swidch

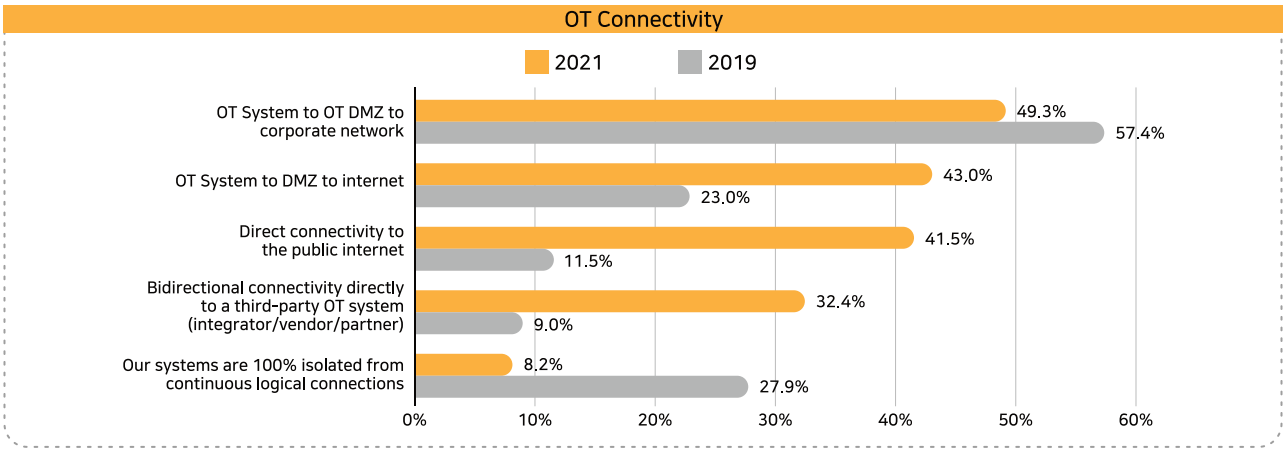
Enabling connected enterprise beyond security

Programmable Logic Controller OTAC

Highly optimised and highly secure authentication solution to resolve global PLC vulnerabilities

Programmable Logic Controllers (PLC) serve as key component of ICS and OT systems and are equally susceptible to cyber-attacks, with inadequate access control and authentication within these systems posing a major challenge. As a result, 93% percent of all organizations with OT environments experienced hacking in the past twelve months by June 2022 with over 78% percent confronted with three or more security incidents. The result is increased demand for enhanced authentication for ICS/IACS and ICS component manufacturers are now actively reviewing the design architecture in building robust password-based credentials.

Changes in the ICS network environment



Note: Increased external connectivity in OT environments
<Source: 2019 vs 2021, A SANS 2021 Survey: OT/ICS Cybersecurity>

Pain points in ICS and OT systems

Traditional Operational Technology (OT) & Information Technology (IT) environments were separate, meaning OT owners relied on the 'air gap' that separated OT from IT systems in order to protect them. Cloud Computing & IoT (Internet of Things) aims to connect OT & ICT (Information and Communication Technology) infrastructure to various devices using different network connectivity technologies, but this bridging of the traditional 'air gap' has resulted in widened endpoints to the industrial network, leaving Industrial Control Systems (ICS) exposed to ever-increasing security risks and vulnerabilities.

Weak authentication in current PLC systems

The password-based credential is commonplace and still being used as an authentication mechanism for human users and processes. However, passwords bring with them significant challenges. These include password sharing, password management, user changes (leavers/contractors) and inherent password weaknesses (static information vulnerable to brute forcing, phishing, credential stuffing etc).

24/7 operation limits OT security upgrades

Many PLCs power mission critical operations, which often need to operate continuously. This means updates to PLCs including applying security patches and enhancing the security stacks are difficult to manage. Once an ICS facility begins to operate, the inherent vulnerabilities within these systems remain. This is common knowledge amongst threat actors resulting in these systems being a constant target.

Reluctance to upgrade existing OT/PLC systems

In addition, security upgrades to existing OT systems often require significant time, manpower and resources, which in turn pose considerable cost implications for ICS and OT organisations and manufacturers. As a result, many PLCs continue to operate despite inherent vulnerabilities, leaving PLCs and the systems they operate at considerable risk.

swidch

Get in touch

info@swidch.com
www.swIDch.com

swIDch Ltd, Office 176, 1st Floor,
3 More London Riverside London SE1 2RE

swIDch

Enabling connected enterprise beyond security

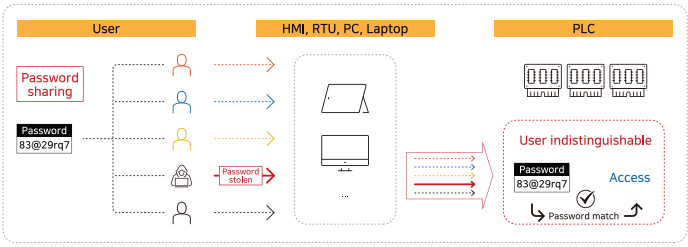
The Solution

swIDch's Programmable Logic Controller OTAC provides a highly optimised and highly secure authentication solution specifically for PLC devices. It utilises our dynamic 'One-time authentication code' (OTAC) technology to resolve typical ICS/OT security challenges. OTAC ensures only known and authorised users/devices can access PLC using dynamic, non-reusable, constantly changing code guaranteed with 0% duplicates (defeats packet sniffing attacks).

OTAC resolves

- Password sharing in password-only authentication systems
- Difficulty managing ID/PW specified for each PLC device
- Difficulty managing user changes (leavers / contractors etc)
- Hacking attempts using password cracking software

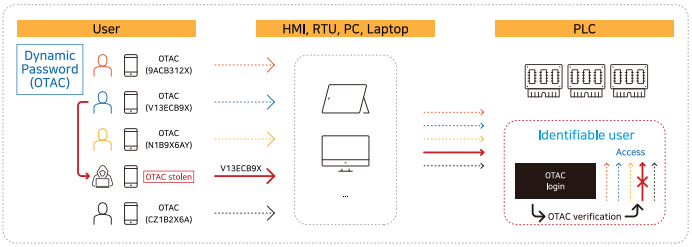
Current PLC certification: Password-based



Issues with current PLC certification using just passwords

1. Password sharing between engineers
2. Access is granted to users who are indistinguishable (un-identified)
3. If a password is stolen (from any user) it can be later used to gain access without any further challenge

Optimal authentication method: OTAC based authentication



Issues resolved by using OTAC-based authentication

1. No password sharing – users enter dynamic codes (OTAC) which are generated differently each time
2. Access is only granted to authorised users – who are also fully identifiable
3. If the OTAC is stolen and later used it will be denied access by the OTAC verification module
4. All of this is possible without any need to modify the existing password interface (8-digit example above)

Benefits

swIDch's Programmable Logic Controller OTAC allows manufacturers and operators to significantly increase security with minimal disruption and minimal computing requirements whilst at the same time removing password associated vulnerabilities, and thus greatly simplifying the authentication process. Increasing productivity and efficiency, which are critical components of all ICS and OT systems, leads to improved competitiveness for organisations that require production and service automation.

Manpower and cost saving

Efficient user and device authentication management can reduce time and manpower requirements. You can not only reduce costs compared to PKI authentication methods, but also expect significant cost saving when compared to alternative solutions.

Improved productivity and efficiency

PLC OTAC provides lightweight SDK/applet enabling implementation of code generator in multiple forms. It requires low CPU overhead for the code verifier which can be implemented on a central backend server or in lightweight module on the PLC itself. Its highly configurable code parameters enable deployment on existing infrastructure with minimal, inexpensive UI changes.

Advanced security environment

PLC OTAC not only resolves password-based PLC system vulnerabilities by blocking indistinguishable user access through unique dynamic codes for each user, but also provides a more robust, less demanding security environment by supporting uni-directional authentication code generation, even in unstable network environments.

swIDch

Get in touch

info@swidch.com
www.swIDch.com

swIDch Ltd, Office 176, 1st Floor,
3 More London Riverside London SE1 2RE