ICS Asset Manager

산업제어시스템 자산탐지 및 분류관리 시스템

운영 지침서

제어시스템 현장에서 실제로 발생하는 21개 상황과

ICS Asset Manager의 기능 기반 해결 절차

Part A 보안 위협 상황 7건 · Part B 운영 업무 프로세스 7건 · Part C 고객 지원 7건

v1.0 · 2026. 8.

온시큐리티㈜

경기도 하남시 미사강변한강로 135 미사강변스카이폴리스 다동 1038~1039호 · TEL 031-792-0633

목 차

01 문서의 목적과 구성

본 문서는 산업제어시스템 자산탐지 및 분류관리 시스템(ICS Asset Manager)이 제어시스템 운영 현장에서 실제로 어떤 문제를 어떤 방식으로 해결하는지를, 기능 단위가 아닌 상황 단위로 설명하기 위해 작성되었습니다.

제품 소개 자료가 「어떤 기능이 있는가」를 다룬다면, 본 문서는 「그 기능이 어떤 상황에서 무엇을 해결하는가」를 설명합니다. 각 시나리오는 상황 설명 → 기존 환경에서의 문제 → 해결 절차 → 기대 효과의 동일한 구조로 기술되며, 해결 절차의 모든 단계에는 실제 구현된 기능이 근거로 명시되어 있습니다.

▪ 문서의 구성

구분	주제	내용
Part A	보안 위협 상황	미인가 자산 통신, MAC 변경, 비인가 정책 통신, 외부 공인 IP 통신, 트래픽 이상·운영 정지, 신규 서비스 포트, 프린트 사용 이력 — 7건
Part B	운영 업무 프로세스	자산 등록, 자산 실사, 물리 배치, 구성도 현행화, 정책 수립·운영, 이벤트 조치, 인수인계·계정 감사 — 7건
Part C	문제 해결	자산 대장 신뢰도, 점검 대응 부담, 논리·물리 단절, 자산 이력 단절, 전사 현황 부재, 가용성 우려, 단계적 도입 — 7건

▪ 기술 원칙

- 본 문서에 인용된 모든 기능은 ICS Asset Manager v1.0에 실제 구현되어 기능 리스트에 등재된 기능입니다.
- 해결 절차의 각 단계에는 「사용 기능」란에 근거 기능을 명시하여, 서술과 제품 사양이 일치함을 확인할 수 있도록 했습니다.
- 기능 참조는 2장의 기능 체계표에 정의된 F1~F9 코드를 따릅니다.

> **참고**
> 본 제품은 보안관제(MSSP) 서비스가 아닙니다. 24×7 상시 대응과 침해사고 대응(IR)은 제공 범위에 포함되지 않으며, 본 문서의 시나리오는 고객사 담당 인력이 시스템을 활용해 수행하는 절차를 기준으로 기술되었습니다.

02 ICS Asset Manager 기능 체계

시나리오 해결 절차에서 참조하는 기능 코드 체계입니다. 9개 대분류, 21개 중분류로 구성되며 총 200개의 세부 기능이 구현되어 있습니다.

코드	대분류	중분류	주요 세부 기능
F1	로그인	로그인 · 로그인 세션 만료	관리자/유지보수 업체 구분 로그인, 인증·유효성 검사, 미사용 30분 세션 만료
F2	대시보드	자산 대시보드 · 이벤트 대시보드	전체·타입별 자산 개수, 미확인 IP·미배치 자산 팝업, 호기별 영역별 배치 현황, 신규·비인가·자산 탐지 카운팅과 실시간 차트
F3	자산 관리	자산 현황 · 통신 현황 · 인수인계 · 캐비닛 관리	자산 등록/수정/폐기, IP·MAC 설정, 자산 상세(토폴로지·추가 정보·금일 알림), Excel 다운로드, 수집 IP·통신 내역, 담당자 인수인계, 시설·캐비닛 배치
F4	네트워크 현황	네트워크 현황 · 트래픽 통계	네트워크 구성·이벤트 발생·통신 현황 토폴로지, 호기별 트래픽량·사용량 TOP 10·포트 점유율, 자산별 트래픽·통신·포트 차트
F5	보안 관제	이벤트 알림 · 프린트 사용 이력	알림 종류·상태 조회, 알림 상세·토폴로지, Packet 분석(요청·기간 설정·프로토콜 상세), 조치 내용 등록/수정, 조치 요약 메시지, 담당자 배정, 프린트 사용 이력 상세
F6	보고서 관리	보고서	호기·유형·월간/연간 기간 선택, 보고서 발행·미리보기·다운로드·삭제
F7	정책	정책 관리 · IP 주소 관리 · 서비스 포트 관리	ACCEPT/DETECT 정책 등록/수정/삭제, 출발지·목적지 IP/Subnet 및 포트 설정, DETECT 알림 레벨, IP 주소·서비스 포트 관리
F8	시스템 관리	계정 관리 · 사용자 로그 · 연동 로그 · 환경설정	사용자·권한 등록/수정/삭제, 사용자 담당 자산 목록, 사용자·연동 로그 조회, 리소스 차트, 데이터 삭제 주기 설정
F9	구성도 관리	네트워크 구성도 관리	호기별 구성도 편집, 그룹·스위치·라우터·버스 아이콘 추가, 장비 간 선 연결, 장비 정보 수정, 구성도 저장

▪ 기능 계층 구조

계층	구성
관제 · 보고	자산 대시보드 · 이벤트 대시보드(F2) · 보고서 관리(F6)
탐지 · 분석	이벤트 알림 · Packet 분석 · 프린트 사용 이력(F5) · 트래픽 통계(F4)
관리	자산 관리 · 캐비닛 관리 · 인수인계(F3) · 정책(F7) · 구성도 관리(F9)
기반	빅데이터 기반 자산 자동 탐지 · 분류 · 제어망 패킷 패시브 수집

하위 계층의 수집·식별 결과가 상위 계층의 분석·관제로 연결되는 구조이며, 모든 시나리오의 해결 절차는 이 흐름을 따릅니다.

Part A 보안 위협 상황 시나리오

제어시스템 환경에서 실제로 발생하는 7개 이상 상황과, ICS Asset Manager가 이를 탐지·분석·조치하는 절차입니다.

시나리오	상황	핵심 대응 기능
A-01	관리되지 않던 장비가 제어망에서 통신할 때	F5 · F2 · F3
A-02	등록된 자산의 MAC 주소가 바뀌었을 때	F5 · F2 · F3
A-03	정책에 정의되지 않은 통신이 발생했을 때	F7 · F5 · F4
A-04	제어망에서 외부 공인 IP로 통신이 나갈 때	F5 · F3 · F4
A-05	설비의 통신량이 급변하거나 통신이 멎었을 때	F5 · F2 · F4
A-06	자산에서 새로운 서비스 포트가 열렸을 때	F5 · F3 · F4 · F7
A-07	제어 문서가 프린터로 출력될 때	F5 · F3

A-01 관리되지 않던 장비가 제어망에서 통신할 때

> **상황**
> 설비 벤더가 납품한 장비 안에 별도의 통신 모듈이 포함되어 있었고, 이 모듈이 제어망에서 통신을 시작했다. 자산 대장에는 존재하지 않는 통신 장비이다.

▪ 기존 환경에서의 문제

- 자산 대장은 도입 시점의 문서를 기준으로 작성되어, 장비 내부에 포함된 부속 통신 모듈까지 반영되지 않는다.
- 통신이 발생해도 제어 기능에는 이상이 없으므로 운전 담당자가 인지할 계기가 없다.
- 대장에 없는 장비는 이후 모든 점검·정책·보고에서 빠진 채로 남는다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**탐지**	제어망 패킷을 패시브 수집·분석하여 대장에 없는 IP가 통신을 시작하면 「신규 IP」 탐지 이벤트가 발생한다.	F5 이벤트 알림
2	**인지**	이벤트 대시보드에서 호기별 신규 탐지 실시간 차트와 신규 IP 탐지 알림 목록으로 즉시 확인한다. 자산 대시보드의 「미확인 IP」 개수와 목록 팝업에도 반영된다.	F2 대시보드
3	**식별**	알림 상세와 알림 토폴로지를 조회해 해당 IP가 어느 구간에서 어떤 자산과 통신했는지 확인한다.	F5 알림 상세 · 알림 토폴로지
4	**내용 확인**	Packet 분석을 요청하고, 분석 기간을 설정한 뒤 프로토콜별 결과와 상세 프로토콜을 조회한다.	F5 Packet 분석
5	**판정**	통신 현황에서 해당 수집 IP의 통신 내역을 조회해 정상 제어 통신인지 확인한다.	F3 통신 현황
6	**조치·등록**	조치 내용을 등록하고 담당자를 배정한다. 정상 장비로 확인되면 자산으로 등록하고 IP/MAC을 설정한다.	F5 조치 등록 · F3 자산 등록

▪ 기대 효과

- 대장이 아니라 실제 통신이 기준이 되어, 문서에 없던 자산이 드러난다.
- 「미확인 IP」가 대시보드에 상시 노출되어 방치되지 않는다.
- 확인된 장비가 자산으로 편입되어 이후 정책·점검·보고 대상에 포함된다.

A-02 등록된 자산의 MAC 주소가 바뀌었을 때

> **상황**
> 기존 자산의 IP는 그대로인데 MAC 주소가 변경된 통신이 관측되었다. 정상적인 NIC 교체일 수도 있고, 장비를 바꿔 끼운 것일 수도 있다.

▪ 기존 환경에서의 문제

- IP만으로 자산을 관리하면 물리 장비가 교체되어도 시스템상으로는 같은 자산으로 보인다.
- 교체 작업 기록이 별도 문서로 관리되어 시스템 데이터와 대조하기 어렵다.
- 정상 교체인지 무단 교체인지 판단할 근거 자료가 남지 않는다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**탐지**	등록 자산의 MAC이 변경되면「자산 탐지」분류의 MAC 변경 이벤트가 발생한다.	F5 이벤트 알림
2	**인지**	이벤트 대시보드의 호기별 자산 탐지 실시간 차트와 미조치 카운팅으로 확인한다.	F2 이벤트 대시보드
3	**대조**	자산 상세에서 해당 자산의 IP/MAC 목록과 기본정보·추가 정보를 조회해 기존 등록 값과 대조한다.	F3 자산 상세
4	**물리 확인**	캐비닛 관리에서 발전소 시설별 캐비닛과 할당 자산을 조회해 실제 설치 위치를 특정하고 현장 작업 이력과 맞춘다.	F3 캐비닛 관리
5	**담당 확인**	인수인계 화면과 계정 관리의 사용자 담당 자산 목록에서 해당 자산의 관리 담당자를 확인한다.	F3 인수인계 · F8 계정 관리
6	**반영**	정상 교체면 자산의 IP/MAC 설정을 수정하고, 그렇지 않으면 조치 내용을 등록한 뒤 담당자를 배정한다.	F3 자산 수정 · F5 조치 등록

▪ 기대 효과

- IP 단독이 아닌 IP·MAC 기준으로 자산을 식별해 물리 장비 교체를 포착한다.
- 물리 배치 정보와 관리 담당자가 함께 조회되어 확인 경로가 단축된다.
- 변경 사실과 판단 근거가 시스템에 함께 남아 다음 점검의 기준이 된다.

A-03 정책에 정의되지 않은 통신이 발생했을 때

> **상황**
> 허용 목록에 없는 자산 간 통신이 관측되었다. 임시 작업을 위해 연결했다가 원복하지 않았거나, 설비 설정 변경으로 새 통신 경로가 생긴 경우다.

▪ 기존 환경에서의 문제

- 제어망 통신은 상대와 주기가 고정적이지만, 무엇이 정상인지 문서로 정의되어 있지 않다.
- 임시 연결은 작업 종료 후 원복 여부를 확인할 방법이 없어 그대로 남는다.
- 통신이 늘어나도 이상으로 인지하지 못한 채 시간이 지난다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**정책 정의**	정책 관리에서 출발지·목적지 IP/Subnet과 포트를 지정해 ACCEPT(허용) 정책과 DETECT(탐지) 정책을 등록한다. DETECT는 알림 레벨을 선택한다.	F7 정책 관리
2	**기준 정비**	IP 주소 관리와 서비스 포트 관리에 사용 중인 IP주소·서비스를 등록해 정책 작성의 기준 목록으로 삼는다.	F7 IP 주소 관리 · 서비스 포트 관리
3	**탐지**	정책에 위배되는 통신이 발생하면 신규 통신(Flow)과 신규 서비스(Service)를 탐지하거나 「비인가 정책」 분류의 DETECT 정책 탐지 이벤트가 발생한다.	F5 이벤트 알림
4	**경로 확인**	네트워크 현황에서 이벤트 발생 토폴로지를 출발지·목적지 기준으로 조회해 통신 경로를 확인한다.	F4 네트워크 현황
5	**내용 확인**	알림 상세에서 Packet 분석을 요청해 실제 통신 내용과 프로토콜을 확인한다.	F5 Packet 분석
6	**정리**	필요한 통신이면 ACCEPT 정책으로 전환하고, 불필요한 통신이면 조치 내용을 등록해 차단 요청 이력을 남긴다.	F7 정책 수정 · F5 조치 등록

▪ 기대 효과

- 무엇이 허용된 통신인지가 정책으로 명문화되어 판단 기준이 생긴다.
- 임시 연결의 원복 누락이 탐지 이벤트로 드러난다.
- 정책 정비 과정 자체가 제어망 통신 구조를 문서화하는 작업이 된다.

A-04 제어망에서 외부 공인 IP 로 통신이 나갈 때

> **상황**
> 제어망 내 자산이 사설 대역을 벗어난 공인 IP와 통신했다. 원격 유지보수용 임시 경로일 수도 있고, 의도하지 않은 연결일 수도 있다.

▪ 기존 환경에서의 문제

- 망 분리는 설계상의 전제이며, 실제로는 임시 회선·업무망 연결 등 경로가 생겨날 수 있다.
- 경로의 존재 자체가 문서화되지 않아 통신 발생을 이상으로 인지하지 못한다.
- 경계 장비 로그만으로는 어느 제어 자산이 나갔는지 특정하기 어렵다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**탐지**	제어망에서 공인 IP 대역으로의 통신이 수집되면 「비인가 정책」 분류의 공인 IP 수집 이벤트가 발생한다.	F5 이벤트 알림
2	**주체 특정**	알림 상세와 알림 토폴로지에서 통신을 발생시킨 자산을 특정한다.	F5 알림 상세 · 알림 토폴로지
3	**이력 확인**	통신 현황에서 해당 자산의 통신 내역을 출발지·목적지 IP와 포트 기준으로 조회하고 Excel로 내려받는다.	F3 통신 현황
4	**패턴 확인**	트래픽 통계에서 해당 자산의 트래픽량·통신·포트 차트를 기간별로 조회해 일회성인지 지속적인지 판단한다.	F4 트래픽 통계
5	**내용 확인**	Packet 분석으로 통신 내용을 확인한다.	F5 Packet 분석
6	**조치·증적**	조치 내용을 등록하고, 해당 월 또는 연 단위 이벤트 보고서를 발행해 증적을 남긴다.	F5 조치 등록 · F6 보고서

▪ 기대 효과

- 「폐쇄망이므로 외부 통신은 없다」는 전제를 실측 데이터로 검증한다.
- 어느 자산이 언제 무엇과 통신했는지가 특정되어 조치 대상이 명확해진다.
- 검증 결과가 보고서로 남아 감사 대응 자료가 된다.

A-05 설비의 통신량이 급변하거나 통신이 멎었을 때

> **상황**
> 특정 자산의 트래픽이 평소와 크게 달라졌거나, 일정 기간 패킷이 전혀 발생하지 않았다. 제어 시스템 알람에는 나타나지 않았다.

▪ 기존 환경에서의 문제

- 제어 시스템 알람은 공정 값 기준이어서 네트워크 계층의 이상을 잡아내지 못한다.
- 통신 중단이 설비 정지 때문인지 네트워크 문제인지 구분되지 않는다.
- 「평소와 다르다」를 판단할 기준 데이터가 축적되어 있지 않다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**탐지**	「자산 탐지」 분류로 트래픽 이상과 운영 정지(1개월 패킷 미발생)를 탐지한다.	F5 이벤트 알림
2	**인지**	이벤트 대시보드의 호기별 트래픽 실시간 차트와 연결 상태 정보에서 즉시 확인한다.	F2 이벤트 대시보드
3	**추이 확인**	트래픽 통계에서 기간 필터로 호기별 트래픽량과 사용량 TOP 10을 조회해 해당 자산의 위치를 파악한다.	F4 트래픽 통계
4	**개별 확인**	선택 자산의 트래픽량·통신·포트 차트를 조회해 변화의 성격을 구분한다.	F4 트래픽 통계
5	**상태 대조**	자산 대시보드의 자산 상태 색상과 호기별 영역별 배치 현황에서 인접 자산도 함께 영향을 받았는지 확인한다.	F2 자산 대시보드
6	**조치**	조치 내용을 등록하고 담당자를 배정한다. 설비 문제로 판단되면 해당 자산의 담당자에게 배정해 후속 확인을 요청한다.	F5 조치 등록 · 담당자 배정

▪ 기대 효과

- 공정 알람이 감지하지 못하는 네트워크 계층의 이상을 조기에 포착한다.
- 1개월 패킷 미발생 자산이 자동으로 드러나 방치된 설비를 찾아낸다.
- 설비 문제와 보안 사안을 같은 화면에서 구분해 담당 부서를 빠르게 정한다.

A-06 자산에서 새로운 서비스 포트가 열렸을 때

> **상황**
> 기존에 사용하지 않던 포트로 통신이 시작되었다. 소프트웨어 업데이트나 원격 관리 도구 설치로 서비스가 추가된 경우가 많다.

▪ 기존 환경에서의 문제

- 설비에 설치된 소프트웨어와 열려 있는 서비스가 대장에 관리되지 않는다.
- 포트가 열려도 제어 기능에 이상이 없어 아무도 알아채지 못한다.
- 점검 대상을 정할 때 실제로 무엇이 동작 중인지 알 수 없다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**탐지**	「신규 탐지」 분류로 신규 통신(Flow)과 신규 서비스(Port) 사용을 탐지한다.	F5 이벤트 알림
2	**확인**	통신 현황에서 발전 호기별 통신 내역을 출발지·목적지 포트와 서비스 포트 기준으로 조회한다.	F3 통신 현황
3	**점유 확인**	트래픽 통계의 호기별 포트 점유율 차트와 선택 자산 포트 차트로 사용 비중을 확인한다.	F4 트래픽 통계
4	**기준 대조**	서비스 포트 관리에 등록된 서비스 목록과 대조해 정의되지 않은 서비스인지 확인한다.	F7 서비스 포트 관리
5	**자산 반영**	정당한 서비스면 서비스 포트를 등록하고 자산 상세의 추가 정보를 갱신한다.	F7 서비스 포트 등록 · F3 자산 수정
6	**정책 반영**	허용 대상이 아니면 DETECT 정책으로 등록해 이후 사용을 탐지하고, 조치 내용을 기록한다.	F7 정책 등록 · F5 조치 등록

▪ 기대 효과

- 설비에서 실제로 동작 중인 서비스가 데이터로 파악된다.
- 정의된 서비스 목록과 실측 사용 현황의 차이가 드러난다.
- 확인된 서비스가 정책에 반영되어 다음부터는 기준으로 작동한다.

A-07 제어 문서가 프린터로 출력될 때

> **상황**
> 제어망 내 프린터에서 출력이 발생했다. 출력물은 물리적으로 반출되면 네트워크 기록으로는 추적되지 않는다.

▪ 기존 환경에서의 문제

- 네트워크 프린터가 자산으로 관리되지 않아 감시 대상에서 빠져 있다.
- 출력은 정상 업무와 형태가 같아 이상 여부를 판단할 기준이 없다.
- 출력 사실 자체가 기록되지 않아 사후 확인이 불가능하다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**수집**	제어시스템 내 프린터 사용 이력을 자동 수집·기록한다.	F5 프린트 사용 이력
2	**조회**	발전 호기와 파일명, 기간으로 검색해 프린트 사용 이력 목록을 조회한다.	F5 프린트 사용 이력
3	**상세 확인**	이력 상세에서 프린트 정보 요약과 프린트 명령·프린트 정보를 확인한다.	F5 프린트 사용 이력 상세
4	**자산 대조**	자산 현황에서 프린터를 자산으로 등록·관리하고, 통신 현황에서 사용 포트를 확인한다.	F3 자산 현황 · 통신 현황
5	**시점 확인**	기간 검색으로 이력 목록을 조회해 출력이 발생한 시점을 확인한다.	F5 프린트 사용 이력
6	**보관**	확인 결과를 이력 상세로 보관하고, 정기 보고 시 별도 자료로 활용한다.	F5 프린트 사용 이력

▪ 기대 효과

- 관리 사각지대였던 출력 행위가 기록 대상으로 편입된다.
- 파일명과 시점이 남아 사후 확인이 가능해진다.
- 내부 통제 항목으로서 점검·보고 시 근거 자료가 된다.

※ 프린트 사용 이력은 네트워크로 전달된 출력 명령 정보를 기준으로 수집됩니다.

Part B 운영 업무 프로세스 시나리오

제어시스템 자산 담당자의 일상 업무 7개 프로세스와, 각 단계에서 ICS Asset Manager가 수행하는 역할입니다.

시나리오	업무	핵심 활용 기능
B-01	신규 설비를 자산으로 등록할 때	F3 · F8
B-02	자산 실사와 대장 현행화를 수행할 때	F3 · F2
B-03	설비의 물리적 배치를 관리할 때	F3 · F2
B-04	네트워크 구성도를 현행화할 때	F4 · F9
B-05	통신 정책을 수립하고 운영할 때	F3 · F7
B-06	이벤트를 확인하고 조치를 기록할 때	F2 · F5
B-07	담당자 인수인계와 계정을 관리할 때	F3 · F8

B-01 신규 설비를 자산으로 등록할 때

> **상황**
> 설비 증설로 신규 장비가 제어망에 편입된다. 각 장비의 IP·MAC·용도·설치 위치를 자산으로 등록해야 한다.

▪ 기존 환경에서의 문제

- 자산 등록이 담당자별 엑셀로 이루어져 표기 방식이 다르고 중복·오기가 발생한다.
- 실제 통신하는 IP·MAC 정보와 등록한 IP·MAC가 일치하는지 검증할 수단이 없다.
- 등록 누락 시 해당 설비는 이후 모든 탐지·정책·보고에서 빠진다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**실측 확인**	통신 현황에서 발전 호기별 수집 IP 목록을 조회해 실제로 통신하고 있는 주소를 먼저 확인한다.	F3 통신 현황
2	**등록**	자산 등록 팝업에서 자산 정보를 입력해 등록한다. 관련 자료가 있으면 자산 관리 파일로 첨부한다.	F3 자산 등록
3	**주소 연결**	자산 IP/MAC 설정 팝업에서 미배정 IP/MAC 목록을 검색해 실제 수집된 주소를 자산에 연결한다.	F3 자산 IP/MAC 설정
4	**분류 확인**	자산 종류별 현황(컨트롤러·리모트컨트롤러·워크스테이션·DB/HST·OPC·네트워크 장비)에서 분류가 올바로 반영되었는지 확인한다.	F3 자산 현황
5	**위치 반영**	캐비닛 관리에서 캐비닛을 등록하고 자산을 배치한다. 미배치 자산은 자산 대시보드에서 확인한다.	F3 캐비닛 관리 · F2 자산 대시보드
6	**담당 확인**	계정 관리에서 사용자 담당 자산 목록을 조회해 관리 책임 소재를 확인한다.	F8 계정 관리

▪ 기대 효과

- 실측 수집 IP/MAC를 먼저 확인하고 등록하므로 대장과 실제가 처음부터 일치한다.
- 미배정 IP/MAC 목록에서 선택하는 방식이라 오기가 발생하지 않는다.
- 논리 정보(IP·MAC)와 물리 정보(캐비닛·시설)가 한 시스템에서 연결된다.

B-02 자산 실사와 대장 현행화를 수행할 때

> **상황**
> 연 1회 자산 실사를 앞두고 대장 정확도를 확인해야 한다. 최근 몇 년간 설비 교체와 폐기가 반복되었다.

▪ 기존 환경에서의 문제

- 실사가 현장 육안 확인에 의존해 인력과 시간이 많이 들고 확인하지 못한 구간이 남는다.
- 폐기된 설비가 대장에 남아 있거나, 교체된 설비가 반영되지 않은 채 방치된다.
- 실사 결과를 유지·관리할 체계가 없어 다음 해에 다시 원점에서 시작한다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**현황 확보**	자산 현황에서 사용 가능·폐기 상태별 자산 목록과 자산 종류별 현황을 조회한다.	F3 자산 현황
2	**미등록 식별**	자산 대시보드의 미확인 IP 개수와 목록 팝업에서 수집되고 있으나 자산으로 등록되지 않은 IP를 추출한다.	F2 자산 대시보드
3	**실측 대조**	통신 현황에서 발전 호기별 수집 IP 목록을 조회하고 Excel로 내려받아 대장과 대조한다.	F3 통신 현황
4	**위치 특정**	캐비닛 관리에서 발전소 시설별 캐비닛과 할당 자산을 조회해 현장 확인 동선을 최소화한다.	F3 캐비닛 관리
5	**반영**	확인 결과에 따라 자산 정보를 수정하고, 사용 종료 자산은 폐기 처리한다.	F3 자산 수정 · 자산 폐기
6	**산출**	자산 목록을 Excel로 다운로드해 실사 결과 자료로 제출하고 보고서를 발행한다.	F3 Excel 다운로드 · F6 보고서

▪ 기대 효과

- 실측 통신 데이터가 실사의 출발점이 되어 현장 확인 대상이 크게 줄어든다.
- 「대장에만 있는 자산」과 「대장에 없는 자산」이 동시에 드러난다.
- 실사 결과가 시스템에 반영되어 다음 해에 처음부터 다시 하지 않는다.

B-03 설비의 물리적 배치를 관리할 때

> **상황**
> 제어반 개조로 다수 설비의 캐비닛 배치가 변경되었다. 기존 배치도는 도면 파일로만 존재해 갱신이 지연되고 있다.

▪ 기존 환경에서의 문제

- 논리 자산 정보(IP·MAC)와 물리 배치 정보(시설·캐비닛)가 서로 다른 문서로 관리된다.
- 장애 발생 시 「어느 설비가 어디에 있는가」를 파악하는 데 시간이 걸린다.
- 도면 갱신이 담당자 개인 작업이어서 최신본 여부를 신뢰하기 어렵다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**캐비닛 등록**	캐비닛 관리에서 캐비닛을 등록하고 발전소 시설별로 배치한다.	F3 캐비닛 등록
2	**자산 배치**	캐비닛 미할당 자산 목록에서 대상을 검색해 캐비닛에 할당한다.	F3 캐비닛 자산 설정
3	**누락 확인**	자산 대시보드의 미배치 자산 개수와 목록 팝업으로 아직 배치되지 않은 자산을 확인한다.	F2 자산 대시보드
4	**변경 반영**	배치가 바뀌면 캐비닛 정보와 캐비닛 자산을 수정하고, 사용하지 않는 캐비닛은 삭제한다.	F3 캐비닛 수정 · 삭제
5	**현황 확인**	자산 대시보드의 발전 호기별 영역별 자산 배치 현황과 자산 상태 색상으로 배치 결과를 확인한다.	F2 자산 대시보드
6	**활용**	배치 정보가 자산의 논리 정보와 연결되어, 이벤트 확인 시 캐비닛 관리 화면에서 해당 자산의 설치 위치를 조회할 수 있다.	F3 자산 상세 · 캐비닛 관리

▪ 기대 효과

- 논리 자산 정보와 물리 위치가 하나의 시스템에서 연결된다.
- 미배치 자산이 대시보드에 노출되어 관리 누락이 드러난다.
- 별도 도면 관리 작업이 시스템 입력으로 대체되어 최신본 문제가 해소된다.

B-04 네트워크 구성도를 현행화할 때

> **상황**
> 제어망 구성도가 파워포인트로 관리되고 있다. 스위치 증설과 구간 분리가 있었지만 도면에 반영되지 않았다.

▪ 기존 환경에서의 문제

- 구성도가 그림 파일이어서 실제 통신 데이터와 대조할 수 없다.
- 작성자만 편집할 수 있어 갱신 주기가 길고, 여러 버전이 존재한다.
- 이벤트가 발생해도 구성도상 어느 위치인지 연결해서 보기 어렵고, 실제 자산의 위치를 찾을 수 없다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**구성 확인**	네트워크 현황에서 발전 호기별 네트워크 구성 토폴로지를 조회한다. 전체·출발지·목적지 기준으로 자산명 또는 IP를 검색한다.	F4 네트워크 현황
2	**구성도 편집**	구성도 관리에서 발전 호기를 선택하고 그룹·스위치·라우터·버스 아이콘을 추가한다.	F9 구성도 관리
3	**연결 정의**	장비 간 선을 연결해 실제 구성에 맞게 배치한 뒤 구성도를 저장한다.	F9 구성도 관리
4	**정보 보완**	선택 장비 정보 수정 화면에서 각 장비의 정보를 갱신한다.	F9 장비 정보 수정
5	**실측 대조**	네트워크 현황의 통신 현황 토폴로지로 실제 통신 흐름과 구성도를 대조한다.	F4 네트워크 현황
6	**활용**	이벤트 발생 토폴로지에서 이벤트가 발생한 위치를 구성 맥락과 함께 조회한다.	F4 네트워크 현황

▪ 기대 효과

- 구성도가 그림이 아니라 시스템 데이터로 관리되어 누구나 최신본을 본다.
- 설계상 구성과 실측 통신 흐름을 같은 화면에서 대조할 수 있다.
- 이벤트가 네트워크 구성 위에 표시되어 영향 범위 판단이 빨라진다.

B-05 통신 정책을 수립하고 운영할 때

> **상황**
> 제어망 통신 허용 기준을 정하고 시스템에 반영해야 한다. 현재는 「필요한 통신만 허용」이라는 원칙만 있고 목록이 없다.

▪ 기존 환경에서의 문제

- 허용해야 할 통신 목록을 처음부터 만들 근거 데이터가 없다.
- 정책을 너무 좁게 잡으면 정상 통신이 대량으로 걸리고, 넓게 잡으면 의미가 없다.
- 정책을 만들어도 실제 통신과 얼마나 맞는지 확인할 방법이 없다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**기준 수집**	통신 현황에서 발전 호기별 통신 내역을 조회하고 Excel로 내려받아 실제 통신 구조를 파악한다.	F3 통신 현황
2	**주소 정비**	IP 주소 관리에 주소 명과 IP/Subnet을 등록하고, 서비스 포트 관리에 서비스 명과 포트를 등록한다.	F7 IP 주소 관리 · 서비스 포트 관리
3	**정책 작성**	정책 관리 등록 팝업에서 출발지·목적지 IP/Subnet과 포트를 설정한다. ACCEPT 선택 시 자산 자동등록 여부를 지정한다.	F7 정책 등록
4	**탐지 설정**	DETECT 정책은 알림 레벨(Notice·Alert·Warning·Critical)을 선택해 중요도를 구분한다.	F7 정책 관리
5	**검증**	허용/탐지 구분으로 정책 목록을 조회하고, 이벤트 대시보드의 비인가 정책 탐지 현황으로 정책 적정성을 확인한다.	F7 정책 조회 · F2 대시보드
6	**조정**	과탐이 많은 정책은 수정하고 불필요한 정책은 삭제한다. 설정한 IP/Subnet·포트 목록을 조회해 내용을 확인한다.	F7 정책 수정 · 삭제

▪ 기대 효과

- 실측 통신 데이터를 기준으로 정책을 만들어 현실과 맞는 허용 목록이 나온다.
- ACCEPT/DETECT 분리와 알림 레벨로 차단이 아닌 단계적 탐지 운영이 가능하다.
- 정책 수립 결과가 이벤트 발생량으로 즉시 확인되어 조정이 빠르다.

B-06 이벤트를 확인하고 조치를 기록할 때

> **상황**
> 담당자가 근무 중 발생한 이벤트를 확인하고, 조치가 필요한 건을 처리한 뒤 결과를 남겨야 한다.

▪ 기존 환경에서의 문제

- 알림이 쌓이기만 하고 누가 무엇을 확인했는지 남지 않는다.
- 조치 진행 상황이 개인 메모나 메신저로 관리되어 인계 시 누락된다.
- 「누가 언제 무엇을 판단했는가」가 없어 감사 대응이 어렵다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**현황 확인**	이벤트 대시보드에서 전체·미조치·신규 탐지·비인가 탐지·자산 탐지 카운팅과 호기별 실시간 차트를 확인한다.	F2 이벤트 대시보드
2	**선별**	이벤트 알림에서 발전 호기·알림 종류·상태를 선택하고 자산명·IP·기간으로 검색해 대상을 좁힌다.	F5 이벤트 알림
3	**분석**	알림 상세와 알림 토폴로지를 조회하고, 필요 시 Packet 분석을 요청해 결과 목록과 상세 프로토콜을 확인한다.	F5 알림 상세 · Packet 분석
4	**배정**	담당자 배정 팝업에서 아이디로 검색해 담당자를 배정한다.	F5 담당자 배정
5	**조치 기록**	알림 조치 내용을 등록하고 진행에 따라 수정한다. 조치 요약 메시지를 전송해 관련자와 공유한다.	F5 조치 등록 · 요약 메시지
6	**확인**	알림조치 내역과 조치 요약 메시지 목록을 조회해 처리 이력을 확인한다.	F5 알림조치 내역

▪ 기대 효과

- 대시보드 → 알림 → 배정 → 조치로 이어지는 단일 동선으로 관제가 표준화된다.
- 담당자와 조치 내용이 시스템에 남아 인계와 감사 추적이 동시에 해결된다.
- 미조치 현황이 상시 노출되어 처리되지 않은 건이 방치되지 않는다.

B-07 담당자 인수인계와 계정을 관리할 때

> **상황**
> 인사 이동으로 자산 담당자가 교체된다. 담당 자산 수십 대의 관리 책임을 후임자에게 넘겨야 한다.

▪ 기존 환경에서의 문제

- 담당 자산 목록이 개인 파일로 관리되어 무엇을 넘겨야 하는지 정리되지 않는다.
- 인계 과정에서 일부 자산이 누락되어 담당자 없는 자산이 생긴다.
- 퇴직·전보 후에도 계정이 남아 있어 접근 권한이 정리되지 않는다.

▪ ICS Asset Manager 의 해결 절차

	단계	수행 내용	사용 기능
1	**현황 확인**	인수인계 화면에서 인계자·인수자 목록과 담당자별 보유 자산 수를 조회한다.	F3 인수인계
2	**대상 확인**	인수인계 자산 목록 화면에서 인계자의 담당 자산 목록을 검색해 확인한다.	F3 인수인계
3	**인계 수행**	자산 담당자 인수인계를 처리해 담당 자산을 후임자에게 이관한다.	F3 인수인계 처리
4	**결과 확인**	인수자의 담당 자산 목록을 조회해 이관 결과를 확인한다.	F3 인수인계
5	**계정 정리**	계정 관리에서 사용자 정보를 수정하고, 필요 시 비밀번호를 수정하거나 사용자를 비활성 처리한다.	F8 계정 관리
6	**감사**	사용자 로그에서 아이디와 기간으로 접근 이력을 조회하고, 연동 로그로 데이터 종류별 연동 내역을 확인한다.	F8 사용자 로그 · 연동 로그

▪ 기대 효과

- 담당 자산이 시스템 데이터로 인계되어 누락 없이 이관된다.
- 담당자별 보유 자산 수가 상시 조회되어 관리 책임 소재가 드러난다.
- 계정 정리와 접근 이력 감사가 같은 화면에서 이루어진다.

Part C 문제 해결 시나리오

제어시스템 자산 담당자들이 현장에서 반복적으로 제기하는 7개 문제 제기와, 그에 대한 ICS Asset Manager의 답변입니다.

시나리오	문제점	주제
C-01	자산 대장이 현실과 얼마나 다른지조차 모릅니다.	자산 대장의 신뢰도 부재
C-02	실태점검 때마다 자산 현황 자료를 새로 만듭니다.	점검 대응의 반복 부담
C-03	설비가 어디 붙어 있는지 찾는 데 시간이 더 걸립니다.	논리 정보와 물리 위치의 단절
C-04	담당자가 바뀌면 그 설비의 이력이 끊깁니다.	자산 이력의 단절
C-05	본사에서는 사업소 자산 현황을 알 방법이 없습니다.	전사 자산 현황의 부재
C-06	보안 시스템이 제어 운전에 영향을 줄까 봐 망설여집니다.	가용성 우려
C-07	통합 보안 모니터링까지 한 번에 가기에는 부담이 큽니다.	단계적 도입의 필요

C-01 자산 대장의 신뢰도 부재

> **고객의 말**
> "자산 대장이 현실과 얼마나 다른 지조차 모릅니다."

▪ 문제의 배경

- 제어 설비는 수십 년에 걸쳐 증설·교체되어 왔고, 그때마다 대장이 온전히 갱신되지는 않았다.
- 대장은 문서를 근거로 작성되어, 실제로 통신하는 장비와 일치하는지 검증할 수단이 없다.
- 보안 대책을 세우려 해도 대상 목록 자체가 부정확해 출발점이 서지 않는다.

▪ ICS Asset Manager 의 답

접근	내용	근거 기능
실측 기반 식별	제어망 패킷을 패시브 수집·분석해 자산을 자동 탐지·분류한다. 문서가 아니라 실제 통신이 근거가 된다.	수집·식별 기반 · F3 자산 현황
차이의 가시화	자산 대시보드가 미확인 IP와 미배치 자산의 개수를 상시 표시하고 목록 팝업으로 바로 확인시킨다.	F2 자산 대시보드
실측 대조	통신 현황의 수집 IP 목록과 통신 내역을 Excel로 내려받아 기존 대장과 대조한다.	F3 통신 현황
상세 축적	자산 상세에 기본정보와 추가 정보를 관리하고, 자산 종류별로 분류해 목록화한다.	F3 자산 상세

> **결과**
> 「대장이 맞는지 모른다」에서 「무엇이 다른 지 숫자로 나온다」로 전환됩니다. 이후의 모든 정책·점검·보고가 이 목록 위에서 성립합니다.

C-02 점검 대응의 반복 부담

> **고객의 말**
> "실태점검 때마다 자산 현황 자료를 새로 만듭니다."

▪ 문제의 배경

- 정보보호 실태점검·보안 감사 때마다 자산 최신현황 대장을 별도로 작성한다.
- 작성 근거가 담당자 기억과 개별 파일이어서 매번 결과가 조금씩 달라진다.
- 점검이 끝나면 자료가 사장되거나 담당자가 변경되어 다음 점검 때 다시 처음부터 만든다.

▪ ICS Asset Manager 의 답

접근	내용	근거 기능
최신현황 유지	실측 데이터가 상시 축적되어, 대장 갱신이 별도 현장 조사 없이 시스템 안에서 이루어진다.	F3 자산 현황
물리 증빙	시설·캐비닛·자산 배치 정보를 함께 관리해 물리적 자산관리 증빙을 제공한다.	F3 캐비닛 관리
구성 증빙	호기별 네트워크 구성도를 시스템에서 관리해 네트워크 구성 자료를 최신 상태로 유지한다.	F9 구성도 관리
통제 증빙	ACCEPT/DETECT 정책과 IP 주소·서비스 포트 목록으로 통신 통제 기준을 문서화한다.	F7 정책
자료 산출	자산 목록·통신 내역 Excel 다운로드와 월간/연간 보고서 발행으로 제출 자료를 즉시 만든다.	F3 · F6 보고서

> **결과**
> 점검 대응이 「그때마다 만드는 일」에서 「상시 축적되는 운영 결과물을 꺼내는 일」로 바뀝니다.

C-03 논리 정보와 물리 위치의 단절

> **고객의 말**
> "설비가 어디 붙어 있는지 찾는 데 시간이 더 걸립니다."

▪ 문제의 배경

- 자산 정보는 IP 중심으로만 관리되어 실제 설치 위치를 알 수 없다.
- 배치도는 도면 파일로 따로 존재하고 갱신이 늦어 신뢰하기 어렵다.
- 장애나 점검 때 현장 확인 동선을 계획할 수 없어 시간이 낭비된다.

▪ ICS Asset Manager 의 답

접근	내용	근거 기능
Layer 기반 배치	발전소 시설과 캐비닛을 등록하고 자산을 배치해 물리적 위치를 시스템에 기록한다.	F3 캐비닛 관리
논리·물리 연결	배치 정보가 자산의 IP·MAC 등 논리 정보와 연결되어 하나의 자산으로 관리된다.	F3 자산 상세
배치 현황 조회	자산 대시보드에서 발전 호기별 영역별 자산 배치 현황과 자산 상태 색상을 조회한다.	F2 자산 대시보드
누락 관리	미배치 자산 개수와 목록이 대시보드에 노출되어 배치되지 않은 자산이 드러난다.	F2 자산 대시보드
구성 연계	구성도 관리에서 호기별 네트워크 구성도를 직접 편집해 배치와 구성을 함께 유지한다.	F9 구성도 관리

> **결과**
> 「어디에 있는가」가 시스템 데이터가 되어, 장애 대응과 현장 점검의 동선이 사전에 계획됩니다.

C-04 자산 이력의 단절

> **고객의 말**
> "담당자가 바뀌면 그 설비의 이력이 끊깁니다."

▪ 문제의 배경

- 설비별 판단 근거와 조치 이력이 담당자 개인 파일과 기억에 축적된다.
- 인수인계 문서로는 담당 자산 목록조차 정확히 넘어가지 않는다.
- 이력이 끊기면 같은 문제를 다시 조사하게 되고 대응이 느려진다.

▪ ICS Asset Manager 의 답

접근	내용	근거 기능
담당 자산의 명시화	인수인계 화면에서 담당자별 보유 자산 수와 담당 자산 목록을 조회하고 이관을 처리한다.	F3 인수인계
판단 이력 축적	이벤트 알림의 조치 내용과 조치 요약 메시지가 남아 과거 판단 근거를 확인할 수 있다.	F5 이벤트 알림
기준의 명문화	정상 통신에 대한 판단이 ACCEPT/DETECT 정책과 IP 주소·서비스 포트 목록으로 기록된다.	F7 정책
구성 이력	최신 구성도가 시스템에 저장되어 개인 파일이 아니라 제품 안에서 유지된다.	F9 구성도 관리
접근 이력	사용자 로그와 연동 로그로 누가 언제 시스템을 사용했는지 확인한다.	F8 사용자 로그 · 연동 로그

> **결과**
> 운영 지식이 개인이 아니라 시스템에 축적됩니다. 담당자 교체가 관리 수준의 하락으로 이어지지 않습니다.

C-05 전사 자산 현황의 부재

> **고객의 말**
> "본사에서는 사업소 자산 현황을 알 방법이 없습니다."

▪ 문제의 배경

- 사업소별로 자산 관리 방식과 대장 양식이 달라 합산이 되지 않는다.
- 본사는 사업소의 보고에 의존하고, 보고 주기 사이의 변화는 알 수 없다.
- 전사 관점에서 자산 규모와 보안 현황을 하나의 숫자로 말할 수 없다.

▪ ICS Asset Manager 의 답

접근	내용	근거 기능
3계층 구조	ICS Asset Collector(호기 단위 수집) → ICS Asset Manager(발전본부 단위 분석) → 본사 ICS Asset Manager(전사 통합)의 계층으로 구성된다.	제품 구성
전사 통합 조회	본사에서 발전본부별 이벤트 탐지 현황과 자산 통계를 통합 조회한다.	전사 통합 구성
본부 단위 관제	발전본부에서는 호기별 자산 유형 통계와 이벤트 대시보드로 관할 범위를 관제한다.	F2 대시보드
공통 기준	동일한 정책 체계(ACCEPT/DETECT)와 자산 분류 체계를 사용해 사업소 간 비교가 성립한다.	F7 정책 · F3 자산 관리
권한 분리	역할별 권한을 등록·관리하고 사용자별 담당 자산 목록을 확인한다.	F8 계정 관리

> **결과**
> 본사와 사업소가 같은 데이터를 같은 기준으로 봅니다. 전사 자산 규모와 보안 현황이 하나의 숫자로 관리됩니다.

※ 전사 통합 구성은 본사에 동일 제품(ICS Asset Manager)을 배치해 발전본부별 데이터를 통합하는 방식입니다.

C-06 가용성 우려

> **고객의 말**
> "보안 시스템이 제어 운전에 영향을 줄까 봐 망설여집니다."

▪ 문제의 배경

- 제어 설비는 정지 시 생산 손실과 안전 문제로 직결되어 어떤 부하도 허용하기 어렵다.
- 능동 스캔 방식의 자산 식별 도구는 구형 설비에서 오작동을 유발한 사례가 보고된다.
- 에이전트 설치는 설비 벤더의 보증 범위를 벗어나는 경우가 많다.

▪ ICS Asset Manager 의 답

접근	내용	근거 기능
패시브 수집	제어망 네트워크 패킷을 패시브 방식으로 수집·분석만 한다. 능동 스캔과 패킷 주입을 수행하지 않는다.	수집 방식
설치 부담 없음	자산 식별과 이상행위 탐지가 네트워크 기반으로 동작해 개별 설비에 설치할 것이 없다.	F3 · F5
품질 검증	TTA 소프트웨어 품질 시험 GS인증 1등급을 획득했다.	인증
현장 검증	2022년 5월 출시와 함께 GS인증 1등급을 획득했고, 한국서부발전 확대 구축(2022.07)과 한국중부발전 보령 신복합 납품(2024.12)으로 운영되고 있다.	구축 실적

> **결과**
> 제어 프로세스에 대한 개입 없이 자산 가시성을 확보합니다. 도입 리스크가 「설비 영향」이 아니라 「수집 구간 설계」 수준으로 축소됩니다.

C-07 단계적 도입의 필요

> **고객의 말**
> "통합 보안 모니터링까지 한 번에 가기에는 부담이 큽니다."

▪ 문제의 배경

- 보안 체계를 한 번에 구축하려면 예산과 조직 준비가 동시에 필요해 착수가 미뤄진다.
- 자산 현황이 부정확한 상태에서 상위 보안 시스템을 도입하면 효과가 나지 않는다.
- 단계적으로 가더라도 나중에 시스템을 갈아엎게 될까 우려된다.

▪ ICS Asset Manager 의 답

접근	내용	근거 기능
자산 가시성	먼저 ICS Asset Manager로 자산을 식별·분류하고 물리 배치와 정책 체계를 세운다.	F3 · F7 · F9
운영 정착	이벤트 알림과 조치 이력, 담당자 배정과 인수인계 운영으로 조직의 관리 체계를 정착시킨다.	F5 · F3 인수인계
상위 확장	동일 인프라에서 ICS Security Monitor로 소프트웨어 업그레이드한다. 별도 하드웨어 교체 없이 전환된다.	업그레이드 경로
확장 후 역량	취약점 탐지(Snort 기반), 악성코드 탐지, 위협 스캐닝·상관분석, 이슈 관리, 정책 다지역 동기화가 추가된다.	ICS Security Monitor

> **결과**
> 자산 가시성 확보를 먼저 끝내고 상위 보안 모니터링으로 확장합니다. 앞 단계의 하드웨어 투자와 정착된 운영 체계가 다음 단계의 기반이 됩니다.

※ 업그레이드 비용은 전 모델 공통 2,000만 원(VAT 별도)이며, 동일 인프라에서 소프트웨어 업그레이드로 진행됩니다.

03 시나리오 – 기능 매핑 종합

본 문서에서 다룬 21개 시나리오가 ICS Asset Manager의 기능 체계 전반을 어떻게 활용하는지 정리한 표입니다. 기능이 특정 영역에 편중되지 않고 수집 · 식별 · 판별 · 관리 · 산출 전 계층에 걸쳐 연계 활용되는 통합 운영 구조임을 확인할 수 있습니다.

코드	기능 대분류	활용 시나리오
F1	**로그인**	전 시나리오 공통 (시스템 접근 기반)
F2	**대시보드**	A-01, A-02, A-05, B-01, B-02, B-03, B-05, B-06, C-01, C-03, C-05
F3	**자산 관리**	A-01, A-02, A-04, A-06, A-07, B-01, B-02, B-03, B-05, B-07, C-01, C-02, C-03, C-04, C-05, C-06, C-07
F4	**네트워크 현황**	A-03, A-04, A-05, A-06, B-04
F5	**보안 관제**	A-01, A-02, A-03, A-04, A-05, A-06, A-07, B-06, C-04, C-06, C-07
F6	**보고서 관리**	A-04, B-02, C-02
F7	**정책**	A-03, A-06, B-05, C-02, C-04, C-05, C-07
F8	**시스템 관리**	A-02, B-01, B-07, C-04, C-05
F9	**구성도 관리**	B-04, C-02, C-03, C-04, C-07

▪ 시나리오 전체 목록

구분	번호	제목
Part A	**A-01**	관리되지 않던 장비가 제어망에서 통신할 때
Part A	**A-02**	등록된 자산의 MAC 주소가 바뀌었을 때
Part A	**A-03**	정책에 정의되지 않은 통신이 발생했을 때
Part A	**A-04**	제어망에서 외부 공인 IP로 통신이 나갈 때
Part A	**A-05**	설비의 통신량이 급변하거나 통신이 멎었을 때
Part A	**A-06**	자산에서 새로운 서비스 포트가 열렸을 때
Part A	**A-07**	제어 자료가 프린터로 출력될 때
Part B	**B-01**	신규 설비를 자산으로 등록할 때
Part B	**B-02**	자산 실사와 대장 현행화를 수행할 때

구분	번호	제목
Part B	**B-03**	설비의 물리적 배치를 관리할 때
Part B	**B-04**	네트워크 구성도를 현행화할 때
Part B	**B-05**	통신 정책을 수립하고 운영할 때
Part B	**B-06**	이벤트를 확인하고 조치를 기록할 때
Part B	**B-07**	담당자 인수인계와 계정을 관리할 때
Part C	**C-01**	자산 대장의 신뢰도 부재 — 자산 대장이 현실과 얼마나 다른지조차 모릅니다.
Part C	**C-02**	점검 대응의 반복 부담 — 실태점검 때마다 자산 현황 자료를 새로 만듭니다.
Part C	**C-03**	논리 정보와 물리 위치의 단절 — 설비가 어디 붙어 있는지 찾는 데 시간이 더 걸립니다.
Part C	**C-04**	자산 이력의 단절 — 담당자가 바뀌면 그 설비의 이력이 끊깁니다.
Part C	**C-05**	전사 자산 현황의 부재 — 본사에서는 사업소 자산 현황을 알 방법이 없습니다.
Part C	**C-06**	가용성 우려 — 보안 시스템이 제어 운전에 영향을 줄까 봐 망설여집니다.
Part C	**C-07**	단계적 도입의 필요 — 통합 보안 모니터링까지 한 번에 가기에는 부담이 큽니다.

04 도입 방식 및 지원 체계

본 문서의 시나리오는 아래 구성과 유지보수 서비스 체계를 전제로 합니다.

▪ 구축 모델

모델	수용 규모	하드웨어	구성
Lite	~100 IP	PC	일체형
SMB	~300 IP	PC 또는 Server	일체형
Enterprise	Unlimited	Server	분산형

▪ 시나리오 수행을 지원하는 유지보수 서비스

항목	Basic	Standard	Premium
정기 방문 점검	연 1회	연 2회	연 4회
오탐 튜닝 (B-05 관련)	방문 시 수행	방문 시 수행	방문 시 수행
자산 · 취약점 리포트 (서비스 항목)	방문 시 수행	방문 시 수행	방문 시 수행
정기 리포트 (B-06 관련)	방문 시 수행	방문 시 수행	방문 시 수행
패치 제공	연 2회	연 2회	연 2회
원격 정기 점검 (C2 원격형)	반기 1회	분기 1회	월간 1회

※ 위 표는 유지보수 서비스 제공 항목이며 제품 기능이 아닙니다. 제품 하자 수정 · 장애 현장 출동 · 기술 문의 대응은 등급과 무관하게 전 계약에 동일 제공됩니다. 운영서비스(원격지원)는 계약 형태 · 등급과 무관하게 별도 요금 없이 제공됩니다.

> **단계적 확장 경로**
> Part C의 「단계적 도입의 필요」(C-07)에서 다룬 것처럼, ICS Asset Manager로 자산 가시성과 정책 체계를 먼저 확보한 뒤 동일 인프라에서 ICS Security Monitor로 업그레이드할 수 있습니다. 업그레이드 비용은 전 모델 공통 2,000만 원(VAT 별도)이며, 하드웨어 교체 없이 소프트웨어 업그레이드로 진행됩니다.

CONTACT

제품 · 견적 문의

주소 (우) 12902 경기도 하남시 미사강변한강로 135(망월동) 미사강변스카이폴리스 다동 1038~1039호

대표전화 031-792-0633 · Fax 031-792-0635

이메일 info@onsecurity.co.kr

홈페이지 www.onsecurity.co.kr