SSenStone

OT 환경 엔드포인트 디바이스 인증보안 & 접근 제어

# OT Auth Solutions

- PLC OTAC
- OTAC Trusted Access Gateway (TAG)

02-569-9668 | im@ssenstone.com | www.ssenstone.com

# OT Auth Solutions

PLC OTAC • OTAC Trusted Access Gateway (TAG)

## Challenges

산업 자동화의 확산으로 OT(Operational Technology)와 IT(Information Technology)가 통합된 제조 환경이 구축되고 있지만, 사용자와 기기 식별을 위한 고도화된 인증 시스템의 부족으로 수많은 기업과 국가 기간시설들이 여전히 외부 위협에 취약합니다. 발전소, 전력망, 국가 방어 시설 등 PLC를 사용하는 주요 시설들이 더욱 혁신적인 인증 보안 시스템을 필요로 하는 이유입니다.

## 비밀번호 기반 로그인의 치명적 보안 취약점

고정값 기반의 비밀번호 인증을 사용하는 OT 기기들은 외부 접근과 해킹에 취약하며, 악성코드 감염 위험까지 높아 효과적인 보안이 사실상 불가능합니다.

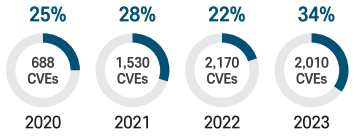
### PLC Access PW 사용 문제점

**비밀번호 공유**
- 규정 미준수 / 보안 규정의 허술함

**반복적인 비밀번호 노출**
- 해킹되는 비밀번호

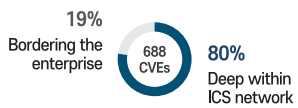
**비밀번호 규칙 강화 어려움**
- 비밀번호를 변경하지 않고 장기간 사용
- 비밀번호 분실

### OT 네트워크 인증 공격 증가



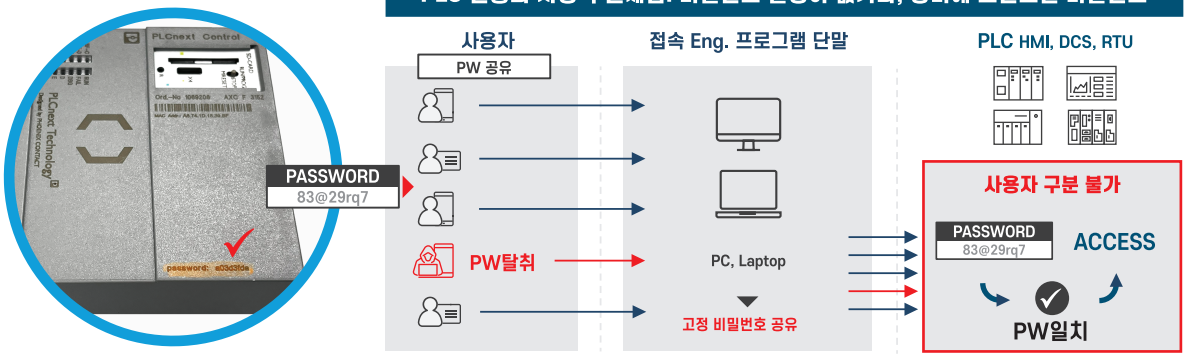

- 인증을 필요로 하는 OT 취약점의 증가
- 인증된 사용자의 권한이 탈취된 경우, 심각한 보안 문제 초래

### OT보안 취약점 80% ICS에서 발생




- 취약점의 80% : ICS 네트워크에서 발견
- 취약점의 62% : 레벨 0-3에서 발견

**병목구간 & End-Point 공격 대상 : PLC**




## OT 보안에서의 기준 규정 문제

NIS2, NERC CIP, IEC 62443, CRA와 같은 프레임워크를 포함한 OT 보안 규제 환경이 발전함에 따라 기업들은 엄격한 보안 기준을 충족해야 하는 압박을 받고 있습니다. 규정을 준수하지 않으면 심각한 금전적 제재, 브랜드 가치 손상 또는 서비스 중단과 같은 결과를 초래할 수 있습니다. 하지만 많은 기존 OT 시스템, 특히 구형 PLC는 고급 보안 조치를 지원하도록 설계되지 않아 규정 준수가 어렵고 비용이 많이 듭니다.

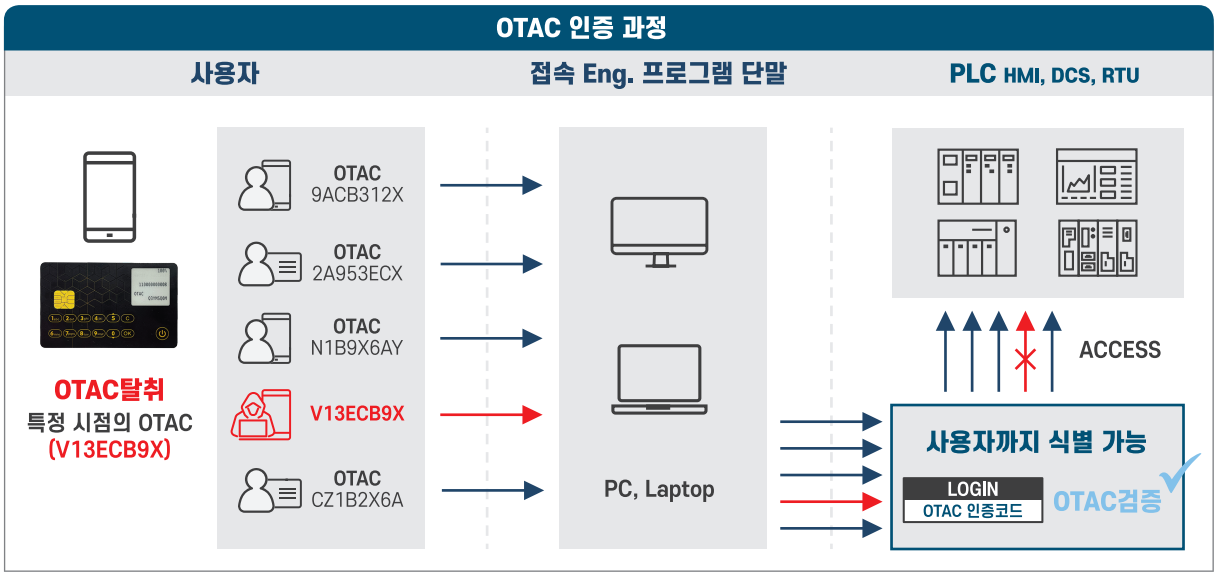
- NIS2, NERC CIP, IEC 62443, CRA와 같은 규정을 준수하기 위해서는 기존 OT 시스템에서 제공하는 것보다 더 고차원적인 보안 솔루션이 필요합니다.
- 비밀번호와 같이 고정값 기반 인증은 비밀번호 크래킹, 피싱, 무차별 공격과 같은 사이버 공격에 취약하여 규정 준수 요구 사항을 충족하기 어렵습니다.
- 기존 OT 시스템은 광범위하고 비용이 많이 드는 업그레이드 없이 최신 보안 솔루션을 수용하기 어렵습니다.
- 각국이 요구하는 규정과 표준을 준수하지 않으면 심각한 제재와 운영 중단에 처할 수 있습니다.

## Solution

센스톤의 OT Auth Solutions 제품군 - PLC OTAC • OTAC Trusted Access Gateway (TAG)-는 PLC, RTU, HMI, DCS 등 OT 기기 인증 취약점 문제 해결을 위한 글로벌 특허 보안 솔루션입니다.

## 복제 불가 다이내믹 인증코드로 비밀번호 취약점 근본적 해결

매번 다르게 생성되는 다이내믹 인증코드(OTAC)를 통해 접근 제어가 가능하며, 기존 8자리 비밀번호 인터페이스 및 인프라 교체 없이도 고도화된 인증 프로세스를 구현할 수 있습니다.




## OT 사이버 보안 규정 준수 해결

센스톤의 OT Auth Solutions 제품군은 OT 환경에 최적화된 고차원 인증 메커니즘을 통해 NIS2, NERC CIP, IEC 62443, CRA와 같은 규정 준수를 해결합니다.

### NIS2

**EU 전역의 사이버보안에 관한 지침**

OT 시스템에 대해 안전하고 비밀번호 없는 접근을 제공하여 고정값 기반 자격 증명의 취약점을 효과적으로 해결합니다.

**미준수 패널티**
- 필수 기업: 최소 1천만 유로 또는 글로벌 연간 매출의 2%
- 중요 기업: 최소 700만 유로 또는 글로벌 연간 매출의 1.4%

### NERC CIP

**북미 전력망 사이보보안을 강화하기 위한 규제**

OT 시스템에 대해 사용자 권한 기반 접근 제어 및 다중인증 절차를 구현하여 OT 인증 보안 취약점을 효과적으로 해결합니다.

**미준수 패널티**
- 위반의 심각도와 지속기간에 따라 일일 최대 100만 달러 벌금 부과
- Entergy 사례: PRC005-6 R3 위반으로 14만1천달러 벌금 부과

### IEC 62443

**IACS 보안 가이드라인 및 모범사례 제공 국제표준**

일회용 다이내믹 코드를 사용하여 FR1에서 요구하는 인증된 사용자만을 허용합니다. 또한, FR2에서 요구하는 명확한 감사 기록을 제공하여 시스템의 투명성과 보안성을 높입니다.

### CRA

**EU 전역 디지털 제품에 대한 최고 보안 수준의 의무화 표준**

기존 비밀번호 기반 시스템을 다이내믹 인증 코드로 대체하여 무단 접근의 위험을 최소화합니다.
이로 인해 인증 프로세스가 간소화되며, 보안성이 크게 향상됩니다.

SSenStone

Next Generation Authentication Security Lab

# Why SSenStone

전 세계 어디에서도 대체 불가능한 단방향 다이내믹 인증 기술인 센스톤의 OTAC(One-Time Authentication Code)가 적용된 PLC OTAC과 OTAC Trusted Access Gateway는 다양한 OT 기기의 고질적인 고정값 기반의 비밀번호 문제를 획기적으로 개선합니다. 이와 함께 다양한 OT환경에 최적화된 맞춤형 솔루션을 제공합니다.

| OTAC 알고리즘 분석 및 학술적 검증 | NET(New Excellent Technology) 인증 획득 | 단방향 다이내믹 인증보안 '국제 CC인증' 획득 | OTAC for Phygital 'IR52 장영실상' 수상 |
|---|---|---|---|
| UNIVERSITY OF SURREY | NET 신기술인증 NEW EXCELLENT TECHNOLOGY | ITSCC | IR52 장영실상 |

## 고도화된 OT 인증 보안을 통한 생산성 및 효율성 제고

센스톤은 PLC 제조사와 운영사가 최소한의 컴퓨팅 리소스만으로도 비밀번호 기반의 취약성을 제거하여 보안성을 높이는 것은 물론, PLC 순환정지에 맞춰 빠르고 원활하게 시스템을 적용할 수 있도록 지원합니다.

| | OTAC 도입 전 | OTAC 도입 후 | 도입 효과 |
|---|---|---|---|
| 비밀번호 타입 | Static : 6~8 자리 고정값 | Dynamic : 매번 변경되는 값 | 다이내믹 코드이므로 탈취되더라도 재사용 불가<br>▷ 재사용 공격(해킹) 불가 |
| 비밀번호 설정 | 관리자가 (기기별) 설정 | (설정 필요 없음) | 매번 변경되는 다이내믹 코드이므로 관리자에 의한 비밀번호의 수동설정 불필요 > 운영(설정 관리)리소스 절감 |
| 비밀번호 관리 | 지정된 비밀번호 공유 필요 | (공유 필요 없음) | 다이내믹 코드만으로 사용자 식별 가능<br>▷ 비밀번호 공유에 따른 보안 위험 차단 |
| | 비밀번호 변경 관리 어려움 | (변경 관리 필요 없음) | 매번 변경되는 다이내믹 코드이므로 관리자에 의한 비밀번호의 변경관리 불필요 ▷ 운영(설정 관리) 리소스 절감 |
| ACL 관리 | 사용자별 액세스 관리 어려움<br>* 퇴사자, 외부인에 대한 관리 어려움 | 사용자별 액세스 관리 용이 | 다이내믹 코드만으로 기기별(PC 또는 PLC) 계층화된 접근 관리 용이 ▷ 비밀번호 탈취/공유로 기기의 액세스 방지 |
| 인증 | 고정된 비밀번호로 인증<br>* 고정값인 비밀번호 입력 후 인증 | 다이내믹 코드로 인증<br>* 사용자 등록 기기에서 생성된 (다이내믹)코드로 인증 | 다이내믹 코드 하나로 사용자/기기 식별 및 인증<br>▷ 사용편의성 보안성 향상 |
| **유지 관리 측면의 운영 효율성** | | ▷ Lightweight Algorithm으로 경량 모듈에 적합 (기기 사양의 제약이 없음)<br>▷ 기존 패스워드 자릿수 조건에 맞추어 다이내믹 코드 생성 가능<br>▷ 기존 시스템의 변경을 최소화하여 적용 가능 | |

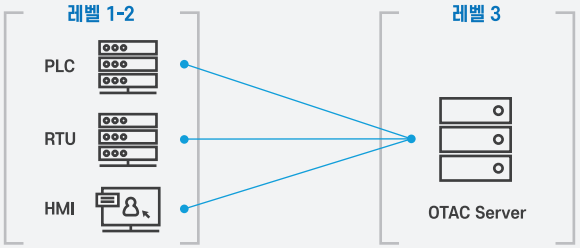
## 다양한 OT 환경에 최적화된 유연한 인증 및 접근 제어 보장

센스톤은 기존 OT 환경을 변경하지 않고 PLC 기기나 중앙 서버에서 사용자 인증을 수행하는 방식(PLC OTAC)과, PLC 수정이나 제조사 지원 없이 고객이 직접 OT 시스템의 인증 및 접근 제어를 고도화 하는 방식(OTAC Trusted Access Gateway)을 지원합니다.

### PLC OTAC

**레벨 1~2의 End-Point에 직접 적용**

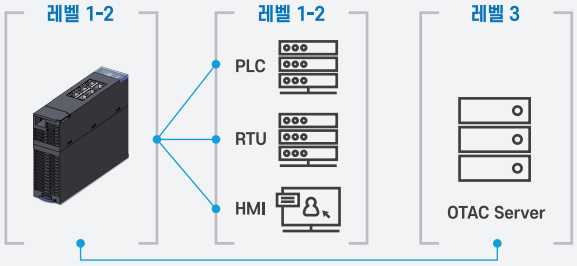
- 퍼듀모델* 레벨 1~2의 End-Point 장비에 검증모듈이 설치되어 OTAC서버에서 인증 (서버형일 경우)
- 기존 OT 환경의 변경 최소화
- PLC 제조사의 지원을 받아 적용 가능




### OTAC Trusted Access Gateway

**레벨1~2의 End-Point의 앞 단에 별도로 적용**

- Agent가 설치되어 OTAC Trusted Access Gateway에서 OTAC 서버를 호출하여 인증
- 기존 OT 환경의 변경 없음
- PLC 제조사의 지원 없이도 적용 가능




* 퍼듀 모델이란? ICS 네트워크의 보안 계층을 설명하는 구조적 모델
  - 레벨2: 실시간 모니터링 및 제어를 수행하는 SCADA 및 HMI 시스템이 있는 레벨
  - 레벨1: PLC 및 RTU 같은 제어 장치가 위치한 레벨