swidch

Authentication & Access Control for OT Endpoint Devices

OT Auth Solutions

- PLC OTAC
- OTAC Trusted Access Gateway (TAG)

(+44)20-3283-4563 | info@swidch.com | www.swidch.com

OT Auth Solutions

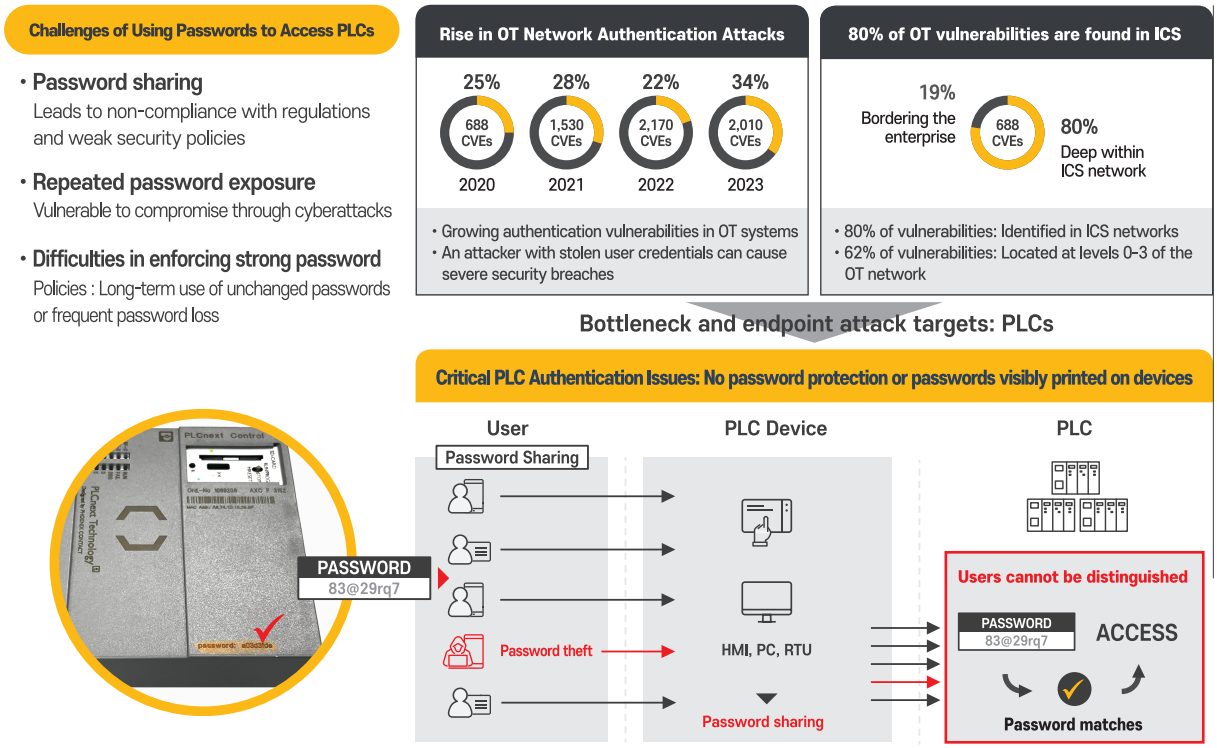
PLC OTAC • OTAC Trusted Access Gateway (TAG)

Challenges

As industrial automation expands, an integrated manufacturing environment combining operational technology(OT) and information technology (IT) is taking shape. However, many critical infrastructure facilities remain highly vulnerable to external threats due to the lack of an advanced authentication system for user and device identification. This highlights the urgent need for more innovative authentication systems in major facilities that rely on PLCs, such as power plants, power grids, and national defence infrastructure.

Critical vulnerabilities of password-based login

OT devices that rely on fixed-value password are highly susceptible to unauthorised access and hacking. The risk of malware infection is also significant, making effective security virtually impossible.



Compliance challenges in OT security

With evolving OT security regulations such as NIS2, NERC CIP, IEC 62443, and CRA, organisations are under increasing pressure to meet stringent security standards. Non-compliance can lead to severe financial penalties, reputational damage, and service disruptions. However, many legacy OT systems—particularly older PLCs—were not designed to support advanced security measures, making compliance both challenging and costly.

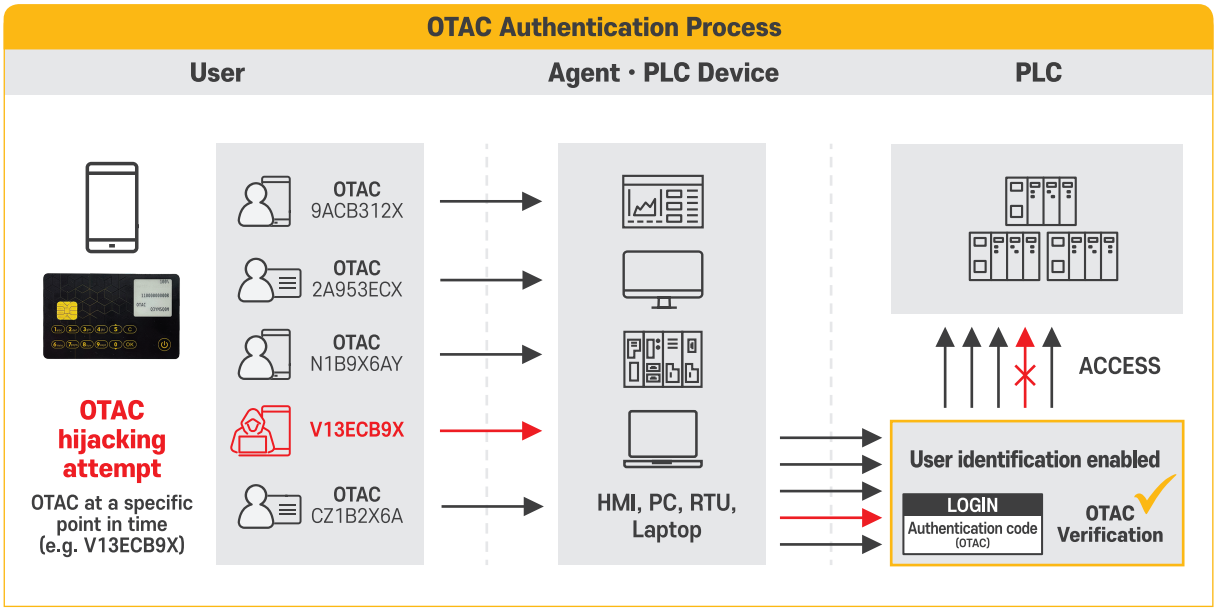
- Compliance with regulations such as NIS2, NERC CIP, IEC 62443, and CRA demands a more advanced security solution than legacy OT systems can provide.
- Static authentication methods, such as passwords, are highly vulnerable to cyberattacks, including password cracking, phishing, and brute-force attacks, making compliance difficult.
- Many existing OT systems lack the capability to integrate modern security solutions without extensive and costly upgrades.
- Failure to comply with country-specific regulations can result in significant penalties and operational disruptions.

Solution

swIDch's OT Auth Solutions product line—PLC OTAC and OTAC Trusted Access Gateway (TAG)—is a globally patented security solution designed to address authentication vulnerabilities in OT devices such as PLCs, RTUs, HMIs, and DCSs.

Eliminating Password Vulnerabilities with a Unique Dynamic Authentication Code

By generating a unique dynamic authentication code (OTAC) for each access attempt, we enable robust access control without requiring modifications to the existing 8-digit password interface or infrastructure.



Addressing OT Cybersecurity Compliance

swIDch's OT Auth Solutions ensure compliance with regulations such as NIS2, NERC CIP, IEC 62443, and CRA by implementing a high-level authentication mechanism tailored for OT environments.

NIS2

EU-Wide Cybersecurity Directive

Provides secure, passwordless access to OT systems, effectively mitigating vulnerabilities associated with fixed-value credentials.

Non-compliance penalties:

- Essential Entities: At least €10M or 2% of global annual revenue
- Important Entities: At least €7M or 1.4% of global annual revenue

NERC CIP

Strengthening Cybersecurity in the North American Power Grid

Enhances OT authentication security by enforcing user rights-based access control and multi-factor authentication.

Non-compliance penalties:

- Fines up to $1M per day, depending on the severity and duration of the violation
- Example: Entergy was fined $141,000 for violating PRC005-6 R3

IEC 62443

International Standard for IACS Security

- Uses one-time dynamic authentication codes to restrict access to authenticated users as required by FR1.
- Ensures transparent audit logs as required by FR2, enhancing system security and accountability.

CRA

EU's Mandatory Cybersecurity Standard for Digital Products

- Replaces password-based systems with dynamic authentication codes, minimising the risk of unauthorised access
- Simplifies authentication processes while significantly improving security

Why swIDch

PLC OTAC and OTAC Trusted Access Gateway (TAG) utilise swIDch's unique one-way dynamic authentication technology—One-Time Authentication Code (OTAC)—which cannot be replicated anywhere in the world. These solutions eliminate static password vulnerabilities in OT devices while providing tailored security solutions for diverse OT environments.

OTAC Algorithm Analysis and Academic Verification

UNIVERSITY OF SURREY

International CC Certification for OTAC

COMMON CRITERIA(CC) CERTIFICATION swIDch

Over 330 patents granted and pending worldwide

★ PATENTED ★

Enhancing Productivity & Efficiency Through Advanced OT Authentication

swIDch enables PLC manufacturers and operators to eliminate password-based vulnerabilities with minimal computing resources, ensuring both security and seamless system integration during PLC shutdown cycles.

Before OTAC (Static Passwords)		After OTAC (Dynamic Authentication)	Benefits
Password Type	6-8 digit fixed password	Dynamic, changes every time	Eliminates reuse attacks: Dynamic codes cannot be reused
Password Setting	Manually set for each device	No manual setup required	Reduces operational burden: No need to manually set or manage passwords
Password Management	Requires sharing between users	No need to share	Prevents password sharing risks: User identification via dynamic authentication
	Difficult to manage	No need to update manually	Eliminates manual password management with dynamic codes, reducing operational burden
Access Control	Difficult to manage access for ex-employees & third parties	Easy user-based access management	Simplifies access management: Hierarchical device access control without passwords
Authentication	Static password entry	Dynamic code authentication	Improves usability & security: One dynamic code for both authentication and user/device identification

Improved operational efficiency in maintenance

- ▷ Designed for compact modules with an efficient algorithm (no hardware limitations)
- ▷ Generates dynamic codes that meet existing password length requirements
- ▷ Easily integrates with minimal changes to the current system

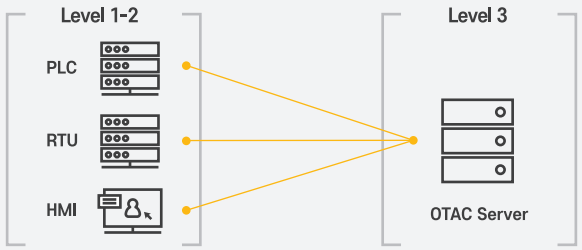
Flexible Authentication & Access Control for Various OT Environments

swIDch offers two deployment options: PLC OTAC, which integrates authentication directly into PLC devices or manages them via central servers without altering existing infrastructure, and OTAC Trusted Access Gateway (TAG), which enhances authentication and access control without modifying PLCs or requiring manufacturer support.

PLC OTAC

Directly Applied to Level 1-2 Endpoints

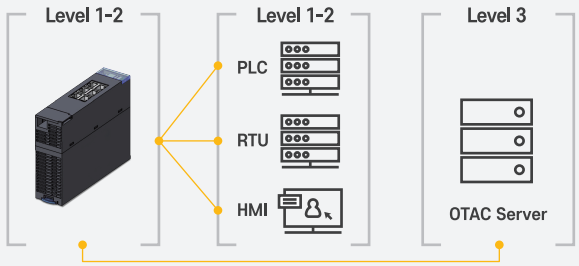
- OTAC verification module installed in Level 1–2 devices of the Purdue Model*
- Minimal impact on existing OT infrastructure
- Requires support from PLC manufacturers



OTAC Trusted Access Gateway

Applied in Front of Level 1-2 Endpoints

- An agent on each OT device lets OTAC Trusted Access Gateway call the OTAC server for authentication.
- No changes required in existing OT infrastructure
- Can be deployed independently without PLC manufacturer support



* The Purdue Model is a hierarchical framework for ICS network security.
  - Level 2: SCADA and HMI systems for real-time monitoring and control.
  - Level 1: Control devices such as PLCs and RTUs.