www.swidch.com

PLC OTAC

Single-step MFA to OT Security Reinvented

swidch

☎ +44-24-7542-4987 | ✉ info@swidch.com

PLC OTAC

Programmable Logic Controller One-Time Authentication Code

Challenges

As industrial automation grows, OT and IT are converging in manufacturing. Yet, without strong authentication, many organizations remain exposed to threats. Notable incidents, like PLC attacks on water treatment systems in Israel and the U.S., nearly led to contamination and chemical hazards, underscoring the urgent need for advanced security in critical facilities such as power plants, electric grids, and defense systems.

Fatal Security Vulnerabilities of Password-based Logins

The password-based authentication used in OT devices leaves them vulnerable to external access and hacking, and it significantly increases the risk of malware infections, rendering effective security nearly impossible.

PLC Password Security Challenges

Password sharing

- Non-compliance with best practice
- Incompatible with security regulations

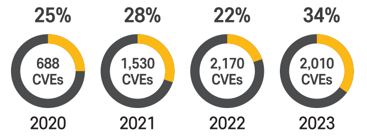
Repeated password exposure

- Compromised passwords

Difficulty enforcing password rules

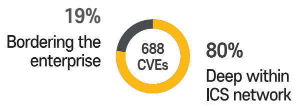
- Extended use of unchanged passwords
- Forgotten passwords

Rising Security Attacks on OT Authentication



- Increasing OT vulnerabilities requiring authentication
- Compromised user credentials pose serious risks

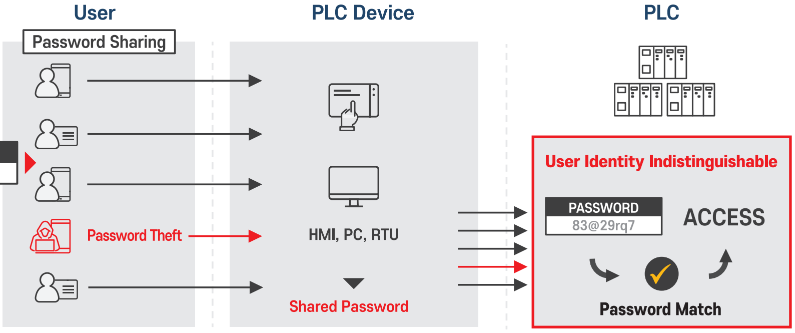
80% of OT Security Vulnerabilities Are in ICS



- 80% of vulnerabilities: Found in ICS networks
- 62% of vulnerabilities: Found at Levels 0-3

Bottleneck & End-Point Attack Target: PLC

Critical Issue with Existing PLC Authentication: Password Printed on Equipment



Compliance Issues in OT Security

As the regulatory compliance environment for OT security evolves, with frameworks such as NIS2, CRA, and IEC 62443, organisations face increasing pressure to meet stringent security standards. Non-compliance can result in severe financial penalties, reputational damage, and operational disruptions. However, legacy OT systems, especially older PLCs, often lack the necessary security features, hindering compliance efforts.

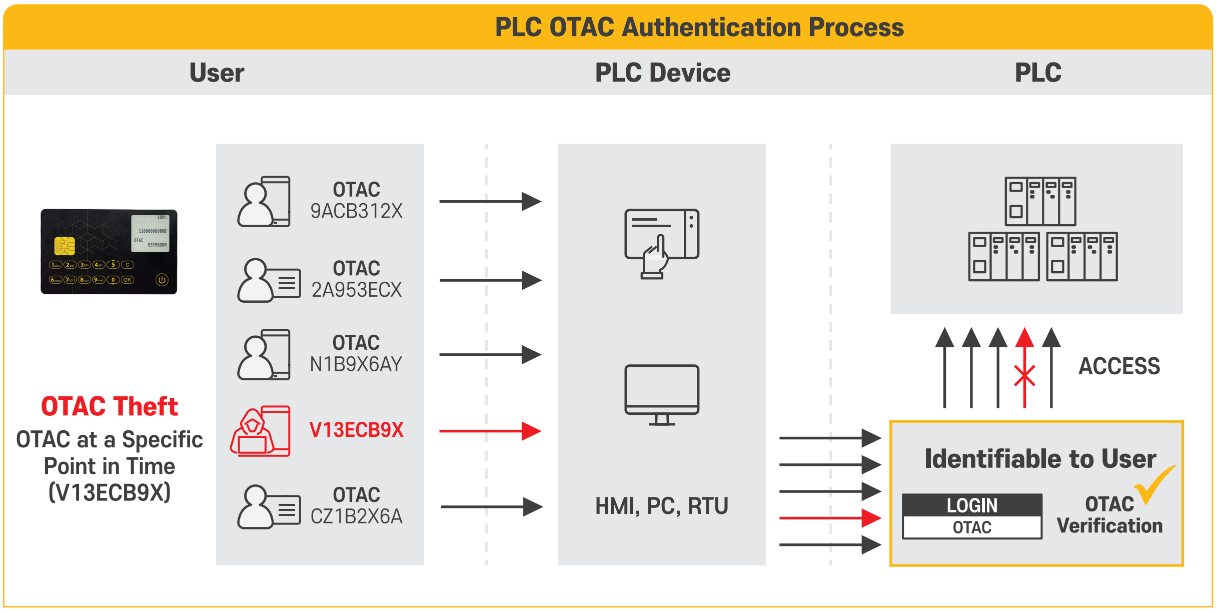
- Compliance with NIS2, CRA, and IEC 62443 requires stronger security than current OT systems offer.
- Fixed-value authentication (e.g., passwords) is vulnerable to attacks, making compliance with strict standards difficult.
- Existing OT systems struggle to adopt new security without costly upgrades.
- Non-compliance with national regulations risks heavy sanctions and operational shutdowns.

Solution

swIDch's Programmable Logic Controller OTAC is a globally patented authentication solution designed to address OT device authentication vulnerabilities, including PLC, RTU, SCADA, and HMI.

Eliminating Password Risks with Dynamic, Non-Replicable Codes

Dynamic authentication codes (OTAC) enable access control by generating unique codes each time, enhancing security without changing the existing 8-digit password setup.



Achieving Compliance with OT Cybersecurity Regulations

swIDch's PLC OTAC meets all regulations, including NIS2, CRA, and IEC 62443, through a high-level authentication mechanism optimised for the OT environment.

IEC 62443

An international standard for IACS cybersecurity guidelines

It allows only authenticated users as required by FR1 through the use of one-time dynamic codes. Additionally, it provides clear audit trails as required by FR2, enhancing system transparency and security.

NIS2

Guidelines for cybersecurity across the EU

It effectively addresses the vulnerabilities of fixed-value credentials by providing secure, passwordless access to OT systems. This ensures all security measures required by NIS2 are met.

CRA

A mandate for the highest security standards for digital products across the EU

It minimises the risk of unauthorised access by replacing existing password-based systems with dynamic authentication codes. This simplifies the authentication process and significantly enhances security.

Why PLC OTAC?

swIDch was recognised as the winner in the OT Security category at the 2024 Top InfoSec Innovator Awards.

> “ swIDch embodies the innovative spirit we seek in award winners—anticipating future threats, offering cost-effective security solutions, and delivering creative strategies that protect OT systems from growing cyber risks. ”

- Gary Miliefsky, Chair of the Top InfoSec Innovator Awards Judges

Enhancing Productivity and Efficiency with Advanced OT Authentication

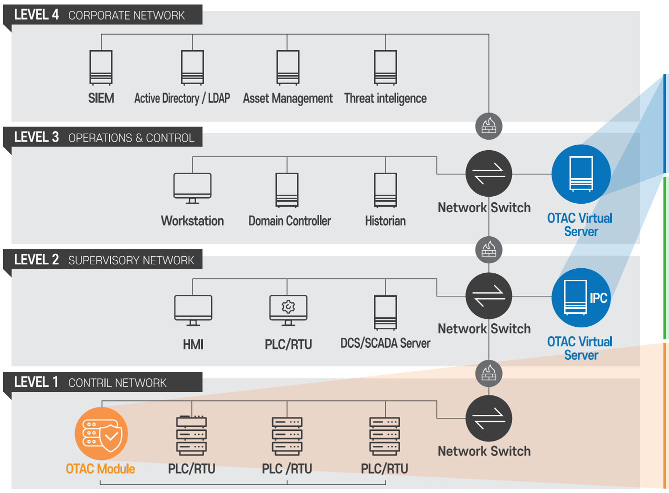
swIDch's PLC-OTAC eliminates password-based vulnerabilities with minimal computing resources for PLC manufacturers and operators, increasing security while supporting smooth system integration to minimise system downtime.

Pre-OTAC Deployment		Post-OTAC Deployment	Benefits
Password Type	Static: Fixed 6-8 character value	Dynamic: Changing value every time	Dynamic codes can't be reused if compromised. ▷ Prevents reuse attacks.
Password Setting	Set by administrator (per device)	(No need for setup)	No manual password setup needed. ▷ Reduces setup management resources.
Password Management	Requires sharing passwords	(No need for sharing)	Users are identified by dynamic codes only. ▷ Eliminates risks of password sharing.
	Hard to manage password changes	(No need for change management)	No password change management required. ▷ Reduces setup management resources.
ACL Management	Difficult to manage user access * Difficult to manage former employees & 3rd parties	Easy access management per user	Single dynamic code for user/device authentication. ▷ Prevents access due to password theft.
Authentication	All users use a static password * Authenticated after password	Authenticate with dynamic code per user Dynamic code authentication	Tiered access management by device with dynamic codes. ▷ Enhances usability and security.
Operational Efficiency in Maintenance		▷ Suitable for lightweight modules with lightweight algorithms (no device specification constraints) ▷ Capable of generating dynamic codes according to existing password length requirements ▷ Can be applied with minimal changes to existing systems	

Custom Models of PLC OTAC by OT Level

swIDch offers three PLC OTAC models optimised for various OT environments. These models ensure flexibility by performing user authentication on PLC devices or a central server, or through a hybrid management approach combining both.

PLC OTAC Application Levels



Application Models

	Manufacturer's Scope of Work	Remarks	Error Handling Measures
Server Model	• Modify authentication /communication modules • Add time synchronization	• Use idle servers or IPC • Development needed per PLC model	• In case of network disconnection or server failure, log in with password under limited permissions
Hybrid Model (Server+ Module)	• Modify authentication modules • Add time synchronization • Integrate OTAC module • Requires 200KB storage for 10 users		• In case of network disconnection or server failure, log in with OTAC module type • If there is an error in the OTAC module type, log in with password under limited permissions
Standalone	• Add time synchronization • Integrate OTAC module • Requires 200KB storage for 10 users	• Use idle servers or IPC • Development needed per PLC model	• If there is an error in the OTAC module type, log in with password under limited permissions