사이트(Criminal IP)는 IoT, ICS 등과 같은 설비에 대해 국가, 기관, 서비스(Port), IP주소 등의 검색어 입력만으로 어떤 서비스가 활성화되어 있고 인터넷상으로 접근 가능한지 검색 가능  [쇼단 홈페이지에서 검색어(예: 제어기기 모델)를 통해 확인한 결과] ※ **제어시스템 취약점 목록 제공:** 미국 국토안보부(DHS) 산하 CISA(CyberSecurity & Infrastructure) 홈페이지(https://cisa.gov/news-events/cybersecurity-advisories)에서는 ICS에서 발견된 최신 취약점 목록을 제공하고 있어, 사용 중인 제어시스템 구성요소에 취약점 존재 여부를 확인할 수 있음



[CISA 홈페이지에서 제공하는 ICS 취약점 목록]

점검 대상 및 판단 기준	
대상	HMI, EWS와 같은 제어 S/W를 제외한 제어시스템 구성요소 전체
판단 기준	**양호** : 제어시스템에 불필요하거나 취약한 서비스가 제거 또는 비활성화된 경우
	취약 : 제어시스템에 불필요하거나 취약한 서비스가 활성화된 경우
조치 방법	제어시스템에 불필요하거나 취약한 서비스를 제거 또는 비활성화 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 현황(목록)과 네트워크 구성도를 확인하고 제어시스템별 감시, 설비제어 등을 위해 필요한 서비스(Port) 종류 확인

Step 2) 구성요소 운영체제의 방화벽 기능 또는 자체적으로 활성화된 서비스 조회 기능 등을 통해 해당 구성요소에 활성화된 서비스(Port)가 불필요한 것인지 또는 취약한 것인지 점검

Step 3) Step 2)에서 확인된 불필요하거나 취약한 서비스에 대해 보안대책 적용 여부 확인

- 보완대책으로는 제어망, 업무망의 방화벽에서 접근통제 정책으로 해당 서비스를 차단하고 있는 경우 또는 네트워크 장비의 접근규칙(ACL)을 적용하여 차단하고 있는 경우 존재
- 불필요하거나 취약한 서비스가 제거 또는 보완대책 적용이 되어있지 않은 경우, 이를 비활성화하거나 보완대책을 적용하도록 조치

[Windows OS]

- 시작 옵션에서 시작유형을 “사용 안 함”으로 설정
- 시작 > 설정 > 제어판 > 관리 도구 > 서비스에서 불필요한 서비스 중지
- 시작 > 설정 > 제어판 > 방화벽 설정에서 접근 가능한 IP 제한

[Unix OS]

- # vi /etc/inetd.conf 파일에서 불필요한 서비스 주석(#) 처리하여, 해당 서비스 비활성화
- # /etc/hosts.allow에 접근 가능한 서비스, IP 지정
- # /etc/hosts.deny에서 차단하고자 하는 서비스, IP 지정

▪ SMB(Session Message Block) 프로토콜은 Windows에서 디스크와 프린터를 네트워크상에서 공유하는 데 사용되며, TCP 139번, 445번 포트를 사용함. SMB를 비활성화하려면 다음과 같은 방법으로 TCP/IP에서 SMB를 언바인드 시킴

바탕화면 또는 제어판에서 [네트워크 환경]의 [등록정보] 실행

현재 인터넷에 접속된 연결의 [등록정보] 선택

[Microsoft 네트워크용 클라이언트] 항목과 [Microsoft 네트워크용 파일 및 프린터 공유] 항목의 체크 해제

C-09 (중)	제어시스템 〉 2. 서비스 관리
	제어시스템 구성요소에 대한 관리자 페이지 운영 시 이에 대한 접근통제(사전인가 접근만 허용) 수행

개요	
점검 내용	제어시스템 구성요소의 관리 페이지에 접근하는 관리자에 대해 사전에 인가된 접근만 가능하도록 접근통제 수행 여부 점검
점검 목적	제어시스템 구성요소를 관리하는 관리 페이지에는 사전에 인가된 관리자만 접근하도록 하여 인가되지 않거나 악의적인 접근을 차단하기 위함
보안 위협	업무를 수행하는데 권한이 없는 사용자가 악의적인 목적으로 관리자 페이지에 접근하여 권한 획득, 인증 우회 등의 공격을 시도하여 해당 장비를 장악할 위험이 존재함
참고	※ **관리자 페이지에 대한 접근통제(사전인가 접근만 허용)** 일반적으로 활용하는 기법은 관리자가 접근할 수 있는 IP주소, MAC 주소 등을 사전에 인가하여 인가되지 않은 IP주소, MAC 주소 등을 통한 접근 시, 이를 차단하도록 하는 기법임 access-list 10 permit 19[redacted]0 log access-list 10 permit 192.168.2.217 log access-list 10 deny any log line vty 0 4 access-class 10 in [네트워크 장비에서 관리자 접근을 특정 IP로 제한 예시] [제어 S/W에서 관리자 접근을 특정 IP로 제한 예시] ※ 관리자 페이지 접근 시, 네트워크를 이용한 모든 접근을 차단하고 있으며 물리적으로 접근하는 콘솔 접근만 허용하고 있는 경우 양호하다고 판단 가능

점검 대상 및 판단 기준	
대상	관리자 페이지가 존재하는 모든 제어시스템 구성요소 및 제어시스템을 구성하는 네트워크 전체
판단 기준	**양호 :** 관리자 페이지에 IP주소, MAC 주소 등을 통해 사전인가된 관리자만 접근이 가능한 경우
	취약 : 모든 사용자가 관리자 페이지에 접근이 가능한 경우
조치 방법	제어시스템 구성요소의 관리자 페이지에 사전 인가된 접근만 가능하도록(IP주소 등) 설정
조치 시 영향	일부 제어시스템 설정에 따라 접속 오류 발생 가능

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소 현황(목록)을 확인하고 관리자 페이지가 존재하는 구성요소를 식별하여 해당 구성요소에 대해, 관리자 페이지 접근 방법 및 사전인가된 접근만 가능하도록 설정되어 있는지 확인

- 물리적인 접근(기기 콘솔 포트를 이용한 접근 등)만 허용하고 있으며, 그 외 관리자 페이지 접근이 불가능한 구성요소의 경우 제외

Step 2) Step 1)에서 사전 인가되지 않은 방법으로 관리자 페이지에 접근 시도
(예시: 설정되지 않은 IP주소의 기기로 접근 등)

- 관리자 페이지가 나타날 경우, 해당 구성요소에서 접근할 수 없도록 설정 변경을 통한 조치 수행

※ 제어시스템 구성요소에서 사전에 인가된 관리자만 접근할 수 있도록 설정할 수 없는 경우, 방화벽, 네트워크 장비, 서버 등에 적용 가능한 접근통제 규칙 변경을 통해 지정된 관리자 IP만 접근할 수 있도록 설정할 수 있음

C-10 (중)	제어시스템 〉 2. 서비스 관리
	제어시스템 내 파일/디렉터리 접근 권한 및 신뢰 관계를 적절히 부여
개요	
점검 내용	제어시스템 내 구성요소에서 적절한 파일/디렉터리 접근 권한 및 신뢰 관계 부여 여부 점검
점검 목적	제어시스템 운영을 위해 파일/디렉터리 접근 권한 및 신뢰 관계를 과다하게 부여하여 인가되지 않은 사용자가 허용되지 않은 파일, 정보에 접근하는 것을 차단하기 위함
보안 위협	제어시스템과 관련된 중요 자료(도면 등)에 대해 접근 권한을 과다하게 부여하여 인가되지 않은 사용자가 해당 정보를 취득하여 외부에 공개하거나 공격을 위한 기초자료로 활용될 위험이 존재함
참고	※ 제어시스템 운영을 위해 공유 폴더 사용 시 볼륨 전체를 공유하거나 모든 사용자 계정이 읽기·쓰기·실행 권한을 가지는 등의 설정은 파일 및 디렉터리 접근 권한 과다 부여에 해당함 ※ 과다한 신뢰관계란 통합인증(Single Sign-on), SSH Key의 트러스트 설정 등을 통해 제어시스템 구성요소 간 인증 없이 접근이 가능한 경우를 의미 ※ 필요 이상의 다중 로그인을 허용, 세션 간 로그인 정보를 지속적으로 유지, 비밀번호 저장을 통한 자동 로그인 등 역시 과다한 신뢰 관계에 해당함
점검 대상 및 판단 기준	
대상	제어시스템 내 구성요소
판단 기준	**양호 :** 제어시스템 내 파일/디렉터리에 접근 권한 및 신뢰 관계를 과다하게 부여하지 않은 경우
	취약 : 제어시스템 내 파일/디렉터리에 접근 권한 및 신뢰 관계를 과다하게 부여한 경우
조치 방법	제어시스템 내 파일/디렉터리에 접근 권한 및 신뢰 관계를 허용할 경우, 반드시 필요한 때에만 설정하도록 하고, 반드시 필요한 특정 위치의 특정 사용자에게만 허용하도록 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 내 구성요소에서 파일/디렉터리 접근 권한 설정을 확인

[Windows OS]

(1) 실행 창에서 fsmgmt.msc를 입력한 후 확인 버튼을 클릭

[실행 창]

(2) 공유 폴더 ‣ 공유 폴더(로컬) ‣ 공유에서 설정 확인하여 기본 공유 설정된 드라이브 또는 IPC가 존재하지 않는지 확인

[공유 폴더]

(3) 내 컴퓨터 > 로컬디스크 속성 > 공유 > 네트워크 파일 및 폴더 공유에서 확인하여 네트워크 파일 및 폴더 공유가 사용되고 있지 않은지 확인

[로컬디스크 속성]

※ 해당 기기에서 설정 변경이 불가능할 경우, 제어시스템 개발업체와 협의하여 이에 대한 보완대책 마련 권고

C-11 (중)	제어시스템 〉 2. 서비스 관리
	제어시스템 내 제어와 직접적인 관련이 없는 불필요 프로그램 삭제
개요	
점검 내용	제어시스템 내 구성요소에 설치된 프로그램 중 제어시스템 운영과 관련이 없는 불필요한 프로그램의 삭제 여부 점검
점검 목적	제어시스템 내 구성요소에 불필요한 프로그램이 설치되어 예상하지 못한 취약점이 발생하거나 제어시스템의 가용성을 저해시킬 수 있어 안정적인 제어시스템 운영을 하기 위함
보안 위협	제어시스템 내 구성요소에 설치된 불필요한 특정 프로그램에서 발견된 취약점으로 인해 해당 정보시스템이 오동작을 일으키거나, 다른 공격에 활용될 위험이 존재함
참고	※ 제어시스템 운영과 관련 없는 불필요한 프로그램의 예시로는 게임, 인스턴트 메신저, 사용하지 않는 문서편집 및 뷰어 프로그램, 개발용이 아닌 시스템에서 사용하지 않는 컴파일러, DB, 설정 파일 등이 있을 수 있음
점검 대상 및 판단 기준	
대상	제어시스템 내 구성요소
판단 기준	**양호 :** 제어시스템 내 구성요소에 운영에 필요하지 않은 프로그램이 존재하지 않는 경우
	취약 : 제어시스템 내 구성요소에 운영에 필요하지 않은 프로그램이 존재하는 경우
조치 방법	제어시스템 운영에 불필요한 프로그램을 삭제하도록 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 내 구성요소의 설치된 프로그램 목록을 확인하여 불필요한 프로그램 유제어시스템 운영에 필요한 프로그램은 제어시스템 공급사, 운영사가 확인하여 관리하는 것을 권고하며, 이러한 목록에 없는 프로그램은 모두 삭제하도록 조치

C-12 (중)	제어시스템 〉 2. 서비스 관리
	제어시스템 운영 정보, 제어 명령 등 중요 정보에 대한 위변조 및 replay 공격 방지 대책 적용
개요	
점검 내용	HMI, PLC 등을 통해 제어설비에 전송되는 제어 명령이 스니핑(임의 지정) 등의 패킷 감청 등으로 중간에 해당 패킷을 가로채 위변조할 수 없도록 하고, 해당 패킷 재사용을 통한 제어설비 전송, 조작 여부 점검
점검 목적	제어 명령이 비인가자에게 노출되거나 중간에서 가로챌 수 없도록 하고, 이를 재사용할 수 없도록 하여 안정적인 제어시스템을 운영하기 위함
보안 위협	• 제어시스템을 구성하는 HMI, PLC 등의 제어 H/W, 제어 S/W에서 보안이 고려되지 않은 프로토콜을 이용하는 시스템에 따라서는 제어 명령을 가로챌 수 있는 취약점이 공개되어 있어 해당 취약점으로 인한 공격이 성공하는 경우 비인가자가 제어설비의 운영 권한을 획득할 위험이 존재함 • **취약점 예시:** '20. 1. 14. 공개된 취약점으로 GE사의 PACSystems RX3i 제품군에서 조작된 패킷이 전달되면 모듈 상태가 중지 모드로 변경되어 서비스거부가 발생하는 취약점이 발견됨 (ICSA-20-014-01)(CVE-2019-13524)
참고	※ **무결성 체크:** 데이터의 무결성을 확인하기 위해 SHA-256 등의 해시 함수를 이용하여 데이터가 최초 원본 상태와 다른 변형된 것이지 확인 ※ **Replay 공격:** 네트워크상의 정보 프레임을 수집한 뒤 해당 메시지를 재전송함으로써 갱신되지 않은 정보의 전달이나, 대상 장비에게 정당한 정보 전송으로 인식시켜 오류를 유도하는 공격 기법으로, HMI 서버와 RTU 사이의 통신선로에 인가되지 않은 해킹 기기를 접속시켜 각각 HMI 서버와 RTU에 해당 공격을 수행 가능
점검 대상 및 판단 기준	
대상	운영 정보 등 중요 정보를 다루는 제어시스템 구성요소
판단 기준	**양호 :** 제어 명령을 암호화 전송하거나 송수신 정보의 무결성을 확인(위·변조 여부 확인)하고, 재사용 방지(인증, 시간 확인, 세션 확인 등) 과정을 거치도록 하는 경우
	취약 : 제어 명령이 암호화되지 않고 평문 전송되거나, 송수신 정보의 무결성을 확인하지 않거나, 재사용 방지(인증, 시간 확인, 세션 확인 등) 과정을 거치지 않는 경우
조치 방법	전송되는 정보를 암호화하거나 무결성을 점검할 수 있도록 하고 재사용을 방지할 수 있도록 설정 변경하거나 불가능할 경우, 제조사와 협의하여 보완대책 마련
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

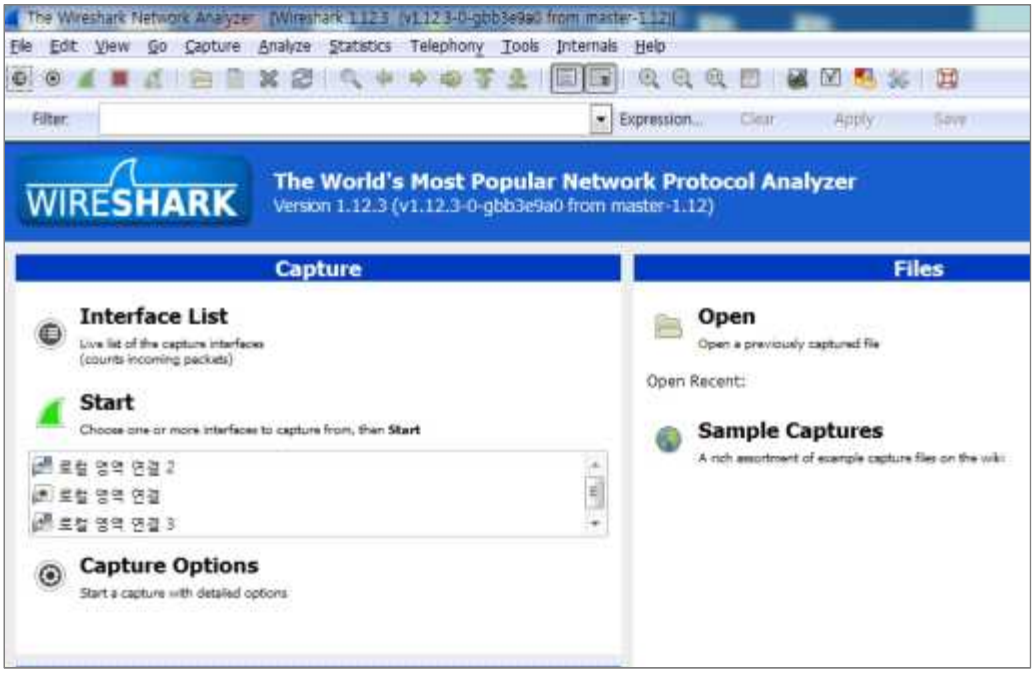
● 공통

Step 1) 전송되는 제어 명령을 스니핑(Sniffing)하여 암호화 송수신이 이루어지는지 확인하고 암호화가

필요함에도 평문 전송이 이루어지고 있다면 암호화 전송되도록 송수신 장비의 설정 변경

Step 2) 제어 명령을 수신 및 송신하는 경로의 네트워크 장비에 트래픽 수집 도구 또는 제어 명령을 수신하는 서버나 PC에서 스니핑 도구를 설치, 이용하여 전송되는 데이터가 암호화되는지 점검

※ 스니핑 도구가 설치된 시스템의 LAN 카드를 지정하면 해당 LAN 카드를 통해 송수신되는 데이터 패킷을 캡쳐하여 문자열이 평문인지 또는 암호화된 것인지 확인할 수 있음



[WirkShark을 설치, 실행한 화면]

Step 3) 제어 명령을 송수신하는 서버 및 PC 등이 전송된 데이터가 원본과 일치하는지를 확인하는 무결성 체크 과정을 거치는지 점검하고 무결성 체크 없이 송수신된다면(별도 전송 장비를 사용하는 경우) 송수신 장비의 설정을 변경하거나 이에 대한 자체적인 보완대책 수립

Step 4) 해당 항목 점검방법은 송수신되는 데이터를 조작하여 발송한 뒤 무결성 점검 없이 정상 수신되는지를 확인하는 방식으로 이루어져야 하나, 점검 환경의 제약이 따르는 경우는 대상 제어시스템의 개발, 운용 확인

C-13 (하)	제어시스템 〉 2. 서비스 관리
	제어시스템 내 전달되는 제어 명령 및 파라미터의 정상 범위를 식별하고 관리
개요	
점검 내용	제어시스템을 통해 설비에 전달되는 제어 명령의 문자열이 운영 목적에 맞는 최소 권한으로 전달되도록 불필요한 파라미터 사용 제한 여부 점검
점검 목적	제어시스템 감시 및 제어를 위한 HMI, PLC 등의 소프트웨어는 제어시스템의 운전정보를 조회하고 제어할 수 있으므로 제어 명령 제한과 파라미터값의 범위를 제한하여 운영자의 부주의(Human Error), 오·남용 및 악성코드에 의한 악의적인 운전 명령 전달 등을 차단하기 위함
보안 위협	• 정상 범위를 초과하는 제어 명령 값을 부여할 수 있다면 부주의(Human Error), 오·남용이 발생할 수 있고 특히 악성코드에 의한 악의적인 운전 명령 및 과도한 파라미터 값 전달을 통해 제어설비의 오작동 등의 피해가 발생할 수 있음 • **위협 사례:** 스턱스넷은 PLC 시스템의 Profibus 메시지 버스 시스템을 감시하는 D8890 블록에 악성코드를 설치하여 특정 조건을 만족하면, 주기적으로 모터의 회전수를 1410Hz, 2Hz, 1064Hz로 변경해 모터에 과부하를 일으킴 또한 PLC 시스템에 루트킷을 설치하여 자기 자신을 숨기고, 모터의 회전수가 변경되고 있다는 것을 숨김
참고	※ HMI, PLC 등의 소프트웨어를 통해 사용 가능한 제어 명령, 파라미터값의 범위 등을 사전에 제한하여 운영자 권한 또는 악성코드에 의해 불필요한 제어 명령과 파라미터값 전송이 일어나지 않도록 제어시스템의 환경설정 강화 필요
점검 대상 및 판단 기준	
대상	HMI, PLC 등의 제어 S/W
판단 기준	**양호 :** 운영 업무 목적에 필요한 최소한의 제어 명령과 파라미터만을 사용하도록 제한하는 경우
	취약 : 운영 업무 범위를 초과하는 제어 명령과 파라미터의 사용 제한이 없는 경우
조치 방법	운영 목적에 맞는 최소한의 제어 명령과 파라미터만을 사용하도록 HMI, PLC 등의 관리설정 강화 (제어 명령 권한 조정)
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) HMI, PLC 등을 통해 사용 가능한 제어명령어와 제어 명령 별 파라미터 등을 확인

Step 2) 확인한 결과, 운영자가 제한 없이 제어 명령 및 파라미터 사용이 가능하다면 HMI, PLC 등의 제어 S/W에서 업무 목적에 필요한 제어 명령과 파라미터 범위만을 사용할 수 있도록 제한하는 설정 조치

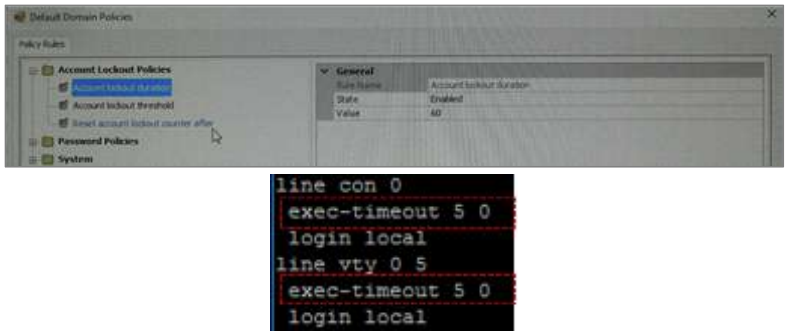
※ 일반적으로 HMI, PLC 설정 변경으로 취약점을 조치할 수 있으나, 개발업체의 환경, 협조 여부에 따라 조치가 어려울 수 있으며, 해당 경우 자체적으로 보완대책 마련 필요

C-14 (하)	제어시스템 〉 2. 서비스 관리
	제어시스템 내 사용자 통신 세션에 대해 세션 타임아웃 적용
개요	
점검 내용	세션 통신을 지원하는 제어시스템 구성요소의 합리적인 시간 범위 내에 세션 타임아웃 설정 운용 여부 점검
점검 목적	제어시스템 구성요소가 세션 통신을 수행하고 있을 때, 일정 시간 동안 입력이 없는 경우 세션을 종료하도록 하여 해당 세션을 가로채어 발생할 수 있는 위협으로부터 제어시스템을 보호하기 위함
보안 위협	관리자가 로그인 후, 세션을 종료하지 않고 자리를 비우는 동안 악의적인 사용자가 접속된 터미널을 이용하여 불법적인 행위를 시도할 위험이 존재함
참고	-
점검 대상 및 판단 기준	
대상	사용자와 세션 통신을 지원하는 제어시스템 구성요소
판단 기준	**양호 :** 사용자 통신 세션 구간에서 타임아웃 기능이 설정된 경우
	취약 : 사용자 통신 세션 구간에서 타임아웃 기능이 설정되지 않은 경우
조치 방법	사용자 통신 세션 구간에서 일정 시간 입력이 없는 경우 자동으로 세션을 종료하는 세션 타임아웃 기능 설정 또는 개발변경
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 점검 대상 장비에서 허용하는 세션 통신을 모두 식별하고, 식별된 세션에서 타임아웃 기능 설정 여부 확인



[타임아웃 설정 화면 예시]

Step 2) Step 1)에서 확인된 설정과 같이 실제로 타임아웃이 이루어지는지 확인

C-15 (하)	제어시스템 〉 2. 서비스 관리
	GPS 스푸핑/재밍 공격 등 시간 동기화 서비스를 교란하기 위한 공격에 대비한 보안 조치 수행
개요	
점검 내용	제어시스템에 구축한 시간 동기화 시스템이 GPS 스푸핑/재밍 공격 등에 대응하는 기능 존재 여부 점검
점검 목적	제어시스템 구성요소들이 같은 시간을 유지할 수 있도록 구축한 시간 동기화 시스템이 GPS 스푸핑/재밍 공격 등에도 같은 시간 정보를 유지하기 위함
보안 위협	GPS 스푸핑/재밍 공격은 제어시스템 구성요소의 시간 정보를 동일하게 유지시키는 NTP의 이상 동작을 발생시키고 이로 인해 제어시스템의 안정성이 저해될 위험이 존재함
참고	※ 일부 NTP/PTP 솔루션에서는 최근 발생하는 GPS 재밍, 스푸핑 공격에 대비하여 이에 대응하는 기능을 가진 제품을 판매하고 있음
점검 대상 및 판단 기준	
대상	GPS 신호를 수신하는 안테나와 이를 사용하는 NTP 서버
판단 기준	**양호 :** GPS 스푸핑/재밍 공격 등 시간 동기화 교란 공격에 대비한 대책이 마련되어 있는 경우
	취약 : GPS 스푸핑/재밍 공격 등 시간 동기화 교란 공격에 대비한 대책이 마련되지 않은 경우
조치 방법	시간 동기화 교란 공격에 대비하여 고정밀 오실레이터(예시: 세슘, 루비듐 등)를 보유한 백업용 시각장치 구비 또는 공격 차단을 위한 능동형 안테나 설치 등의 대책을 적용
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 내 NTP 서버를 구축하고 GPS 신호를 이용한 시간 정보 수신 여부를 확인

Step 2) Step 1)에서 확인된 NTP 서버가 GPS 스푸핑/재밍 공격에 대응하는 기술이 적용되어 있는지 확인

- 세슘, 루비듐 등의 고정밀 오실레이터 내장된 백업 시각 유지 장치 등의 자체 대응 기술 여부 확인
- 대응하는 기술이 적용되어 있지 않은 경우, 고정밀 오실레이터를 보유한 백업용 시각장치 구비 또는 공격 차단을 위한 능동형 안테나 설치 등의 조치 수행

C-16 (상)	제어시스템 〉 2. 서비스 관리
	제어시스템에 대한 최신 업데이트, 보안패치를 안전하게 적용하기 위한 제조사 협력방안, 테스트 방안 등의 절차 수립
개요	
점검 내용	제어시스템을 구성하는 소프트웨어, 시스템(OS), 장비 등에 대한 최신 업데이트, 보안패치를 적용할 수 있는 절차 수립 여부 점검
점검 목적	최신 발견된 보안취약점에 대해 이를 조치할 수 있는 업무절차가 수립되어 있는지 점검하여 향후 새로운 보안취약점이 발견되었을 때 대응할 수 있는지 확인하기 위함
보안 위협	알려진 취약점이 존재하는 제어시스템을 대상으로 해당 취약점을 악용한 비인가자의 침해 시도 또는 자동화된 악성코드의 감염 위험이 존재함
참고	※ 본 점검항목에서는 제어시스템의 업데이트, 보안패치를 안전하게 수행할 수 있는 절차에 대한 상세 점검항목이며, 취약점의 존재 유무에 대한 점검항목은 C-08 항목을 참고 ※ 일반적인 IT 환경과 달리 제어시스템의 경우, 높은 가용성을 요구하는 특징에 따라 최신 업데이트 및 보안 패치가 신속하게 이루어지지 않는 경우가 있으며 이러한 경우 업데이트 및 보안 패치가 이루어질 때까지 발생할 수 있는 위협을 완화할 수 있는 방안 적용을 권고함
점검 대상 및 판단 기준	
대상	전체 제어시스템 구성요소
판단 기준	**양호 :** 제어시스템 업데이트 및 보안패치 적용 절차가 수립된 경우
	취약 : 제어시스템 업데이트 및 보안패치 적용 절차가 수립되지 않은 경우
조치 방법	제어시스템 구성요소가 안전하게 업데이트 및 보안패치를 수행할 수 있도록 하는 절차 수립
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소의 납품 계약 문서, 기타 유지보수 계약 문서 등을 통해 업데이트 및 보안패치 적용 방안이 수립되어 있는지 확인

Step 2) 수립된 보안패치 적용 방안에 따라 제어시스템 구성요소의 업데이트 및 보안패치가 가능한지 확인

C-17 (상)	제어시스템 〉 3. 패치 관리
	외부 업체, 인터넷을 통한 다운로드 등의 경로로 반입된 각종 패치·업데이트 파일에 대해 무결성 검증 및 클린 PC를 통한 악성코드 존재 여부 검사 수행
개요	
점검 내용	외부 업체, 인터넷 등을 통해 다운로드 등의 경로로 제어망 내부에 반입되는 각종 패치, 업데이트 파일에 대해 무결성 검증 및 악성코드 검사 수행 여부 점검
점검 목적	제어망 내부로 악성코드 유입을 차단하기 위해 패치, 업데이트 수단을 안전하게 보호하기 위함
보안 위협	• 악성코드를 은밀히 유포하기 위해 업데이트 서버나 협력업체 서버, 노트북 등에 침투하여 업데이트 파일로 위장하는 사례가 있음 • **위협 사례:** '19. 3. 25. Kaspersky Lab에서 발표한 "Operation Shadow Hammer"는 ASUS의 소프트웨어 업데이트 서버가 해킹되어 대부분의 ASUS 컴퓨터에 설치된 Asus Live Update가 추가적인 악성코드를 받을 수 있는 경로로 백도어가 포함된 버전으로 업데이트되도록 하는 공격임
참고	※ 최근 사이버 공격에 자주 활용되는 공급망 공격(Supply Chain Attack)은 직접 침투가 어려운 시설에 악성코드를 감염시키기 위해 공격 대상 시설이 사용하는 소프트웨어, 하드웨어 업체를 활용하는 공격으로, 이러한 공격 기법의 하나로 제공하는 패치, 업데이트 파일에 악성코드를 숨겨 대상 시설에 악성코드를 설치하도록 유도할 수 있음
점검 대상 및 판단 기준	
대상	업데이트 또는 패치를 위해 제어망 내 반입되는 모든 외부 파일
판단 기준	**양호 :** 제어망 내 반입되는 패치·업데이트 파일의 무결성 검증 및 악성코드 검사가 수행되는 경우
	취약 : 제어망 내 반입되는 패치·업데이트 파일의 무결성 검증 및 악성코드 검사가 이루어지지 않은 경우
조치 방법	제어망 내 반입되는 패치·업데이트 파일을 제공하는 공급사로부터 무결성을 확인받는 절차를 도입 및 악성코드를 검사할 수 있는 클린 PC를 구축하여 해당 파일의 악성코드 존재 유무 확인 후 제어시스템 설치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

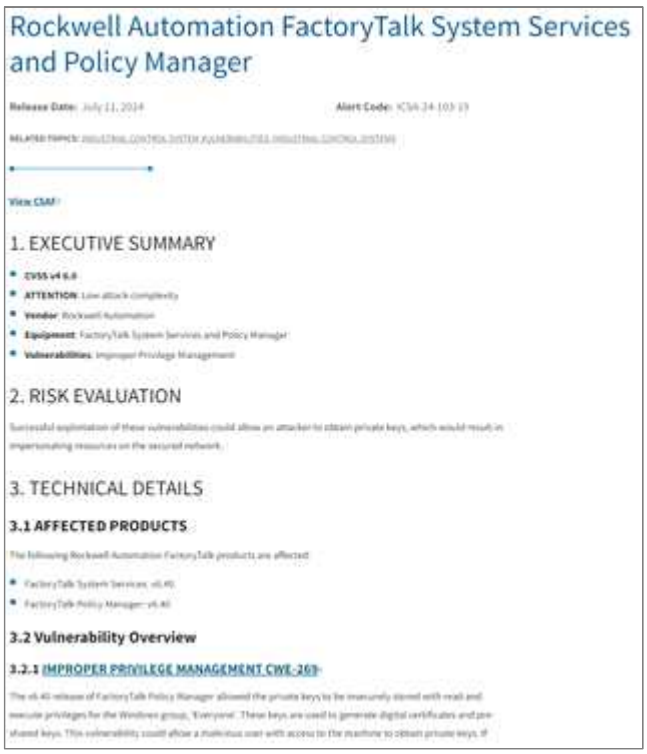
● 공통

Step 1) 제어시스템 구성요소의 업데이트 또는 패치의 절차에서 무결성을 검증할 수 있는 방안이 마련되어 있는지 확인

Step 2) 제어시스템 구성요소의 업데이트 또는 패치 파일의 악성코드를 검사할 수 있는 클린 PC가 구축되어 있으며, 이를 관리 및 운용하고 있는지 확인

C-18 (상)	제어시스템 〉 3. 패치 관리
	제어시스템 구성요소의 알려진 취약점에 대해 보안패치 적용 또는 상응하는 대응책 적용
개요	
점검 내용	제어시스템 구성요소에서 알려진 취약점이 제거되어 있거나, 취약점이 존재하는 경우에 대한 대응방안 존재 여부 점검
점검 목적	최신 보안취약점의 주기적인 확인, 조치 전 영향성 검토, 취약점 조치 등의 체계적인 업무절차를 수립하고 이를 이행함으로써 알려진 취약점으로 인한 제어시스템의 보안위협을 감소시키기 위함
보안 위협	알려진 취약점에 대해 조치하지 못한 제어시스템을 대상으로 해당 취약점을 악용한 비인가자의 침해 시도 또는 자동화된 악성코드의 감염 우려가 있음
참고	※ 스턱스넷(Stuxnet)의 경우 다음과 같은 취약점을 이용하고 있으므로 다음 취약점이 조치되지 않은 경우, 매우 취약한 환경으로 볼 수 있음 CVE-2008-4250 (MS08-067) – 윈도우 서버 서비스 NetPathCanonicalize() 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms08-067.mspx CVE-2010-2568 (MS10-046) – 윈도우 쉘 LNK 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms10-046.mspx CVE-2010-2729 (MS10-061) – 윈도우 프린트 스풀러 서비스 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms10-061.mspx CVE-2010-2743 (MS10-073) – 윈도우 Win32K 키보드 레이아웃 취약점: http://www.microsoft.com/korea/technet/security/bulletin/ms10-073.mspx CVE-2010-2772 – 지멘스 SIMATIC WinCC 기본 패스워드 취약점 http://support.automation.siemens.com/WW/view/en/43876783 현재까지 아직 패치되지 않은 윈도우 작업 스케줄러 취약점 [스턱스넷 이용 취약점] ※ **제어시스템 취약점 목록 제공:** 미국 국토안보부(DHS) 산하 CISA(CyberSecurity & Infrastructure) 홈페이지(https://cisa.gov/news-events/cybersecurity-advisories)에서는 ICS에서 발견된 최신 취약점 목록을 제공하고 있어, 사용 중인 제어시스템 구성요소에 취약점 존재 여부를 확인할 수 있음

[CISA 홈페이지에서 제공하는 ICS 취약점 예시]



[CISA 홈페이지에서 제공하는 ICS 취약점 예시]

점검 대상 및 판단 기준	
대상	전체 제어시스템 구성요소
판단 기준	**양호** : 제어시스템 내부 구성요소에서 알려진 취약점이 없거나, 존재하는 취약점에 대한 조치방안이 이루어진 경우
	취약 : 제어시스템 내부 구성요소에서 알려진 취약점이 있으며, 이에 대한 조치방안이 이루어지지 않은 경우

조치 방법	알려진 취약점에 대한 조치방안(업그레이드 또는 패치, 이에 상응하는 대응방안 적용) 테스트 후 영향성 검토 및 승인절차를 통한 해당 취약점 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소 현황에 대해 취약점 관련 사이트에 제품명, 버전에 대한 취약점 검색 수행 후, 공개된 취약점이 있는지 확인

(예시: CISA ICS 취약점 목록, CVE 목록, 제조사의 제품 보안 관련 웹페이지 등)

C-19 (중)	제어시스템 〉 3. 패치 관리 운영체제, 응용프로그램, 펌웨어 등에 대한 안정성이 확인된 최신 버전의 소프트웨어 사용 및 기술지원이 종료된 제품 미사용
개요	
점검 내용	제어시스템 구성요소의 운영체제, 응용프로그램, 펌웨어 등이 안정성이 확인된 최신 버전 S/W 사용 여부 및 해당 S/W의 기술지원 종료 여부 점검
점검 목적	제어시스템에서 사용하는 운영체제, 응용프로그램, 펌웨어 등이 기술지원이 종료되지 않은 최신 버전으로 운용하도록 하여 안정적인 제어시스템 운영이 가능하도록 하기 위함
보안 위협	기술지원이 종료된 S/W에 취약점이 발견될 경우, 이에 대한 조치가 불가능하여 해당 취약점이 지속적으로 노출될 위험이 존재함
참고	※ **Microsoft Windows 7, Windows Server 2008 R2 지원 종료:** '20. 1. 24. 이후로 Microsoft Windows의 지원이 종료되어 업데이트, 문제 관련 기술지원, 보안 업데이트가 수행되지 않으므로, 이를 사용하지 않아야 함
점검 대상 및 판단 기준	
대상	제어시스템 구성요소 전체
판단 기준	**양호 :** 제어시스템 구성요소가 사용하는 운영체제, 응용프로그램, 펌웨어 등이 기술지원이 종료되지 않은 최신 제품을 사용하는 경우
	취약 : 제어시스템 구성요소가 사용하는 운영체제, 응용프로그램, 펌웨어 등이 기술지원이 종료되었거나, 최신 버전이 아닌 경우
조치 방법	제어시스템 구성요소가 사용하는 운영체제, 응용프로그램, 펌웨어 등이 기술지원이 종료되지 않은 최신 버전 업데이트 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소 현황을 통해 제어 H/W, 정보시스템, 네트워크 장비에서 사용하는 운영체제, 펌웨어가 제조사에서 제공하는 최신 버전이 맞는지 확인하고, 제어 S/W가 제조사에서 제공하는 최신 버전이 맞는지 확인

- 제조사에서 제공하는 최신 버전이 아닌 경우, 이에 대한 사유(제조사 공식 의견)가 안정성 확보이며, 해당 버전이 취약점이 없는 경우 양호한 것으로 판단 가능

Step 2) Step 1)에서 확인한 버전이 제조사에 확인하여 기술지원 종료 예정이 없는지 확인

※ 제어시스템에서 사용하는 운영체제, 펌웨어, 응용프로그램 등이 기술지원 종료 예정일 경우, 이에 대한 대응방안(업데이트 일정 수립, 별도 기술지원 계약 등) 수립을 권고

C-20 (하)	제어시스템 〉 3. 패치 관리
	제어시스템 개선, 신규 시스템 도입, 패치 및 수정 시, 안전성을 테스트하기 위한 테스트베드 또는 시험환경을 구축
개요	
점검 내용	제어시스템의 신규 구축 및 변경(개발수정, 업그레이드, 패치 포함) 전 안정성 테스트 등의 시험환경 구축 여부 점검
점검 목적	제어시스템은 각 제어설비를 감시, 통제하기 위한 다양한 구성요소(HMI, PLC, RTU 등)를 포함하고 있고 해당 구성요소의 신규 구축, 변경 등에 따라서 제어시스템의 일부 또는 전체의 오작동이 발생할 수 있으므로 시험환경을 구축하여 안정성을 검증한 뒤 신규 구축 및 변경 등을 적용하기 위함
보안 위협	안정성 검증 없이 신규 구축 및 변경 등을 적용하는 경우 제어시스템의 일부 또는 전체의 오작동 등의 위험이 존재함
참고	※ **시험환경의 구축 고려사항:** 제어시스템은 IT와 기계적 요소가 결합된 구조를 이루고 있으므로 IT 환경과 같이 이중화, 유지보수 시간 서비스 정지, 테스트서버 구축 등의 방법 적용이 어려울 수 있으므로 기계적 요소의 오작동 가능성을 시험할 수 있는 산업특성을 고려한 자체적인 방안을 수립하는 것이 필요
점검 대상 및 판단 기준	
대상	제어시스템 구성요소 전체
판단 기준	**양호 :** 제어시스템의 변경사항을 시험할 수 있는 환경이 구축된 경우
	취약 : 제어시스템의 변경사항을 시험할 수 있는 환경이 구축되지 않은 경우
조치 방법	제어시스템의 변경사항을 테스트할 수 있는 테스트베드 구축
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 운영 중인 제어시스템에 대한 시험환경 구축이 되어있는지 확인

- 운영 중인 제어시스템의 특성이 고려된 테스트베드 또는 시험할 수 있는 환경 구축이 이루어져 있는지 확인

C-21 (상)	제어시스템 〉 4. 네트워크 접근통제
	제어 네트워크는 업무망, 인터넷, CCTV 망 등 외부망과 물리적으로 분리하여 사용
개요	
점검 내용	제어시스템을 감시, 통제하는 네트워크 구성에서 제어망(Production Control System Network)의 업무망(Business Network), 인터넷망 등으로 물리적 분리 여부 점검
점검 목적	제어시스템에 인터넷을 통한 각종 침해위협(예시: 악성코드 등)으로부터 보호하기 위함
보안 위협	• 업무망과 제어망이 분리된 경우에도 업무망 PC에서 제어망에 있는 설비를 모니터링할 수 있는 경우 해당 PC의 인터넷을 차단하지 않아 스턱스넷과 같은 악성코드에 감염되고 제어망에 있는 설비의 운영 정보 수집은 물론, 취약점을 악용한 제어시스템 마비를 초래할 위험이 존재함 • 제어망과 시설 감시를 위한 CCTV 망이 연결되어있는 경우 CCTV에서 발생시키는 다수의 트래픽으로 인해 제어망의 가용성이 침해되는 경우를 초래할 위험이 존재함 • **위협 사례:** 쇼단(Shodan) 연구원에 따르면 미국은 5만 7천 개라는 전 세계에서 가장 많은 수의 산업제어시스템(ICS)을 가지고 있으며 인터넷에 연결되어있다고 밝힘. 또한, '14년 12월 독일 언론에 따르면, 독일의 한 제철소 용광로의 제어시스템에 대한 해킹 공격으로 제어시스템이 파괴되면서 관련 산업 전체에 큰 피해를 준 바 있으며 이는 당시 해커들은 보안 의식이 낮은 용광로 운영 직원의 인터넷 Email을 이용해 로그인 계정을 탈취한 뒤 제어시스템을 장악한 것으로 알려져 있음
참고	※ **제어시스템 네트워크 구분(Segmentation):** NIST SP 800-82 Guide to Industrial Control Systems Security에서 제어시스템의 안전한 네트워크 구성을 위해 네트워크를 도메인별로 구분하고 구분된 도메인 간 접근 통제할 것을 권장함. 이때, 네트워크를 구분하는 방식 중 물리적인 분리의 경우 두 도메인 간 통신을 완전히 막을 수 있는 방법의 하나로 제시하고 있음. 이에 따라 제어망의 경우 인터넷망과는 물리적으로 분리할 것을 권고하고, 제어시스템 운영 특성상 업무망과 연계가 필수적일 경우 C-10 항목을 참고하여 물리적 일방향 자료전달 환경 구축을 권고함
점검 대상 및 판단 기준	
대상	제어시스템을 구성하는 네트워크 전체
판단 기준	**양호 :** 외부망(인터넷) 또는 내부망(업무망)과 분리하여 운영하는 경우
	취약 : 외부망(인터넷) 또는 내부망(업무망)과 동일네트워크로 구성하여 운영하는 경우
조치 방법	제어시스템 운영망과 업무망 분리 및 인터넷 차단
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

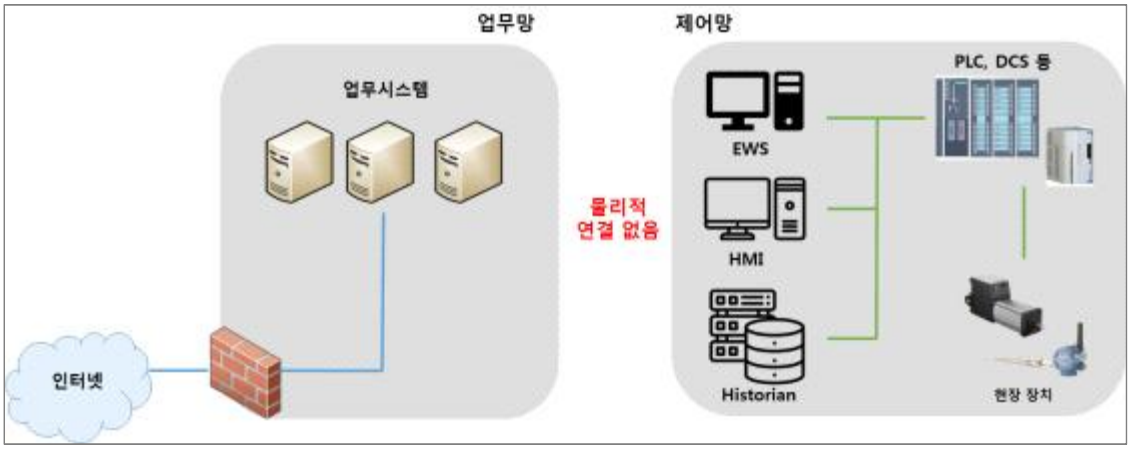
Step 1) 제어시스템 네트워크 구성도를 검토하여 제어망, 업무망, 인터넷망 등이 모두 분리되어 접근이 차단되도록 구성되었는지 확인

Step 2) 제어망의 네트워크 분리는 물리적 분리 방식이며, 제어망 내부에서 다른망으로 데이터 전달이 불가능한지 확인

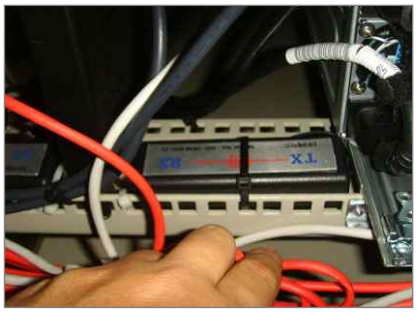
- 제어망 내 임의의 정보시스템을 선택하여 정보시스템에서 다음 명령어를 수행하고, 수행 결과 연결이 되지 않는지 확인
  (1) 콘솔 창에서 ping, tracert 등의 명령어를 제어망이 아닌 업무망, 또는 다른 망의 IP와 공개 DNS IP주소, 포털사이트의 IP주소를 대상으로 수행
- (다른망과 연결이 되는 경우) 해당 연결의 목적, 원인을 파악하여 불필요한 연결일 경우, 연계지점을 확인하고 물리적으로 분리하도록 조치하고 반드시 필요한 연결일 경우, C-10 항목을 참고하여 일방향 자료전달 체계 구축을 권고

※ 제어시스템의 네트워크 구성

제어시스템을 운영하는 조직은 제어망(Production Control System Network)과 업무망(Business Network)을 물리적으로 분리하여 운용할 것을 권장



[제어망과 업무망의 물리적 분리 예시]

C-22 (상)	제어시스템 〉 4. 네트워크 접근통제
	제어 네트워크 외부로 자료전달 시 물리적 일방향 자료전달 환경을 구축하여 외부에서 제어 네트워크로의 침입을 차단
개요	
점검 내용	제어 네트워크와 외부 자료 연계가 필요한 경우 제어망으로부터 업무망으로의 일방향 데이터 전송 여부 점검
점검 목적	업무망에 대한 침해위협으로 인해 제어망에 직접적인 피해(예시: 운전 조작 등)가 발생하지 않도록 하기 위함
보안 위협	제어망과 업무망 간 운전정보를 양방향 전송하게 되는 경우 업무망의 운영자 PC를 통한 내부자 부주의 또는 오·남용(예시: 운전 조작 등) 우려가 있고, 악성코드가 유입되는 경우 제어망 내부에 위치한 시스템까지 감염될 위험이 존재함
참고	※ 본 점검항목은 제어망에 위치한 설비 또는 시스템 등의 정보를 외부(내부 업무망 또는 외부 업무망)로 전송하는 경우 일방향 전송을 요구하는 항목으로 일방향 전송 장비의 예시는 다음 그림과 같음  [일방향 자료 전달 제품 예시]
점검 대상 및 판단 기준	
대상	제어망으로부터 내부 업무망으로 정보 연계가 이루어지는 시스템 제어망으로부터 외부 업무망으로 제어망의 운전정보 등을 전송하는 설비 및 시스템
판단 기준	**양호 :** 제어망의 운전정보를 업무망으로 일방향 전송하는 경우
	취약 : 제어망의 운전정보를 업무망으로 양방향 전송하는 경우
조치 방법	내·외부의 통신선로에 대한 물리적 일방향 전송이 이루어지도록 조치하거나, DMZ를 구성하고 방화벽 등을 통한 일방향 접근통제 정책(Rule) 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

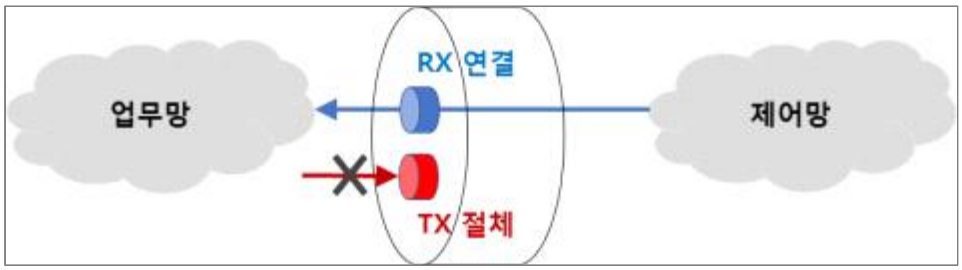
Step 1) 제어시스템 네트워크 구성도를 검토하여 제어망으로부터 내부 업무망 또는 외부 업무망과 연계지점이 있는지 확인

Step 2) 해당 연계지점에서의 정보 전송이 다음 각 호의 방법과 같은 일방향으로 이루어지는지 확인

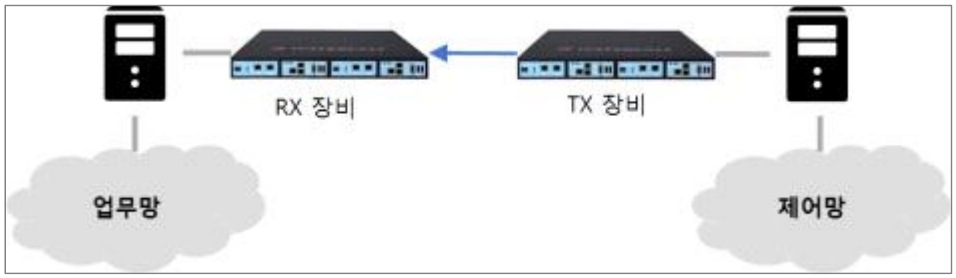
- 송·수신 회선 한쪽을 물리적으로 단절
  (예시: LAN, 시리얼 라인의 업무망에서 제어망으로의 TX-RX 라인을 절체)
- 데이터 송신용 장비, 수신용 장비를 한 쌍으로 하여 일방향으로만 정보 전달이 가능하도록 개발된 전용 장비 사용

※ 물리적 일방향 자료전달 환경 구축

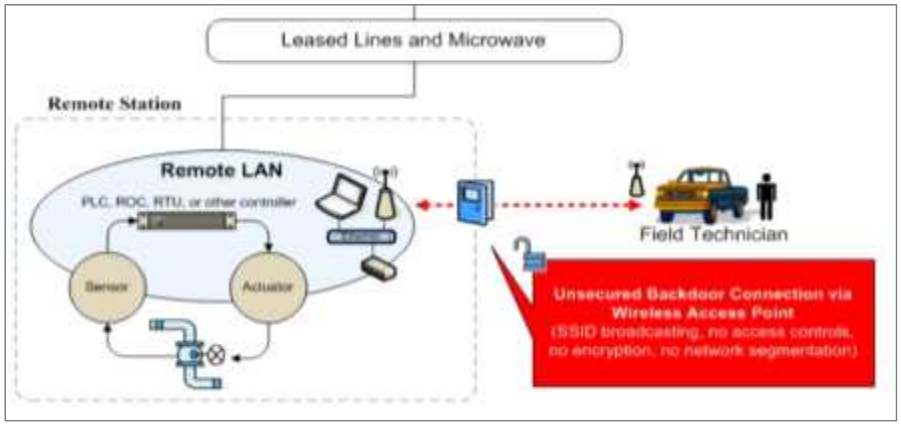
일방향 자료전달 환경을 구축의 방안으로는 물리적으로 절체한 일방향 전송 장비를 이용하여 구축하는 방안이 있음



[RX 장비와 TX 장비를 활용한 일방향 전송 환경1]



[RX 장비와 TX 장비를 활용한 일방향 전송 환경2]

C-23 (상)	제어시스템 〉 4. 네트워크 접근통제
	제어 네트워크에 무선인터넷, 테더링, 외부 유선망 등의 외부망 연결을 제한하고 주기적으로 점검
개요	
점검 내용	제어망, 업무망, 인터넷망 등의 물리적 망 분리 이외에도 이를 우회할 수 있는 무선인터넷, 테더링 등의 통제 여부 점검
점검 목적	내부 보안정책을 우회할 수 있는 비인가 무선 AP 설치, 스마트폰의 테더링 이용 등과 같은 외부해킹 및 악성코드 감염 경로를 차단하기 위함
보안 위협	• 제어망 또는 업무망 등에 비인가 무선 AP 설치, 스마트폰의 테더링 이용 등과 같은 외부로의 인터넷 연결 점검이 생기는 경우는 물리적 망 분리를 우회할 수 있고 이를 통해 악성코드가 유입되는 경우 제어망에 위치한 시스템까지 감염될 위험이 존재함 • **무선통신 인터셉트(EM/RF Interception):** 일반적인 제어시스템 통신 구간에서는 무선통신을 사용하지 않지만, RTU 하단의 제어 구성요소들과 IED에는 무선통신이 적용되는 경우가 있고 해당 통신 구간의 통신은 비인가 기기를 이용한 가로채기가 상대적으로 용이
참고	※ **제어시스템의 보안정책 우회 접근:** 제어시스템을 구성하는 환경에서 내부망 내에 위치한 비인가 무선 AP(또는 외부로부터 수신되는 무선 AP), 스마트폰의 테더링 등을 이용한 외부 인터넷 연결이 이루어질 수 있으며 이를 차단하기 위해서는 비인가 기기의 반·출입 통제, 무선랜카드 사용통제 등의 물리적 통제를 함께 고려해야 함  [무선 AP를 이용한 제어망 무단 접근]
점검 대상 및 판단 기준	
대상	제어시스템을 구성하는 네트워크 전체
판단 기준	**양호 :** 제어 시설에 비인가 장비에 대한 반입이 불가능하며, 제어망 및 내부 업무망의 유·무선 인터넷 접속차단이 이루어지는 경우
	취약 : 제어 시설에 비인가 장비에 대한 반입 통제가 이루어지지 않거나, 제어망 및 내부 업무망에서 유·무선 인터넷 접속이 가능한 경우
조치 방법	외부 연계 접점 차단 설정(외부 연계일 경우 물리적 일방향 시스템 적용)
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어망 및 업무망에 외부 노트북, 태블릿PC, 스마트폰 등이 반입될 때 이를 통제, 보안 조치하는 절차가 있는지 확인하고, 해당 절차가 없다면 기반시설에 대한 관리·물리 점검항목을 참조하여 개선조치

Step 2) 제어망 및 업무망의 서버, PC에 대해 인터넷 접속 사실이 있는지 다음 각 호의 방법으로 확인하고, 접속이 가능하다면 C-09(상), C-10(상) 등의 조치 방법을 참고하여 개선조치

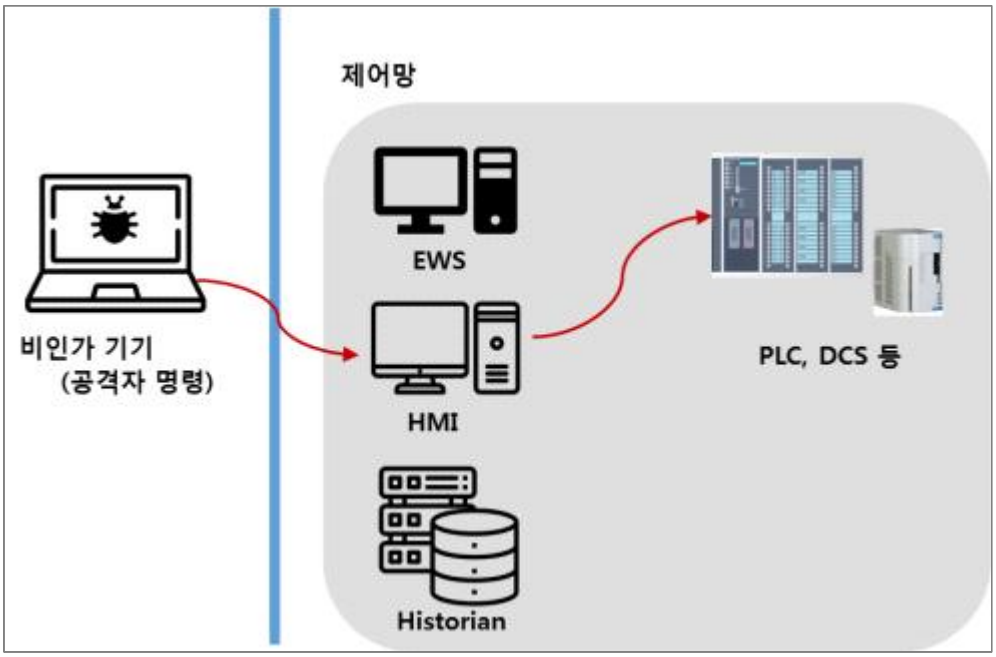
- Windows 환경인 경우, 웹브라우저에서 인터넷 사이트 연결 이력이 있는지 점검
  - (1) Windows의 레지스트리 값을 확인하는 방법으로써, CMD 창에 다음 명령어를 입력
    reg query “HKCU\Software\Microsoft\Internet Explorer\TypedURLs”
  - (2) 상기 명령어 입력 시 웹브라우저 창에 입력한 값이 저장되는 레지스트리 값을 확인
    url1 REG_SZ http://www.kisa.or.kr/
  - (3) Cookie 파일 확인하는 방법으로서, Cookie 파일 안에 내용에 URL을 확인하여 인터넷 사용 여부 판단 (단, 쿠키 및 웹사이트 데이터 삭제 시는 확인 불가)
    - CMD 창에 "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders" | findstr "Cookies" 입력하여 쿠키 저장 위치 파악
    - 쿠키가 저장된 폴더에 들어가 쿠키 파일 내용에 포함된 URL 확인
- 망 분리가 이루어지지 않고 외부 인터넷 서버로의 패킷 전달이 가능한지 점검
  #ping 외부 IP(예시: 공개 DNS IP주소, 포털사이트의 IP주소 등)

Step 3) 노트북 등을 이용해 제어 시설을 이동하면서 근거리에서 수신되는 내부 무선 AP가 있는지 점검하고, 비인가 무선 AP가 있으면 제거

- (내부가 아닌 외부) 무선 AP가 감지되면 해당 구역의 시스템 무선랜카드를 제거
- (장비가 있는 경우) 무선 AP, 무선네트워크 전파 스캐너를 사용하여 점검

Step 4) 노트북 등을 이용해 제어 시설을 이동하며 근거리에서 수신되는 외부 WiFi 접속 가능성과 스마트폰의 테더링을 통한 접속 가능성이 있는지 점검하고, 가능한 경우, 다음 방법을 적용하여 조치

- 해당 구역 내 서버 및 업무 PC의 무선랜카드를 물리적으로 제거하거나 기능 정지
- (장비가 있는 경우) 무선 방화벽을 통한 무선망 이용 차단

C-24 (상)	제어시스템 〉 4. 네트워크 접근통제
	제어 네트워크에 비인가된 시스템/기기에 대한 연결 및 접속을 차단
개요	
점검 내용	제어 네트워크에 비인가된 시스템/기기 등을 연결하는 경우의 연결 및 접속 차단 여부 점검
점검 목적	출입자가 비인가 기기, 서버 및 노트북 등을 반입하여 임의로 제어 네트워크에 연결할 수 없도록 하기 위함
보안 위협	악성코드가 감염된 기기, 서버 및 노트북 등을 악의적인 목적으로 반입하여 제어 네트워크에 연결하고 접속하는 경우 해당 시스템을 경유하여 업무망 또는 제어망의 취약한 시스템(예시: 특정 버전의 OPC 시스템)을 위협하고 제어설비의 권한을 획득할 위험이 존재함  [비인가된 기기를 통한 제어시스템 접근 및 제어명령]
참고	※ **제어시스템의 비인가 기기 연결통제 방안 :** 제어시스템을 구성하는 환경에서 비인가 서버 및 노트북 등이 반입되고 이를 손쉽게 제어 네트워크에 연결하는 것을 차단하기 위해서는 비인가 기기의 반·출입 통제, 기기의 네트워크 연결통제 등을 함께 고려해야 함
점검 대상 및 판단 기준	
대상	제어시스템을 구성하는 네트워크 전체
판단 기준	**양호 :** 사전 허가된 시스템 및 기기만 제어 네트워크에 연결 및 접속이 가능한 경우
	취약 : 사전 허가되지 않은 임의의 시스템 및 기기가 제어 네트워크에 연결 및 접속이 가능한 경우
조치 방법	제어시스템을 구성하는 네트워크에 시스템 또는 기기를 연결하는 경우 사전 승인 및 MAC 식별 등에 의한 접근통제 조치 설정
조치 시 영향	현재 제어시스템 내 운영 서비스에 대한 정확한 파악이 되지 않은 경우, 장애 발생 가능

점검 및 조치 사례

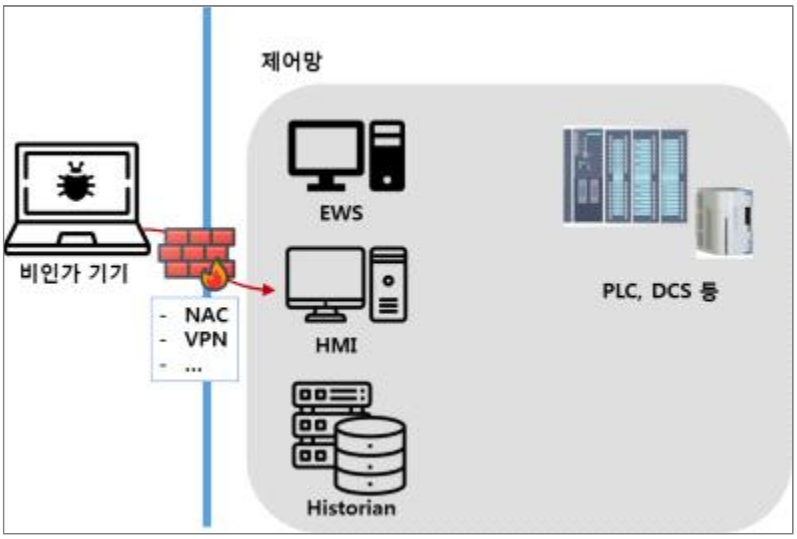
● 공통

Step 1) 제어 네트워크에 비인가 시스템 및 기기를 임의로 연결할 수 없도록 다음 각 호의 방법과 같은 조치가 적용되는지 확인

- 연결하려는 기기의 MAC 주소 등의 정보를 식별하고 내부 신청절차에 따라 허가된 IP주소를 부여(관리적 통제)
- NAC(Network Access Control) 등의 시스템을 적용하여 허가되지 않은 임의의 시스템 및 기기 연결을 차단(기술적 통제)

Step 2) 유지보수 등을 위해 제어망의 시스템 접근이 필요한 경우에는 사전 허가된 제어망 시스템에 대하여만 접근할 수 있도록 하는 보안대책을 적용

(예시: 방화벽을 경유한 VPN 접속)



[허가받지 않은 외부기기의 접속 통제]

C-25 (상)	제어시스템 〉 4. 네트워크 접근통제
	물리적 일방향 자료전달 환경의 올바른 동작 및 운용에 대한 주기적인 점검 수행
개요	
점검 내용	제어망으로부터 업무망으로의 데이터 전송을 위한 물리적 일방향 전송 환경이 정상 동작하고 있는지 운용상태를 주기적으로 점검
점검 목적	물리적 일방향 자료전달을 위한 장비가 올바르게 운용되었는지 확인하여 업무망 침해위협으로 인한 제어망에 직접적인 피해(예시: 운전 조작 등)가 발생하지 않도록 하기 위함
보안 위협	제어망과 업무망 간 운전정보를 양방향 전송하게 되는 경우 업무망의 운영자 PC를 통한 내부자 부주의 또는 오·남용(예시: 운전 조작 등) 우려가 있고, 악성코드가 유입되는 경우 제어망에 위치한 시스템까지 감염될 수 있음
참고	※ 본 점검항목은 제어망에 위치한 설비 또는 시스템 등의 정보를 외부(내부 업무망 또는 외부 업무망)로 전송하는 경우 물리적 일방향 전송을 위한 환경을 올바르게 설정하고 운용하고 있는지 확인함 ※ 본 항목은 C-10 항목에서 확인한 일방향 전송 장비의 운용현황을 점검하는 항목으로 잘못된 운용으로 인한 분리된 네트워크의 외부 노출 가능성을 방지하기 위한 항목임
점검 대상 및 판단 기준	
대상	제어망으로부터 내부 업무망으로 정보 연계가 이루어지는 시스템 제어망으로부터 외부 업무망으로 제어망의 운전정보 등을 전송하는 설비 및 시스템
판단 기준	**양호 :** 제어망의 운전정보를 업무망으로 일방향 전송하도록 설정한 것으로 확인되고 일방향 트래픽만 존재하는 경우
	취약 : 제어망의 운전정보를 업무망으로 양방향 전송하도록 설정되거나 양방향 트래픽이 확인되는 경우
조치 방법	내·외부의 통신선로에 대한 물리적 일방향 전송이 이루어지도록 조치하거나, 방화벽 등을 통한 일방향 접근통제 정책(Rule) 설정
조치 시 영향	현재 제어시스템 내 운영 서비스에 대한 정확한 파악이 안될 경우, 장애 발생 가능

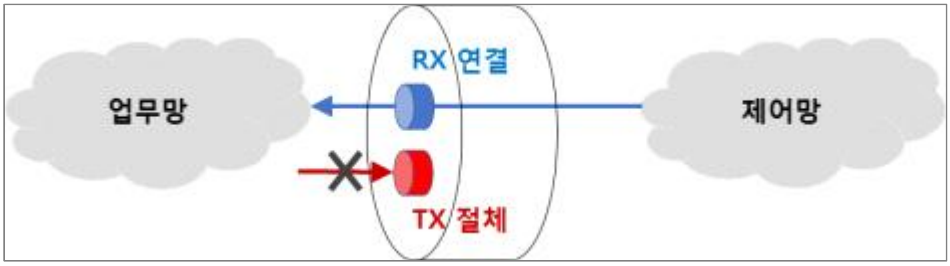
점검 및 조치 사례

● 공통

Step 1) 제어시스템 네트워크 구성도를 검토하여 제어망으로부터 내부 업무망 또는 외부 업무망과의 연계지점에 일방향 전송을 위한 장비가 구축되어 있는지 확인

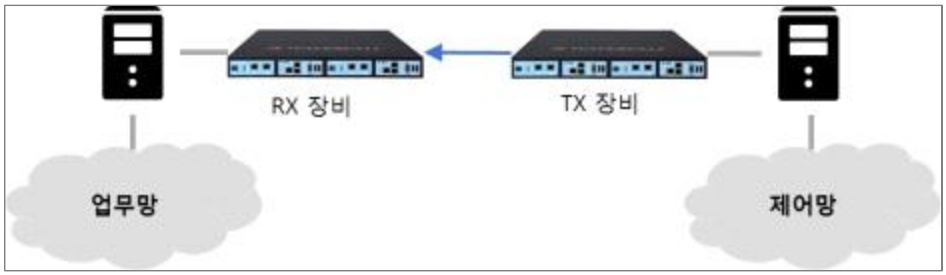
Step 2) 해당 연계 지점에서의 정보 전송이 다음 각 호의 방법과 같이 운용하고 있는지 실제로 현장에서 확인

- 송·수신 회선 한쪽을 물리적으로 단절
  (예시: LAN, 시리얼 라인의 업무망에서 제어망으로의 TX-RX 라인을 절체)



[일방향 전송을 위한 물리적 절체]

- 데이터 송신용 장비, 수신용 장비를 한 쌍으로 하여 일방향으로만 정보 전달이 가능하도록 개발된 전용 장비 사용



[RX 장비와 TX 장비를 활용한 일방향 전송 환경]

- 제어망 송신자 주소에서 내·외부 업무망 수신자 주소 및 포트에 대해서만 제한적인 out-bound 정책 허용(in-bound 정책 적용은 금지)

Step 3) 제어망과 내부 업무망 또는 외부 업무망 간의 트래픽 분석 결과, 일방향 전송 트래픽만 존재하는지 확인

C-26 (하)	제어시스템 〉 4. 네트워크 접근통제
	제어 네트워크를 용도에 따라 세분화하고, 접근제어를 수행하여 제어시스템 운영에 필요한 네트워크, 시스템 간의 통신만 허용
개요	
점검 내용	제어시스템을 구성하는 서브넷(Subnet) 등의 방법으로 세분화(예시: 제어망을 종류별로 구분)하고 이에 따른 접근통제 여부 점검
점검 목적	제어시스템 및 운영조직의 규모에 따라 네트워크 내부를 계통 및 역할에 따라 세분화하여 이에 대한 접근통제를 강화하기 위함
보안 위협	단일 네트워크 내에 있는 모든 시스템, 기기에 대해 운영자의 임의 접근이 가능하거나 악성코드 감염에 따른 피해 확산의 위험이 존재함
참고	※ 계통의 경우 에너지 생산 분야를 예로 들면, 터빈(가스, 스팀), 보일러, 전기(ECMS) 등의 각 제어시스템을 의미하며 PLC 등을 이용한 소규모 제어시스템(예시: 탈황·탈질, 집진, 수처리 등) 각각을 뜻함 ※ 역할의 경우 상기 계통을 효과적으로 운영하기 위해 구축하는 분석·감시시스템, 패치 및 업데이트의 안정성을 확보하기 위한 시험·평가시스템, 운전원의 교육을 위한 훈련 시스템 등을 의미
점검 대상 및 판단 기준	
대상	제어시스템을 구성하는 네트워크 전체
판단 기준	**양호 :** 제어망 내부 네트워크를 세분화하여 구성하고 접근통제 규칙이 적용된 경우
	취약 : 제어망 내부 네트워크를 단일 구성한 경우
조치 방법	제어망 내부 네트워크를 용도에 따라 세분화하여 구성하고 세분화된 네트워크 간에 접근통제 규칙을 방화벽, 스위치 등을 통해 설정
조치 시 영향	접근 정책 설정에 따라 일부 제어시스템, 설비 간의 오작동 발생 가능

점검 및 조치 사례

● 공통

Step 1) 제어시스템 네트워크 전체 구성도와 제어망 내의 상세 네트워크 구성도(IP 대역 포함)를 확인하되 다음 사항을 함께 점검

- 제어망이 단일 네트워크로 이루어지지 않고 제어설비의 역할 따라 서브넷(Subnet) 구성
- IP 대역을 분리, 구성한 장비(예시: 방화벽, 스위치 등)에 설정된 접근통제 규칙

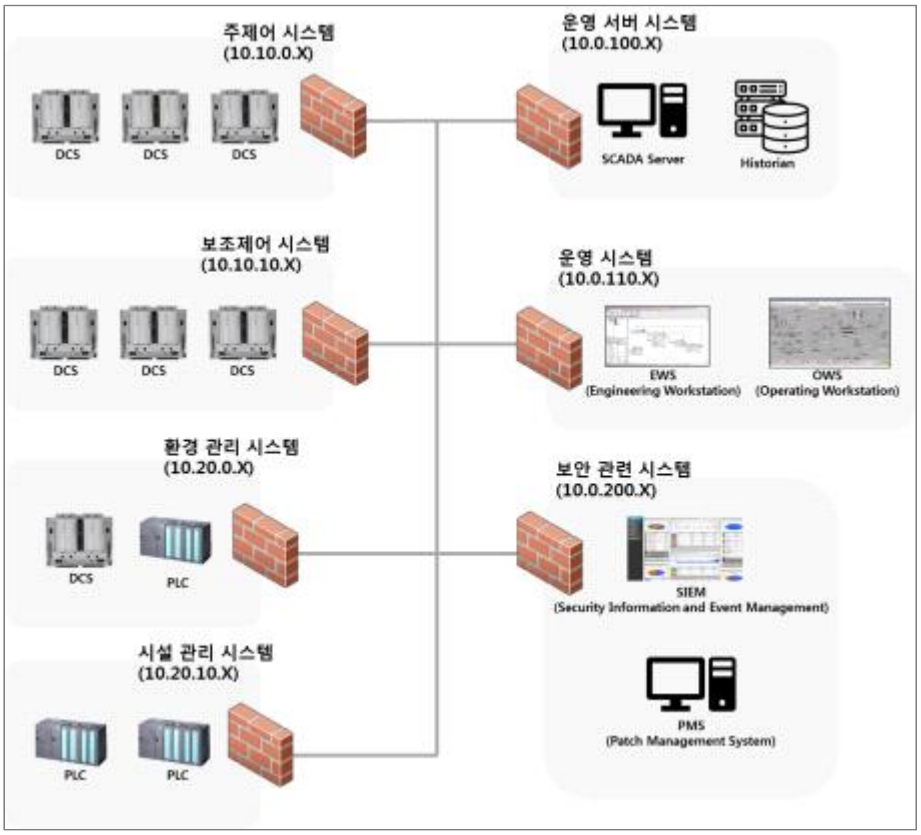
Step 2) Step 1)에 따라 점검한 결과, 제어망을 세분화하여 네트워크 구성이 이루어졌고 분리 구성된 네트워크 간에 접근통제 규칙이 네트워크 장비 또는 방화벽에 적절하게 적용되었는지 점검

※ 네트워크 구성을 변경하는 것은 제어시스템 일부 또는 전체에 큰 영향을 줄 수 있음 즉 서브넷 구성 실수(예시: IP주소 충돌 등)와 스위치 및 방화벽의 접근규칙 오류(예시: 서브넷 간의 IP 차단)만으로 HMI 등의 모니터링 장애, 특정 제어설비에 제어 명령 수신 오류 등의 발생 가능성이 높으므로 점검항목 C-34에 따른 시험환경 구축은 물론 긴급 상황 발생 시 복구 대책 등을 함께 고려한 뒤에 개선조치 수행을 권고

※ 계층적으로 구성된 IP 체계 예시

네트워크 단위		IP
중앙제어 네트워크		10.0.0.1~255
광역 지역 제어 네트워크	광역 지역 제어 네트워크1	10.10.0.1~255
	광역 지역 제어 네트워크2	10.20.0.1~255
	광역 지역 제어 네트워크3	10.30.0.1~255
지역 제어 네트워크	지역 제어 네트워크1	10.30.10.1~255
	지역 제어 네트워크2	10.30.20.1~255
	지역 제어 네트워크3	10.30.30.1~255

※ 내부 네트워크의 구성을 표준적으로 요구할 수는 없기 때문에 산업특성, 규모 등을 고려해 적절한 세분화가 이루어지는 확인



[방화벽을 이용한 네트워크 세분화 구성 예시]

C-27 (상)	제어시스템 〉 5. 물리적 접근 통제
	제어시스템에 대해 네트워크 포트, USB 포트 등 외부 연결 접점에 대해 허가받은 사항을 제외하고 모두 물리적 또는 논리적으로 차단
개요	
점검 내용	제어시스템 구성요소에 존재하는 네트워크 포트, USB 포트 등 외부 연결접점에 대한 사용 통제(예시: 원천 차단 및 허가 시 접근) 여부 점검
점검 목적	제어시스템 구성요소의 사용하지 않는 포트에 대해 봉인 및 차단을 함으로써 제어시스템의 외부 접점을 통한 허가받지 않은 사용자의 제어시스템 무단 접근을 차단하기 위함
보안 위협	• 제어시스템의 네트워크 포트를 통해 악의적인 장비가 제어망에 접근하여 공격을 시도할 위험이 존재함 • 제어시스템의 USB 포트에 안전하지 않은 이동형 저장 매체 연결 시 악성코드 감염을 통해 제어시스템의 장애 또는 정지 등의 피해가 발생할 위험이 존재함 • 제어시스템 구성요소의 디버깅 포트를 통해 구성요소에 접근하여 펌웨어 추출, 악성 펌웨어 삽입, 제어 명령 실행 등을 통해 제어시스템의 장애 또는 정지가 발생할 위험이 존재함
참고	※ **외부 연결 접점 통제방안:** 제어시스템 구성요소의 물리적으로 접근 가능한 모든 인터페이스에 대해 봉인장치 또는 일련번호가 있는 보안스티커를 활용하여 봉인하거나 해당 포트의 비활성화를 통해 논리적으로 차단 및 봉인 또는 차단된 인터페이스를 불가피하게 개폐하는 경우 정보보호 책임자의 승인을 획득하고 봉인장치 관리대장에 사용내역을 기록하여 관리하도록 권고
점검 대상 및 판단 기준	
대상	제어시스템 구성요소 전체
판단 기준	**양호 :** 사용하지 않는 네트워크 포트, USB 포트 등을 물리적 봉인장치 또는 일련번호가 있는 스티커로 봉인하거나 논리적으로 차단하는 경우
	취약 : 사용하지 않는 네트워크 포트, USB 포트 등을 물리적으로 봉인하지 않고 논리적으로도 차단하지 않은 경우
조치 방법	미사용 인터페이스(네트워크 포트, USB 포트 등)에 대해 물리적 차단 조치를 적용하거나 해당 기능을 논리적으로 차단하도록 설정
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

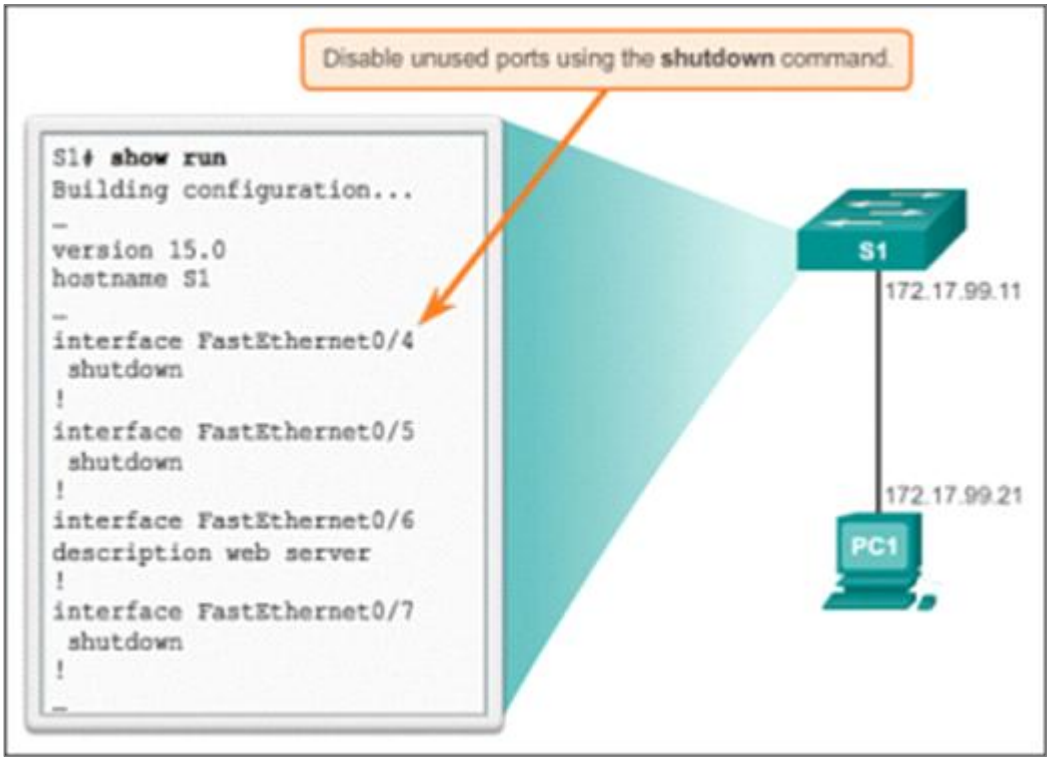
Step 1) 제어시스템 구성요소의 미사용 인터페이스(네트워크 포트, USB 포트 등)에 대한 물리적 봉인 여부 확인

※ 점검 대상은 제어 H/W(PLC, DCS 등), 서버, PC, 현장장치(센서, 액추에이터 등), 네트워크 장치, 방화벽, 단방향 장치, 프린터, 엔지니어링 노트북 등 제어시스템에 연결 가능한 모든 구성요소임

[네트워크 포트 봉인 예시]

[USB 포트 봉인 예시]

Step 2) 물리적 봉인이 되지 않은 제어시스템 구성요소의 미사용 인터페이스(네트워크 포트, USB 포트 등)에 대한 논리적 차단 여부 확인



[네트워크 장비 미사용 인터페이스 비활성화(shutdown) 예시]

C-28 (중)	제어시스템 〉 5. 물리적 접근 통제
	제어시스템 구성요소를 물리적으로 보호할 수 있는 조치 적용(잠금장치가 있는 함체, 랙, 수납 책상 등)
개요	
점검 내용	물리적으로 보호될 수 있는 잠금장치가 있는 함체, 랙, 수납 책상 등을 통한 제어시스템 구성요소 보호 여부 점검
점검 목적	제어시스템 구성요소가 물리적인 공격으로부터 보호하기 위해 인가되지 않은 물리적인 접근을 차단하고 있는지 확인하기 위함
보안 위협	제어시스템의 가용성을 방해하기 위한 여러 공격 중 하나로 제어기기에 대한 물리적인 손상이 있으며, 이를 통해 직접적인 가용성 방해 및 물리적 공격을 통한 내부정보 유출 등의 위험이 존재함
참고	※ 본 점검항목은 제어시스템 구성요소의 물리적인 보호를 위한 기초적인 보호 조치로, 물리적인 보호 조치(함체, 랙, 수납 책상 등)에 대한 무단 해제 시도 시 이를 탐지할 수 있는 방법(CCTV 등)도 적용할 것을 권고
점검 대상 및 판단 기준	
대상	제어시스템 모든 구성요소
판단 기준	**양호 :** 제어시스템의 모든 구성요소가 잠금장치가 있는 함체, 랙, 수납 책상 등으로 보호되고 있는 경우
	취약 : 제어시스템의 모든 구성요소가 별도의 보호장치 없이 바로 접근이 가능한 경우
조치 방법	별도의 보호장치 없이 노출된 제어시스템 구성요소에 잠금장치가 있는 함체, 랙, 수납 책상 등으로 인가되지 않은 물리적 접근이 불가능하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소가 잠금장치가 있는 함체, 랙, 수납 책상 등을 통해서 보호되고 있는지 확인

- 특히, 현장에 설치된 제어시스템의 구성요소인 경우 인가되지 않은 물리적인 접근으로부터 보호되고 있는지 점검
- 잠금장치가 있는 함체, 랙, 수납 책상 등으로 제어시스템 구성요소가 보호되고 있으며 인가된 사용자만 이에 대한 잠금 해제할 수 있도록 해야 하며, 보호되지 않은 제어시스템 구성요소는 이러한 보호장치를 구비하여 적용하도록 조치

C-29 (상)	제어시스템 〉 6. 보안위협 탐지
	백신 프로그램 설치가 가능한 제어시스템 구성요소에 대해 악성코드 감염 및 차단을 위한 백신 프로그램 설치
개요	
점검 내용	백신 프로그램 설치가 가능한 제어시스템 구성요소에 백신 프로그램 설치 여부 확인
점검 목적	제어시스템을 악성코드 감염으로부터 보호하기 위한 백신 설치 여부를 확인하기 위함
보안 위협	백신 프로그램이 설치되지 않은 경우, 악성 바이러스로 인한 제어시스템 장애, 정지 등의 발생 위험이 존재함
참고	※ **바이러스** : 프로그램을 통해 감염되는 악성 소프트웨어 ※ **웜** : 자체 복제하고 네트워크를 통해 스스로 감염되는 악성 소프트웨어 ※ **트로이목마** : 겉보기에는 정상적인 프로그램으로 보이지만 악성 루틴이 숨어 있어 실행하면 악성코드를 실행하는 소프트웨어 ※ **랜섬웨어** : 특정 파일을 암호화하여 파일을 사용 불가능한 상태로 만들어 복구를 위해 돈을 요구하는 악성 소프트웨어
점검 대상 및 판단 기준	
대상	제어시스템 구성요소 중 정보시스템(서버, PC 등)과 같이 백신 프로그램 설치가 가능한 구성요소
판단 기준	**양호** : 백신 프로그램이 설치된 경우
	취약 : 백신 프로그램이 설치되지 않은 경우
조치 방법	제어시스템 제조사와 협의하여 안정성이 보장되는 백신 프로그램을 설치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소 중 백신 프로그램 설치가 가능한 구성요소 확인

Step 2) 백신 프로그램 설치가 가능한 구성요소에 모두 백신 프로그램이 설치되어 운용되고 있는지 확인

※ 백신 프로그램 예시

[Windows Defender(MS)]

[Kaspersky Antivirus(Kaspersky)]

[알약(이스트소프트)]

[V3(안랩)]

※ 제어시스템 가용성 등의 문제로 인해 백신 프로그램 설치가 불가능한 구성요소의 경우 이에 대해 인지하고 보완대책 마련 필요

C-30 (하)	제어시스템 〉 6. 보안위협 탐지
	이상 트래픽 발생 탐지 등 제어시스템 내의 보안 관리를 위해 적합한 침입탐지시스템 등을 구축 및 운용하고, 구축된 보안 솔루션 및 보안 장비에서 탐지한 보안 이벤트에 대해 모니터링 수행
개요	
점검 내용	제어시스템 내에 침입탐지시스템 등의 보안 관리 방안 구축 및 구축된 보안 장비에서 탐지한 보안 이벤트에 대한 모니터링 수행 여부 점검
점검 목적	제어망 내 이상 트래픽 발생 등을 탐지하기 위해 침입탐지시스템 등을 구축하고 보안 이벤트를 모니터링하여 제어시스템을 안전하게 운용하기 위함
보안 위협	가용성을 중요시하는 제어시스템의 특성상 공격에 대한 적시 가능이 매우 중요하며 보안 이벤트에 대한 실시간 모니터링이 이루어지지 않고 있는 경우 사고 발생 시 이에 대한 탐지가 늦어 피해 파급 효과가 증대될 위험이 존재함
참고	※ 오용(Misuse) 침입탐지시스템을 구축한 경우, 공격 패턴은 물론 충분한 양의 과거 공격 패턴을 적용하여 탐지 정책을 설정해야 함 ※ 비정상행위(Anomaly) 침입탐지시스템을 구축한 경우, 도입 기관의 트래픽 패턴을 분석하여 정상행위 프로파일이 최적화되어 있어야 함
점검 대상 및 판단 기준	
대상	제어망 네트워크
판단 기준	**양호 :** 제어시스템 내에 침입탐지시스템이 구축되어 있고 이상 트래픽, 보안 이벤트 등에 대해 모니터링을 수행하는 경우
	취약 : 제어시스템 내에 이상 트래픽, 보안 이벤트 등에 대해 모니터링을 수행하지 않는 경우
조치 방법	제어망 전체에 대해 이상 트래픽 발생 등을 탐지할 수 있는 침입탐지시스템 등을 구축하고 보안 이벤트를 모니터링하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소 현황(목록)을 활용하여 제어시스템 이상 트래픽 발생 탐지 등을 위한 장비(침입탐지시스템 등) 구축 유무를 확인

Step 2) Step 1) 에서 확인한 구축 장비를 활용하여 탐지한 보안 이벤트를 모니터링하는지 확인

※ 이상 트래픽 탐지 장비는 제어망 내의 전체 트래픽에 대해 탐지할 수 있는 위치에 구축 및 운용되어야 함

C-31 (상)	제어시스템 〉 7. 복구 대응
	제어시스템 대상 사이버 위기대응 매뉴얼을 수립
개요	
점검 내용	제어시스템 대상 사이버 침해사고 발생 시 대응을 위한 사이버 위기대응 매뉴얼 수립 여부 점검
점검 목적	비상상황에 의한 피해 파급 효과가 큰 제어시스템의 사이버 위협, 침해사고 발생 시 신속한 원인 규명, 복구 등이 이루어질 수 있도록 하기 위함
보안 위협	사이버 위기대응 매뉴얼이 수립되지 않은 경우, 제어시스템에 사이버 침해사고 발생 시 신속한 복구 및 안정적인 운영이 어려울 수 있음
참고	※ 본 점검항목은 사이버 침해사고 발생 시 대응을 위한 매뉴얼의 문서화 여부를 확인하는 항목으로 경보 단계별 조치사항, 사고대응 및 조치 절차, 사고신고 절차 등을 포함하고 신고 및 대응을 위한 유관 기관 연락처, 제어시스템 구성요소 제조사 및 협력업체 담당자 연락처 등이 포함되어야 함
점검 대상 및 판단 기준	
대상	제어시스템 전체 및 관련 운영조직
판단 기준	**양호** : 제어시스템 운용환경에 맞는 사이버 위기대응 매뉴얼이 수립되었고, 해당 자료가 모두 최신으로 개정된 경우
	취약 : 제어시스템 운용환경에 맞는 사이버 위기대응 매뉴얼의 전부 또는 일부가 수립되지 않았거나, 해당 자료가 최신 시스템에 맞게 현행화(개정)되어 있지 않은 경우
조치 방법	제어시스템 환경에 맞는 사이버 위기대응 매뉴얼을 수립(문서화)하고 정기적 또는 주기적인 개정(현행화) 적용
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 사이버 위기대응 매뉴얼이 다음의 내용을 포함하여 수립되어 있는지 확인하고 미수립되어 있다면 해당 자료를 수립하도록 조치

- 경보 단계별 조치사항
- 사고대응 및 조치 절차
- 사고신고 절차
- 유관기관 연락처
- 제어시스템 구성요소 제조사 담당자 연락처
- 제어시스템 관련 협력업체 담당자 연락처

Step 2) Step 1) 에 따라 수립된 자료가 제어시스템 변경 등에 따라 현행화(개정)되어 있는지 점검하고 미흡한

경우 현행화하도록 조치

C-32 (상)	제어시스템 〉 7. 복구 대응
	제어시스템 대상 사이버 위기대응 훈련을 정기적으로 시행
개요	
점검 내용	제어시스템 대상 사이버 침해사고 발생 시 체계적인 대응을 위한 정기적인 사이버 위기대응 훈련 시행 여부 점검
점검 목적	비상상황에 의한 피해 파급 효과가 큰 제어시스템의 사이버 위협, 침해사고 발생 시 신속한 원인 규명, 복구 등이 이루어질 수 있도록 하기 위함
보안 위협	사이버 위기대응 훈련이 시행되지 않은 경우, 제어시스템에 사이버 침해사고 발생 시 체계적인 대응 및 신속한 복구 작업이 어려울 수 있음
참고	※ 본 점검항목은 사이버 침해사고 발생 시 대응을 위한 매뉴얼의 문서화 여부를 확인하는 항목으로 경보 단계별 조치사항, 사고대응 및 조치 절차, 사고신고 절차 등을 포함하고 신고 및 대응을 위한 유관 기관 연락처, 제어시스템 구성요소 제조사 및 협력업체 담당자 연락처 등이 포함되어야 함
점검 대상 및 판단 기준	
대상	제어시스템 관련 조직 및 운영인력 전체
판단 기준	**양호 :** 제어시스템 관련 모든 인력에 대한 사이버 위기대응 훈련계획을 수립하고 정기적으로 시행한 경우
	취약 : 제어시스템 관련 일부 인력에 대해서만 사이버 위기대응 훈련을 시행하거나 수행하지 않은 경우
조치 방법	제어시스템 관련 모든 인력에 대한 사이버 위기대응 훈련계획을 수립하고 정기적으로 훈련을 수행하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 정기적인 사이버 위기대응 훈련계획이 수립되어 있는지 확인하고 미수립되어 있다면 수립하도록 조치

Step 2) Step 1) 에 따라 수립된 계획에 따라 정기적으로 사이버 위기대응 훈련을 시행하고 훈련결과를 보고하였는지 점검하고 미흡한 경우 정기적인 훈련을 시행하도록 조치

C-33 (상)	제어시스템 〉 7. 복구 대응
	제어시스템 침해사고 대응을 위한 제어시스템 설정, 중요 데이터 등을 백업 및 관리
개요	
점검 내용	제어시스템의 장애 및 사고 발생 시 복구에 활용하기 위한 제어시스템의 설정, 중요 데이터 등 백업 및 관리 여부 점검
점검 목적	제어시스템의 장애 발생 시 복구에 필요한 중요 데이터를 백업함으로써 제어시스템의 운영 연속성을 확보하기 위함
보안 위협	제어시스템 설정 및 중요 데이터의 백업이 관리되지 않은 경우, 제어시스템에 사이버 침해사고 발생 시 신속한 복구 및 지속적인 운영이 어려울 수 있음
참고	※ 본 점검항목은 제어시스템 관련 데이터의 백업 및 관리 여부를 확인하는 항목으로 제어 I/O 포인트, 제어 로직, PC, 서버 관련 데이터, 설정 정보 등 제어시스템의 복구에 필요한 중요 정보를 백업하고 관리하는지 확인함
점검 대상 및 판단 기준	
대상	제어시스템 구성요소 전체
판단 기준	**양호 :** 제어시스템의 설정, 중요 데이터 등을 백업하여 관리하는 경우
	취약 : 제어시스템의 설정, 중요 데이터 등을 백업하지 않았거나 백업 데이터를 관리하지 않는 경우
조치 방법	제어시스템 구성요소의 설정 및 중요 데이터 등을 주기적으로 백업 및 관리하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소의 설정 및 중요 데이터에 대한 백업본이 존재하는지 확인하고 없는 경우 백업을 수행하도록 조치

Step 2) 중요 데이터에 대한 백업을 주기적으로 수행하고 있는지 확인하고 아닌 경우 주기적인 백업 작업을 수행하도록 조치

Step 3) 제어시스템 구성요소의 백업본에 중요 데이터가 모두 포함되었는지 확인하고 중요 데이터 중 빠진 것이 있으면 백업본에 포함하도록 조치

Step 4) 백업본을 안전하게 보관하고 있는지 확인하고 그렇지 않은 경우 안전하게 보관하도록 조치

C-34 (중)	제어시스템 〉 7. 복구 대응
	제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 수립
개요	
점검 내용	제어시스템의 장애, 사이버 공격, 물리적 테러 등이 발생하는 경우에 대비한 비상계획 수립 여부 점검
점검 목적	제어시스템의 장애, 사이버 공격, 물리적 테러 등이 발생하는 경우, 계획된 대응방안에 따라 적절한 조치를 하여 제어시스템을 복구하고 사회, 경제적 파급 효과 및 피해를 최소화하기 위함
보안 위협	제어시스템의 장애 등이 발생하는 상황에서 비상계획에 따른 적절한 대응 및 조치가 이루어지지 않아 제어시스템의 운영이 불가능할 수 있고 이에 따른 경제적, 사회적 손실이 발생할 위험이 존재함
참고	※ 본 점검항목은 제어시스템의 각종 장애 발생, 사이버 공격, 물리적 테러, 환경 재해 등의 모든 비상상황에 대비한 재난관리체계, 재난대응절차, 프로세스 및 장애의 종류에 따른 대응방안과 행동요령을 포함하는 것으로 이중 사이버 공격에 대한 대응은 C-16 항목에서 점검하고 있음
점검 대상 및 판단 기준	
대상	제어시스템 전체 및 관련 운영조직
판단 기준	**양호** : 제어시스템 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획이 수립되었고, 해당 자료가 모두 최신으로 개정된 경우
	취약 : 제어시스템 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획이 수립되지 않았거나 해당 자료가 최신이 아닌 경우
조치 방법	제어시스템 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획을 모두 수립(문서화)하고 정기적 또는 주기적으로 개정하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 장애, 사이버 공격, 물리적 테러 등이 발생하는 경우에 대한 비상계획이 수립되어 있는지 확인하고 비상계획이 없는 경우 수립하도록 조치

- 비상상황 발생 시 제어시스템 운영 모드 및 운영 정책
- 비상상황 발생 시 제어시스템의 중요 데이터 보호 및 복원 절차

Step 2) 수립된 비상계획에 재난대응 절차, 재난관리체계 및 관련 인력들의 행동요령 및 협업체계 등이 모두 포함되어 있는지 확인하고 빠진 부분이 있는 경우 포함하도록 조치

Step 3) 수립된 비상계획이 최신 제어시스템에 맞추어 수립되어 있는지 확인하고 그렇지 않은 경우 최신 구성요소 및 인력, 조직에 맞추어 개정하도록 조치

C-35 (중)	제어시스템 〉 7. 복구 대응
	제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행
개요	
점검 내용	제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대비한 정기적인 비상계획 훈련 실시 여부 점검
점검 목적	제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등이 발생하는 경우 수립된 비상계획에 따라 신속한 복구 및 대응을 통해 사회, 경제적 파급 효과 및 피해를 최소화하기 위함
보안 위협	비상계획 훈련을 정기적으로 실시하지 않는 경우 제어시스템의 장애 등이 발생하는 상황에서 비상계획에 따른 적절한 대응 및 조치가 이루어지지 않아 제어시스템의 운영이 불가능할 수 있고 이에 따른 경제적, 사회적 손실 발생이 발생할 위험이 존재함
참고	※ 본 점검항목은 제어시스템 장애 발생 시 대응 및 복구를 위한 훈련계획의 수립과 시행 여부를 확인하는 항목으로, 정기적인 훈련계획을 수립하여 정보보호 책임자가 승인하고 시행해야 함 ※ 비상계획 훈련은 제어시스템 운전원, 제어시스템 관리자, 유지보수 인력, 전담 보안 인력 등 제어시스템 운영과 관련된 인력 전체를 훈련 참여 대상으로 함
점검 대상 및 판단 기준	
대상	제어시스템 관련 운영조직 전체
판단 기준	**양호** : 제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행하는 경우
	취약 : 제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행하지 않는 경우
조치 방법	제어시스템 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련계획을 수립하고 계획에 따라 정기적으로 비상계획 훈련을 시행하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 장애, 사이버 공격, 물리적 테러 등이 발생하는 경우에 대비한 비상계획 훈련이 정기적으로 실시되는지 확인하고 그렇지 않은 경우 정기적인 비상계획 훈련을 실시하도록 조치

Step 2) 비상계획 훈련이 제어시스템 운전원, 관리자, 유지보수 인력 등 제어시스템 운영과 관련된 모든 인력을 대상으로 하여 실시되는지 확인하고 그렇지 않은 경우 관련 인력을 모두 포함하여 실시하도록 조치

C-36 (중)	제어시스템 〉 7. 복구 대응
	제어시스템 조작 불능에 대비하여 수작업 운전 매뉴얼 작성 및 교육 훈련 시행
개요	
점검 내용	제어시스템의 조작 불능에 대비한 수작업 운전 매뉴얼 작성 및 이에 대한 교육 훈련 시행 여부 점검
점검 목적	제어시스템 조작에 문제가 발생하는 경우에 대비한 수작업 운전 매뉴얼을 구비하고 정기적으로 교육 훈련을 실시하여 제어시스템의 조작 불능 시에도 매뉴얼에 따라 제어시스템 가용성을 확보하기 위함
보안 위협	수작업 운전 매뉴얼이 없는 경우 제어시스템의 조작 불능 상황 발생 시 적절한 대응 및 조치가 이루어지지 않아 제어시스템의 지속적인 운영이 불가능할 수 있음
참고	※ 본 점검항목은 제어시스템의 조작 불능에 대비한 수작업 운전 매뉴얼 작성 및 이에 대한 정기적인 교육을 실시하는지 확인하는 것으로, 수작업 운전 매뉴얼은 장애 등으로 인해 제어시스템의 자동 제어가 불가능한 경우 수작업 전환에 대비하여 작성 사이버 위기대응 훈련 또는 비상계획 훈련에서 수작업 운전 훈련을 병행하는 경우 이를 수작업 운전 훈련으로 간주함
점검 대상 및 판단 기준	
대상	제어시스템 전체 및 관련 운영조직
판단 기준	**양호** : 제어시스템 조작 불능에 대비한 수작업 운전 매뉴얼을 작성하고 정기적으로 수작업 운전 교육 훈련을 시행하는 경우
	취약 : 제어시스템 조작 불능에 대비한 수작업 운전 매뉴얼을 작성하지 않았거나 정기적으로 수작업 운전 교육 훈련을 시행하지 않는 경우
조치 방법	제어시스템 조작 불능에 대비한 수작업 운전 매뉴얼을 작성하고 정기적으로 수작업 운전 교육 훈련을 시행하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템의 조작 불능에 대비한 수작업 운전 매뉴얼이 작성되었는지 확인하고 없는 경우 수작업 운전 매뉴얼을 작성하도록 조치

Step 2) 제어시스템의 수작업 운전에 대한 교육 및 훈련을 정기적으로 실시하는지 확인하고 그렇지 않은 경우 정기적인 교육 훈련을 시행하도록 조치

C-37 (하)	제어시스템 〉 7. 복구 대응
	제어시스템의 각종 이벤트에 대한 로그를 관리하기 위한 중앙집중식 로그관리 수행
개요	
점검 내용	제어시스템의 각종 이벤트를 관리할 수 있는 중앙집중식 로그관리 수행 여부 점검
점검 목적	중앙집중식 로그관리를 통해 제어시스템의 사고 발생 상황 시 사고 원인 파악 및 분석에 활용하여 유사 사고를 방지하기 위함
보안 위협	로그가 중앙집중식으로 관리되지 않는 경우 침해사고 발생 시 원인 파악 및 대응책 마련에 시간이 소요되어 유사한 사고가 반복하여 발생할 위험이 존재함
참고	※ 사고 발생 시 신속한 원인 분석을 위해 다음의 로그 정보 수집 및 중앙집중식 관리가 필요함 - 제어시스템 내 구성요소의 운영체제 이벤트 로그 - 네트워크 및 보안 장비 로그 - PLC, DCS 등의 제어 H/W와 EWS, HMI등의 제어를 위한 제어 S/W 관련 감사 로그 - 이상 트래픽 탐지, 백신, 미디어 통제 등의 보안 이벤트 로그
점검 대상 및 판단 기준	
대상	제어시스템 전체
판단 기준	**양호 :** 중앙집중식 로그관리 체계를 구축하여 제어시스템의 로그를 관리하는 경우
	취약 : 중앙집중식 로그관리 체계를 구축하지 않은 경우
조치 방법	중앙집중식 로그관리 체계를 구축하여 제어시스템의 로그를 관리하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템의 이벤트를 집중하여 관리할 수 있는 중앙집중식 로그관리 시스템을 구축하였는지 확인하고 없는 경우 제어시스템의 로그를 통합하여 관리할 수 있는 시스템을 구축하여 운영하도록 조치

C-38 (하)	제어시스템 〉 7. 복구 대응
	제어시스템 구성요소의 기준 형상을 설정하고 변경 및 업데이트 시 형상관리 수행
개요	
점검 내용	제어시스템 구성요소 각각의 기준 형상이 설정되어 있고 업데이트 또는 설정 변경이 발생하는 경우 형상관리 수행 여부 점검
점검 목적	제어시스템의 기준 형상을 설정하고 최신 형상을 지속적으로 관리하여 제어시스템의 장애, 고장 등이 발생하는 경우 복구에 활용하기 위함
보안 위협	형상관리가 이루어지지 않은 경우, 제어시스템의 재설정이 필요한 고장 또는 장애 발생 시 안정적인 제어시스템 운영이 되지 않을 수 있음
참고	※ 형상관리는 제어시스템 모든 구성요소(PLC, DCS, OWS, 네트워크 스위치, SCADA 서버 등)의 하드웨어 및 소프트웨어(OS, 미들웨어, 응용프로그램 등) 변경, 소프트웨어 버전 변경, 설정 변경, 네트워크 변경, 제어시스템 구성 변경, IP/MAC 주소의 변경, 패치 및 업데이트 등의 각종 제어시스템 형상변경에 모두 적용되어야 함
점검 대상 및 판단 기준	
대상	제어시스템 구성요소 전체
판단 기준	**양호 :** 제어시스템 구성요소의 기준 형상을 수립하고 업데이트 시 형상관리를 수행하는 경우
	취약 : 제어시스템 구성요소의 기준 형상이 없거나 업데이트 시 형상관리가 이루어지지 않는 경우
조치 방법	제어시스템 구성요소의 기준 형상을 수립하고 업데이트 시 형상관리를 수행하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템의 모든 구성요소(PLC, DCS, OWS, SCADA 서버, 네트워크 스위치 등)에 대한 기준 형상이 수립되어 있는지 확인하고 없는 경우 기준 형상을 문서화하도록 조치

- 장비의 설치 소프트웨어 및 버전
- 장비의 사용 서비스 및 포트
- 장비의 네트워크 및 보안 설정
- 장비의 로그 설정
- 장비의 네트워크 정책
- 이외의 장비별 주요 형상 정보

Step 2) 제어시스템 구성요소의 업데이트 또는 설정 변경 시 형상관리가 이루어지는지 확인하고 그렇지 않은

경우 형상관리를 수행하도록 조치

C-39 (히)	제어시스템 〉 7. 복구 대응
	제어시스템 주요 장비 및 제어 네트워크 장비에 대해 이중화
개요	
점검 내용	제어시스템의 주요 장비 및 제어 네트워크 장비의 이중화 여부 점검
점검 목적	제어시스템의 주요 장비를 이중화하여 하나의 구성요소에서 장애가 발생하는 경우에도 제어시스템을 지속적으로 운용하기 위함
보안 위협	주요 장비가 이중화되어 있지 않은 경우, 해당 장비에 문제가 발생하면 제어시스템의 가용성에 문제가 발생할 위험이 존재함
참고	※ 본 점검항목은 제어시스템의 주요 장비 및 제어 네트워크 장비의 이중화를 확인하는 항목으로 제어시스템의 주요 장비는 제어를 위한 SCADA 서버, 컨트롤러 기능을 하는 DCS, PLC 등의 제어 H/W, 운영을 위한 HMI 등 핵심 운영과 관련된 장비를 기준으로 하여 선정함
점검 대상 및 판단 기준	
대상	제어시스템의 주요 장비 및 제어 네트워크 장비
판단 기준	**양호 :** 제어시스템의 주요 장비 및 제어 네트워크 장비에 대해 이중화되어 있는 경우
	취약 : 제어시스템의 주요 장비 및 제어 네트워크 장비에 대해 이중화되어 있지 않은 경우
조치 방법	제어시스템의 주요 장비 및 제어 네트워크 장비에 대해 이중화하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템의 주요 장비(예: 핵심 운영과 관련된 DCS, PLC 컨트롤러, HMI, SCADA 등)를 식별하여 모두 이중화하였는지 확인하고 그렇지 않은 경우 이중화하도록 조치

[제어 H/W 이중화 및 3중화 예시]

Step 2) 제어 네트워크 장비가 이중화되었는지 확인하고 그렇지 않은 경우 이중화하도록 조치

C-40 (하)	제어시스템 〉 7. 복구 대응
	제어시스템 보호를 위한 화재탐지 설비 및 화재 진압설비를 구비
개요	
점검 내용	제어시스템을 보호하기 위한 화재탐지 설비 및 화재 진압설비 구비 여부 점검
점검 목적	제어시스템 설치 장소에 화재가 발생하는 경우 신속한 탐지 및 진압을 통해 운용 지속성 및 가용성을 확보하기 위함
보안 위협	화재탐지 및 진압이 신속히 되지 않는 경우 제어시스템의 운영 장애가 발생할 위험이 존재함
참고	-
점검 대상 및 판단 기준	
대상	제어시스템 설치 장소 전체
판단 기준	**양호 :** 제어시스템 설치장소에 화재탐지 및 화재 진압설비가 구축된 경우
	취약 : 제어시스템 설치장소에 화재탐지 및 화재 진압설비가 구축되지 않은 경우
조치 방법	제어시스템 설치장소에 화재탐지 및 화재 진압설비 설치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 설치 장소에 화재탐지 설비와 화재 진압설비가 구축되어 있는지 확인하고 없는 경우 구비하도록 조치

[연기감지기 예시]

[화재진화기 예시]

[CO2 소화기 예시]

C-41 (하)	제어시스템 〉 7. 복구 대응
	제어시스템 보호를 위한 누수탐지 설비 및 침수 대응 장비 구비
개요	
점검 내용	제어시스템을 보호하기 위한 누수탐지 설비 및 침수 대응 장비 구비 여부 점검
점검 목적	제어시스템 설치장소에 누수 발생 시 신속한 탐지 및 대응을 통해 운용 지속성 및 가용성을 확보하기 위함
보안 위협	누수탐지 및 대응이 신속히 되지 않는 경우 제어시스템의 침수 등에 의해 운영 장애가 발생할 위험이 존재함
참고	-
점검 대상 및 판단 기준	
대상	제어시스템 설치장소 전체
판단 기준	**양호 :** 제어시스템 설치장소에 누수탐지 및 침수 대응 장비가 구축된 경우
	취약 : 제어시스템 설치장소에 누수탐지 및 침수 대응 장비가 구축되지 않은 경우
조치 방법	제어시스템 설치장소에 누수탐지 및 침수 대응 장비 구비
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 설치 장소에 누수, 침수 등의 탐지설비를 구축하고 있는지 확인하고 없는 경우 구비하도록 조치

[누수알람시스템 예시]

Step 2) 제어시스템 설치 장소에 침수 시 대응을 위한 방수포, 배수펌프 등이 구비되어 있는지 확인하고 없는 경우 구비하도록 조치

C-42 (하)	제어시스템 〉 7. 복구 대응
	제어시스템에 대하여 정기적으로 사이버 위험 시나리오를 식별하고, 완화방안 수립
개요	
점검 내용	제어시스템의 사이버 위험 시나리오 정기적 식별 및 이를 완화하기 위한 대책 수립 여부 점검
점검 목적	제어시스템에 대한 새로운 사이버 위험 시나리오를 정기적으로 식별하고 완화방안을 수립하여 매년 증가하고 있는 제어시스템 대상의 사이버 위협에 대응하기 위함
보안 위협	제어시스템에 대한 최신 공격 기법에 대한 완화방안을 적용하지 않은 경우, 최신 사이버 공격 및 위협에 취약할 수 있음
참고	※ **제어시스템 사이버 공격 기법:** 제어시스템이 점차 발전하고 고도화됨에 따라 다양한 기기들과의 연결접점이 증가하고 제어시스템 구성요소들의 취약점이 지속적으로 공개됨에 따라 사회적인 파급효과가 큰 제어시스템을 대상으로 하는 공격은 점차 증가하고 있음
점검 대상 및 판단 기준	
대상	제어시스템 전체
판단 기준	**양호 :** 제어시스템의 사이버 위험 시나리오를 정기적으로 식별하고 완화방안을 수립한 경우
	취약 : 제어시스템의 사이버 위험 시나리오 및 완화방안을 정기적으로 수립하지 않는 경우
조치 방법	제어시스템의 사이버 위험 시나리오를 정기적으로 식별하고 완화방안을 수립하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 운영 중인 제어시스템 기능, 환경에 초점을 맞춘 각종 보안위협 및 사이버 위험 시나리오를 식별하고 이를 완화하기 위한 대책을 수립하였는지 확인하고 그렇지 않은 경우 사이버 공격 완화방안을 마련하도록 조치

Step 2) 수립한 사이버 위험 시나리오 및 완화방안을 정기적으로 업데이트하는지 확인하고 그렇지 않은 경우 정기적으로 위험 시나리오 식별 및 완화방안을 업데이트하도록 조치

C-43 (상)	제어시스템 〉 8. 보안 관리
	제어시스템 구성요소에 대한 자산정보(담당자, 제조사, 모델명, 펌웨어 버전, 설치 SW 등)를 항상 최신으로 유지관리
개요	
점검 내용	제어시스템 구성요소에 대한 자산정보(담당자, 제조사, 모델명, IP주소, 펌웨어 버전, 설치 SW 등) 문서화 및 최신 시스템 구성에 맞는 유지관리 실시 여부 점검
점검 목적	비상상황에 의한 피해 파급 효과가 큰 제어시스템의 사이버 위협, 침해사고 발생 시 신속한 원인 규명, 복구 등이 이루어질 수 있도록 하기 위함
보안 위협	제어시스템의 현황, 네트워크 구성 등이 현행화되지 않아 장애 및 시스템 장애 발생 시 신속한 복구 및 지속적인 운영이 어려울 수 있음
참고	※ 본 점검항목은 자산정보의 문서화와 개정(현행화) 여부를 확인하는 항목이며, 제어시스템의 구성 변경 및 최신 보안위협 등에 따른 펌웨어 업데이트 등 자산의 변경이 발생할 때마다 해당 시점에서 개정 작업을 해야 함
점검 대상 및 판단 기준	
대상	제어시스템 전체 및 관련 운영조직
판단 기준	**양호** : 제어시스템 자산정보 자료가 존재하고 해당 자료가 모두 최신 제어시스템 구성요소 정보와 일치하는 경우
	취약 : 제어시스템 자산정보 자료의 전부 또는 일부가 존재하지 않거나, 작성된 자료의 전부 또는 일부가 현행화(개정)되지 않은 경우
조치 방법	제어시스템 자산정보를 모두 문서화하고 정기적 또는 주기적으로 현행화(개정)하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소의 자산정보 자료가 존재하는지 확인하고 확인되지 않는 경우 해당 자료를 작성하도록 조치

Step 2) Step 1)에 따라 확인된 자산정보 자료가 제어시스템 변경 등에 따라 개정되어 있는지 다음 각 호의 사항을 고려한 점검을 수행하고 미흡한 경우 현행화하도록 조치

- 제어설비가 위치한 곳을 실사하여 최신 자산정보 자료와 실제 제어시스템이 현재 구성된 현황과 일치하는지 확인

※ 자산정보 자료는 제어시스템 구성요소 전체(PLC, DCS 컨트롤러, RTU, OWS, EWS, HSR, 서버, 네트워크 장치, 방화벽, UTM 등)에 대한 담당자, 제조사, 모델명, IP주소, 펌웨어 버전, 설치 SW 등의 정보를 포함한 자산정보 목록과 네트워크 구성도 등을 포함

C-44 (상)	제어시스템 〉 8. 복구 대응
	제어시스템 중요 구성요소가 설치된 장소를 보호구역으로 설정
개요	
점검 내용	제어시스템 중요 구성요소가 설치된 장소(통제센터, 서버실, 기계실 등) 보호구역 설정 여부 점검
점검 목적	제어시스템 중요 구성요소가 설치된 구역을 보호구역으로 지정하여 허가받지 않은 사용자의 제어시스템에 대한 물리적 접근 경로를 차단하기 위함
보안 위협	허가받지 않은 사용자가 제어시스템 중요 구성요소에 접근할 수 있는 경우 물리적 접근을 통해 악성코드 설치, 제어시스템 오동작, 시스템 정지 등의 보안위협이 발생할 위험이 존재함
참고	※ 통제구역은 출입문을 제외하고는 외부와 완전히 차단되어 출입통제장치를 통해 출입자 식별 및 인증을 수행하여 허가받은 사람만 출입하도록 관리해야 함 ※ 본 항목은 P-15 항목과 중복되는 내용이 있으나 장애 발생 시 파급 효과가 큰 제어시스템의 운영 특성을 고려하여 제어시스템 설치장소를 대상으로 "상" 항목으로 점검
점검 대상 및 판단 기준	
대상	제어시스템 설치장소
판단 기준	**양호 :** 제어시스템 구성요소가 설치된 장소가 모두 보호구역으로 설정된 경우
	취약 : 제어시스템 구성요소가 설치된 장소의 일부 또는 전체가 보호구역이 아닌 경우
조치 방법	제어시스템 구성요소가 설치된 장소를 보호구역으로 지정하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템이 설치된 구역을 보호구역으로 설정하고 출입통제장치를 통해 출입자 식별·인증을 수행하고 있는지 확인하고 그렇지 않은 경우 보호구역으로 지정하고 출입자를 통제할 수 있는 방안을 수립하도록 조치

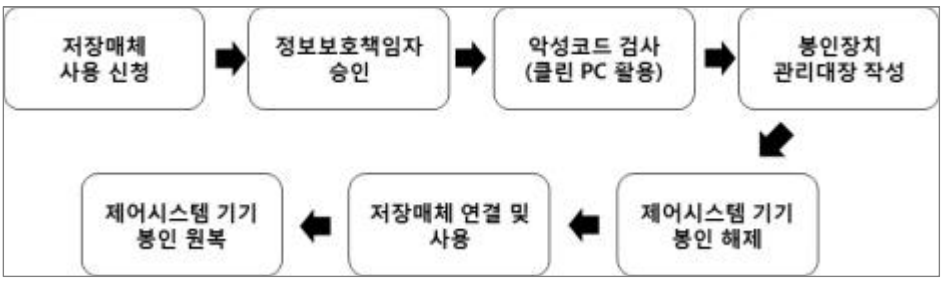
※ 원격지에 분산 배치된 소규모 무인 제어시스템이나 현장장치에 대해 보호구역 지정 및 출입자 통제가 어려운 경우, 점검에서 제외하고 제어시스템 구성요소에 대해 물리적 접근을 통제할 수 있는 보완대책 마련

C-45 (상)	제어시스템 〉 8. 보안 관리
	제어시스템에서 USB 등 이동형 저장 매체를 사용해야 하는 경우, 사전 정의된 정책에 따라 사용
개요	
점검 내용	제어시스템에서 USB 등의 이동형 저장 매체를 사용해야 하는 경우, 사전에 정의된 정책에 따른 사용 여부 점검
점검 목적	제어시스템에 USB 등의 이동형 저장 매체를 사용해야 하는 경우 사전 승인절차 및 안전한 저장 매체만 연결하도록 하는 등의 통제 정책을 사용하여 악성코드 감염 등의 위협을 차단하기 위함
보안 위협	• 제어시스템에 안전하지 않은 USB 등의 이동형 저장 매체 연결 시 악성코드 감염이 이루어지고 이를 통해 제어시스템의 장애 또는 정지 등의 피해가 발생할 위험이 존재함 • **위협 사례:** 스턱스넷(Stuxnet) - 이동형 저장 매체 자동실행 기능이 비활성화되어 있는 PC 환경에서 감염 및 전파를 하기 위해 MS10-046, CVE-2010-2568 등의 취약점(LNK 파일에 대한 윈도우 쉘 아이콘 처리자 취약점)을 이용 - 스턱스넷(Stuxnet)에 감염된 USB를 아직 감염되지 않은 PC에 연결하여 USB 내의 파일과 디렉터리를 검색하기 위해 브라우저 창이 열리는 순간 이동형 저장 매체상에 있는 DLL 파일을 실행하여 해당 PC 감염 05/20/2010 10:35 AM 4,171 Copy of Copy of Copy of Copy of Shortcut to.lnk 05/20/2010 10:35 AM 4,171 Copy of Copy of Copy of Shortcut to.lnk 05/20/2010 10:35 AM 4,171 Copy of Copy of Shortcut to.lnk 05/20/2010 10:35 AM 4,171 Copy of Shortcut to.lnk 05/20/2010 10:35 AM 517,632 ~WTR4132.tmp 05/20/2010 10:35 AM 25,720 ~WTR4141.tmp [스턱스넷(Stuxnet)에 감염된 이동형 저장 매체(USB 메모리) 내의 디렉터리 목록]
참고	※ **제어시스템 내 이동형 저장 매체 사용통제 정책** - USB 등의 이동형 저장 매체는 제어시스템에 연결이 불가하도록 조치하는 것이 원칙임 - 이동형 저장 매체의 사용이 불가피한 경우, 사전에 인가된 저장 매체를 활용하고 해당 저장 매체의 사용 승인절차와 안전조치(예시: 사용 전, 사용 후 악성코드 감염 여부 검사)가 적용되도록 하는 통제절차 필요
점검 대상 및 판단 기준	
대상	제어시스템을 구성하는 서버, PC 등 이동형 저장 매체가 연결 가능한 시스템
판단 기준	**양호 :** 이동형 저장 매체 통제 정책을 수립하고 이동형 저장 매체 사용 시 수립된 정책에 따르는 경우
	취약 : 이동형 저장 매체 통제 정책을 수립하지 않았거나 이동형 저장 매체 사용 시 수립된 정책에 따르지 않는 경우
조치 방법	이동형 저장 매체에 대한 사용통제 정책을 수립하고 불가피한 경우 정책에 따라 사용하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 불가피하게 이동형 저장 매체를 사용해야 하는 경우를 위한 사용통제 정책이 수립되어 있는지 확인하고 미수립되어 있다면 해당 정책을 수립하도록 조치



[저장 매체 사용 통제절차 예시]

Step 2) 불가피하게 이동형 저장 매체를 사용해야 하는 경우, Step 1) 에서 정의한 정책에 따라 휴대용 저장 매체 사용을 관리하고 있는지 확인하고 미흡한 경우 정의된 정책에 따라 사용하도록 조치

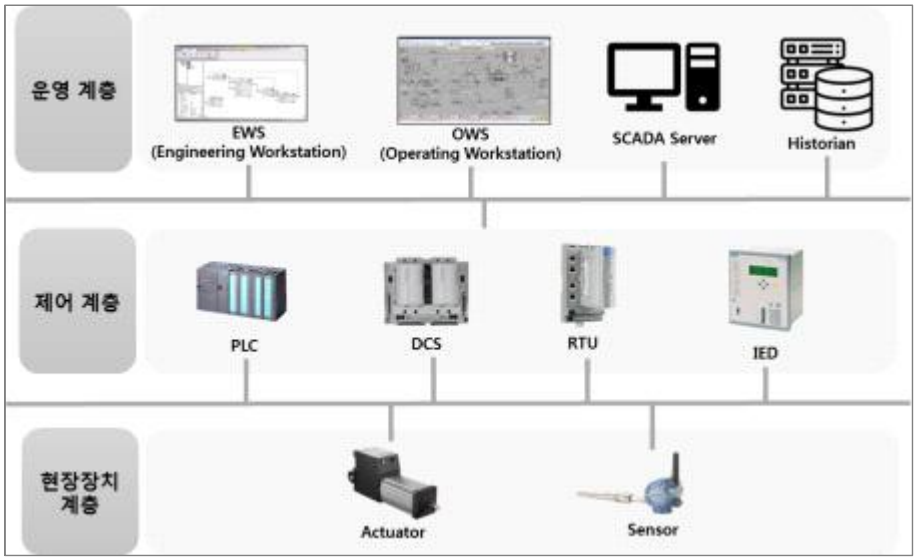
C-46 (상)	제어시스템 〉 8. 복구 대응
	제어 네트워크에 연결되는 외부 정보통신기기 반·출입 시 클린존 통과, 관리대장 작성 등 관리절차 마련
개요	
점검 내용	제어 네트워크에 연결되는 외부 정보통신기기의 반출·입 시 클린존 통과, 관리대장 작성 등의 관리절차 마련 여부 점검
점검 목적	제어 네트워크에 승인받은 안전한 정보통신기기만 반·출입 되도록 하는 통제 정책을 적용하여 제어 네트워크에 통제되지 않은 기기의 접근을 차단하기 위함
보안 위협	안전하지 않은 외부 정보통신기기가 반출·입 되는 경우 네트워크 정보유출 또는 악성코드 감염의 가능성이 있으며 이를 통해 제어시스템의 사이버 공격, 장애 또는 정지 등의 피해가 발생할 위험이 존재함
참고	※ 외부 정보통신기기는 제어 네트워크에 연결이 불가하도록 조치하는 것이 원칙이나 사용이 불가피한 경우에는 사전 사용 승인절차와 안전조치를 포함한 반출·입 절차(예시: 사용 전 악성코드 감염 여부 검사, 사용 후 민감한 정보 저장 여부 확인 등)를 통해 관리해야 함
점검 대상 및 판단 기준	
대상	제어 네트워크와 연결되는 모든 외부 정보통신기기
판단 기준	**양호** : 외부 정보통신기기 반·출입 시 클린존 통과, 반입 및 반출 장비에 대한 관리대장 작성 등의 관리절차를 수립하여 해당 절차에 따르는 경우
	취약 : 외부 정보통신기기 반·출입을 위한 관리절차를 마련하지 않은 경우
조치 방법	외부 정보통신기기 반·출입 시 클린존 통과, 반입 및 반출 장비에 대해 관리대장 작성 등의 관리절차를 수립하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어 네트워크에 연결되는 외부 정보통신기기 반출·입 시 다음의 내용을 포함한 관리절차가 수립되어 있는지 확인하고 수립되지 않은 경우 절차를 수립하도록 조치

- 클린존에서 외부 정보통신기기 통제조치 시행
- 외부 정보통신기기 반출·입 대장 기록 및 관리
- 일련번호 등의 식별번호를 활용한 외부 정보통신기기 반출·입 신청 및 승인
- 반입 시 초기화 수행 및 악성코드 존재 여부 확인
- 반출 시 제어시스템 관련 민감 정보 수록 여부 확인

C-47 (중)	제어시스템 〉 8. 복구 대응
	제어시스템의 특성을 반영한 정보보안 정책, 지침을 수립
개요	
점검 내용	제어시스템의 특성을 반영한 정보보안 정책 및 지침 수립 여부 점검
점검 목적	제어시스템에 특화된 정보보안 지침을 수립하여 제어시스템 보안 관리 주체를 지정하고, 제어시스템에 특화된 관리적·물리적·기술적 보안을 체계적으로 관리하기 위함
보안 위협	일반 IT시스템 중심의 보안 관리 이외에 제어시스템에 특화된 보안 관리 요소, 취약점 조치 등이 누락되어 운영인력의 부주의(Human Error) 또는 운영상의 취약점을 악용한 사이버 침해위협이 발생할 위험이 존재함
참고	※ **제어시스템 특성** - EWS, OWS, Historian 등의 제어 S/W가 포함된 운영계층, PLC, DCS, RTU, IED 등의 제어 H/W로 구성되는 제어 계층, 액추에이터, 센서 등이 포함된 현장장치 계층으로 구성됨 - 제어시스템 보안의 경우 일반 IT시스템과 달리 가용성 측면이 가장 중요하게 고려되어야 함 - 제어시스템의 경우 각자 특화된 시스템 및 기기로 구성되고 일반적인 IT시스템의 보안 기능과 우선순위에 차이점이 있으므로 제어시스템을 위한 별도의 관리적, 기술적인 정책과 지침이 필요  [제어시스템 운영환경]
점검 대상 및 판단 기준	
대상	제어시스템 정보보안 정책 및 지침
판단 기준	**양호 :** 제어시스템의 특성을 반영한 정보보안 정책 및 지침이 별도로 수립된 경우
	취약 : 제어시스템의 특성을 반영한 정보보안 정책 및 지침이 별도로 수립되지 않은 경우
조치 방법	제어시스템의 특성을 반영한 정보보안 정책 및 지침을 수립
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템에 대한 보안 관리 주체와 역할, 제어시스템에 대한 접근통제 및 운영 보안 등을 포함하는 제어시스템 정보보안지침이 별도 존재하는지 확인하고 존재하지 않는다면 제어시스템 정보보안지침을 수립

제 1 장 총 칙
제1조 (목적)
제2조 (적용범위)
제3조 (정의)
제 2 장 제어보안 관리체계에 대한 활동
제4조 (활동방향)
제5조 (제어보안책임자 및 제어보안담당자)
제6조 (제어보안담당자 임무)
제7조 (취약점 진단 및 보호대책 수립)
제8조 (제어보안 교육)
제9조 (긴급사태 관리)
제10조 (제어망 운영)
제11조 (보안관리 절차 수립)
제12조 (통제구역)
제13조 (백신 프로그램 운영)
제14조 (휴대용 저장매체 사용통제)
제15조 (유지보수 통제 및 기록 관리)
제16조 (원격 유지보수 제한)
제17조 (보안성 검토 및 보안적합성 검증)
제18조 (자료관리)
제19조 (계약사항)
제 3 장 보 칙

[제어시스템 정보보안지침 예시]

※ 제어시스템 정보보안지침의 목차 및 세부 내용은 제어시스템을 관리하는 조직에 따라 다를 수 있으나, 제어시스템에 대한 기반시설 취약점 점검항목(총 50개)을 고려하여 그 내용이 포함되도록 함

C-48 (중)	제어시스템 〉 8. 복구 대응
	제어시스템 운영 업무에 대해 표준업무 절차서를 작성하고 적용
개요	
점검 내용	제어시스템의 운영 업무에 대해 표준업무 절차서 작성 및 적용 여부 점검
점검 목적	제어시스템의 운영 업무를 표준 절차에 따라 진행하여 운영자의 숙련도, 부주의나 실수에 따른 위험을 최소화하고 제어시스템의 안정적인 운영을 수행하기 위함
보안 위협	제어시스템 운영에 대한 표준업무절차가 문서화되지 않는 경우 숙련되지 않은 운영자의 부주의나 실수에 의해 제어시스템의 장애 또는 오동작이 발생할 위험이 존재함
참고	※ 본 점검항목은 제어시스템의 조작 및 운영 업무절차의 문서화 여부를 확인하는 항목으로 제어시스템의 구성 변경, 정책에 따른 조직 및 업무절차 변경 등이 발생하는 경우 개정 작업이 필요함
점검 대상 및 판단 기준	
대상	제어시스템 관련 운영조직
판단 기준	**양호 :** 제어시스템 운영 업무에 대해 표준업무 절차서가 작성되었고, 해당 자료가 모두 최신으로 개정된 경우
	취약 : 제어시스템 운영 업무에 대해 표준업무 절차서의 전부 또는 일부가 작성되지 않았거나, 절차서의 전부 또는 일부가 현행화(개정)되어 있지 않은 경우
조치 방법	제어시스템 운영 업무에 대해 표준업무절차를 모두 문서화하고 정기적 또는 주기적으로 개정(현행화)하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템의 운영 업무에 대한 표준업무 절차서가 작성되어 있는지 확인하고 그렇지 않은 경우 해당 자료를 작성하도록 조치

Step 2) Step 1) 에 따라 작성된 자료가 제어시스템 변경 등에 따라 현행화(개정)되어 있는지 점검을 수행하고 미흡한 경우 현행화하도록 조치

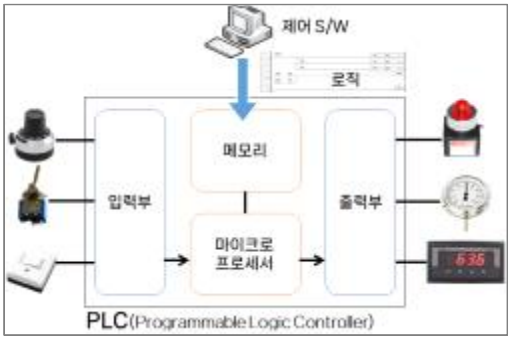
C-49 (하)	제어시스템 〉 8. 보안 관리
	제어시스템 유지보수를 위한 전용 장비(노트북 등)를 마련하고 관련 정책을 시행
개요	
점검 내용	제어시스템 유지보수를 위한 전용 장비(노트북, PC 등)를 마련하고 이를 안전하게 관리하기 위한 관련 정책 수립 및 시행 여부 점검
점검 목적	제어시스템 유지보수 사유로 외부에서 관리되지 않은 장비를 반입함으로써 발생하는 위협을 차단하기 위함
보안 위협	외부에서 악성코드가 감염된 기기, 서버 및 노트북 등을 제어시스템 유지보수를 위해 연결하는 경우 제어시스템의 장애 및 오동작이 발생할 위험이 존재함
참고	※ 제어시스템은 지정·관리하는 유지·관리용 전용 장비로만 유지보수를 수행하는 것을 원칙으로 하되 부득이한 사유로 유지보수 업체의 장비나 저장 매체를 활용하여 유지·관리를 수행하는 경우 반·출입 시 철저한 통제 및 보안 조치를 수행해야 함
점검 대상 및 판단 기준	
대상	제어시스템 관련 운영조직
판단 기준	**양호** : 제어시스템 구성요소의 유지보수 전용 장비를 별도로 마련하고 이를 안전하게 관리하기 위한 정책을 수립·시행하는 경우
	취약 : 제어시스템 구성요소의 유지보수 전용 장비를 별도로 마련하지 않았거나 유지보수용 장비를 안전하게 관리하기 위한 정책이 수립되지 않은 경우
조치 방법	제어시스템 구성요소의 유지보수 전용 장비를 별도로 마련하고 이를 안전하게 관리하기 위한 정책을 수립하여 시행하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 구성요소의 유지보수를 위한 전용 장비를 확인하고 해당 장비가 없는 경우 유지보수 전용 장비를 마련하도록 조치

Step 2) 제어시스템 유지보수 전용 장비의 안전한 관리 정책을 수립하여 시행하는지 확인하고 미흡한 경우 유지보수 전용 장비의 안전한 관리 정책을 수립하고 시행하도록 조치

C-50 (상)	제어시스템 〉 8. 보안 관리
	허가에 의한 로직 변경 정책 수립
개요	
점검 내용	제어기기의 로직 변경에 대한 사전 검토 및 허가를 포함하는 로직 변경 정책 수립 및 이행 여부 점검
점검 목적	내부자(현장 엔지니어, 유지보수 작업자)에 의해서 검증되지 않은 로직이 제어기기에 다운로드 시 발생할 수 있는 제어시스템 오동작 문제를 차단하고, 제어기기의 세밀한 형상관리를 통해 제어시스템의 안정성 및 운영 영속성을 보장하기 위함
보안 위협	• 제어기기 로직은 단일 제어기기는 물론 제어시스템 전체에 영향을 끼치므로 안전성이 검증되지 않은 로직의 오작동은 전체 제어시스템의 예기치 않은 동작을 유발할 위험이 존재함 • 제어기기 로직의 오류는 시스템의 중단을 일으키거나 제어 공정의 변경을 통해서 물리적 피해를 유발할 위험이 존재함 • **위협 사례:** 2010년에 발견된 스턱스넷(stuxnet)은 이란의 나탄즈(Natanz) 원자력 시설을 공격하였으며, 일련의 단계를 거쳐 시설 내 제어기기(PLC)의 로직을 변경하였고, 이를 통해서 원심분리기의 속도를 비정상적으로 조절할 수 있었으며, 결국 일부 원심분리기의 물리적 파손을 유발함
참고	※ **제어기기 로직:** 프로그래머블 로직 컨트롤러(PLC), 분산 제어시스템(DCS) 컨트롤러 등의 동작을 제어하고 조정하기 위한 일련의 논리적 명령 집합이며, PLC 및 DCS 컨트롤러는 센서 및 입력 장치로부터 수신한 데이터를 처리하여 로직에 따라 출력을 발생하고 이를 통해 현장의 액추에이터를 동작하게 함  [PLC 동작 구조]
점검 대상 및 판단 기준	
대상	PLC, DCS 컨트롤러 등 로직에 의해서 동작하는 제어시스템 구성요소 전체
판단 기준	**양호 :** 로직 변경 정책이 수립되어 있고, 정책에 변경 로직에 대한 사전 검토 및 승인 후 변경하도록 절차가 마련되어 있으며, 절차를 정확히 이행하는 경우
	취약 : 로직 변경 정책이 수립되어 있지 않거나, 정책이 수립되어 있더라도 변경 로직에 대한 사전 검토 및 승인절차가 포함되어 있지 않거나, 정책이 바르게 수립되어 있더라도 시행하지 않고 있는 경우
조치 방법	로직 변경 시 변경할 로직에 대해서 사전 검토 및 승인 후 변경할 로직을 적용하는 절차가 포함된 로직 변경 정책을 수립하고 문서화하며, 수립된 정책에 명시된 절차에 따라 실제 변경을 수행하도록 관리
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어기기 로직 변경 정책 문서에 사전 검토 및 승인 후 설치 절차가 포함되어 있는지 확인

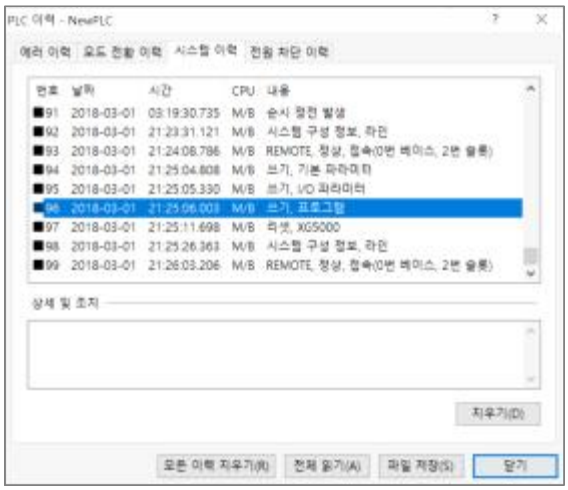
- 제어기기 로직 변경 정책은 별도 문서로 관리하지 않고 조직의 보안 정책에 포함하여 관리할 수 있음

Step 2) 제어기기 로직 변경 시 정책에 명시된 절차를 준수하는지 확인

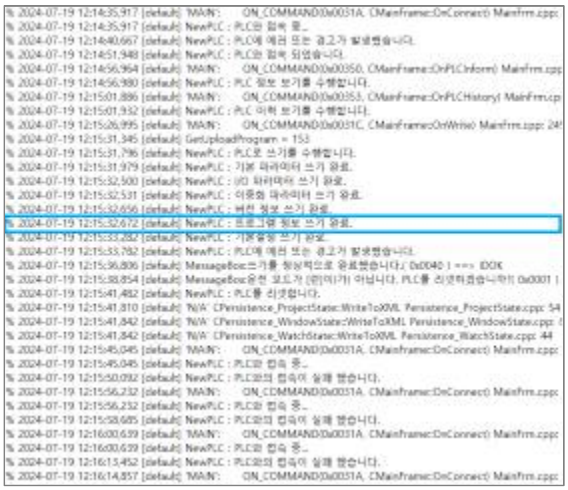
- 변경 예정 로직의 검토 결과 문서 확인
- 제어기기의 로직 변경 허가와 관련한 내부 문서 확인

※ 제어기기 로직 변경 여부 확인 예시

- 제어기기 로직 변경 여부를 시스템에서 확인하고자 할 경우, 제어 S/W 또는 제어기기의 로그에서 프로그램 다운로드와 관련한 로그를 확인하여 파악할 수 있음



[제어 S/W를 통한 제어기기의 로그 확인 예시]



[제어 S/W의 로그 확인 예시]

C-51 (하)	제어시스템 〉 9. 교육훈련
	제어시스템 운전원, 관리자, 유지보수인력, 보안 인력에 대해 직무별 직무교육을 정기적으로 실시
개요	
점검 내용	제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대비한 정기적인 비상계획 훈련 실시 여부 점검
점검 목적	제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등이 발생하는 경우 수립된 비상계획에 따라 신속한 복구 및 대응을 통해 사회, 경제적 파급 효과 및 피해를 최소화하기 위함
보안 위협	비상계획 훈련이 정기적으로 실시되지 않는 경우 제어시스템의 장애 등이 발생하는 상황에서 비상계획에 따른 적절한 대응 및 조치가 이루어지지 않아 제어시스템의 운영이 불가능할 수 있고 이에 따른 경제적, 사회적 손실이 발생할 위험이 존재함
참고	※ 본 점검항목은 제어시스템 장애 발생 시 대응 및 복구를 위한 훈련계획의 수립과 시행 여부를 확인하는 항목으로, 정기적인 훈련계획을 수립하여 정보보호 책임자가 승인하고 시행해야 함 ※ 비상계획 훈련은 제어시스템 운전원, 제어시스템 관리자, 유지보수 인력, 전담 보안 인력 등 제어시스템 운영과 관련된 인력 전체를 훈련 참여 대상으로 함
점검 대상 및 판단 기준	
대상	제어시스템 관련 운영조직 전체
판단 기준	**양호** : 제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행하는 경우
	취약 : 제어시스템의 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련을 정기적으로 시행하지 않는 경우
조치 방법	제어시스템 장애 발생, 사이버 공격, 물리적 테러 등에 대한 비상계획 훈련계획을 수립하고 계획에 따라 정기적으로 비상계획 훈련을 시행하도록 조치
조치 시 영향	일반적인 경우 영향 없음

점검 및 조치 사례

● 공통

Step 1) 제어시스템 장애, 사이버 공격, 물리적 테러 등이 발생하는 경우에 대비한 비상계획 훈련이 정기적으로 실시되는지 확인하고 그렇지 않은 경우 정기적인 비상계획 훈련을 실시하도록 조치

Step 2) 비상계획 훈련이 제어시스템 운전원, 관리자, 유지보수 인력 등 제어시스템 운영과 관련된 모든 인력을 대상으로 하여 실시되는지 확인하고 그렇지 않은 경우 관련 인력을 모두 포함하여 실시하도록 조치