

Secure OT Access in a Hyperconnected World

24 June 2026, 16:00

Annanda Rath

Identity and access management for connected industrial environments

Industry 4.0 is reshaping manufacturing and improving efficiency, performance and competitiveness. As more machines and systems become connected, exposure to cybersecurity risks increases. Legacy OT devices often cannot support modern security solutions because of technical limitations. Secure identification and access control therefore provide an essential layer of protection. New regulations such as NIS2 and the Cyber Resilience Act (CRA) make this challenge even more urgent.

Key components of secure OT access management

Secure OT access management combines several complementary measures:

1. **Centralised identity repository:** a unified directory maps human and machine identities. This helps prevent unmanaged, rogue devices and unknown assets from appearing on the factory floor.
2. **Secure remote access:** secure bastion hosts and industrial demilitarised zones (iDMZs) isolate OT networks from the public internet. This allows remote engineers to perform maintenance activities without creating direct network exposure.
3. **Advanced authentication:** attack-resistant multifactor authentication (MFA) secures both local and external logins, especially for accounts that can issue critical control commands. Certificate-based authentication can provide additional protection while maintaining operational continuity.
4. **Privileged access management and least privilege:** access credentials should be managed securely. Remote sessions can be monitored or recorded when needed. Users should receive only the permissions required to perform their specific tasks.
5. **Continuous monitoring and auditing:** continuous monitoring tracks user activity and records configuration changes. Regular audits help identify inactive accounts and excessive privileges before they create security risks.
6. **Zero Trust architecture:** a Zero Trust approach follows the principle of “never trust, always verify”. Every session, whether initiated by a person or a machine, must be authenticated and authorised before access is granted.



Demonstrator's key features

The access control system we developed combines these technologies to deliver advanced security capabilities:

- **Secure user identification and access control:** SSI enables decentralised identity management, user-controlled data and privacy-preserving authentication through selective disclosure mechanisms.
- **Trusted access logging:** blockchain technology provides tamper-resistant logging of access events and ensures transparent traceability.
- **Reliable auditing and compliance support:** verifiable and immutable records support audits and help organisations comply with evolving cybersecurity regulations.
- **Offline authentication capability:** the solution supports secure authentication even when devices are temporarily disconnected from IT or OT networks.

SecuWeb: addressing OT security challenges

Within the [SecuWeb project](#), Sirris and its partners address these challenges through practical research and innovation. The project explores methods, technologies and procedures that enable secure identification and access control for users and operators in OT environments. By combining emerging technologies such as Self-Sovereign Identity (SSI), Solid and blockchain, the project team has developed a state-of-the-art demonstrator for identity management and access control.

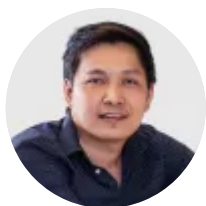
[Discover the SecuWeb project](#)

Join the SecuWeb project as an industrial partner

Would you like to explore innovative cybersecurity solutions in an industrial setting? Within the SecuWeb project, we are looking for industrial partners to collaborate on real-world use cases and validate new approaches to identity and access management in OT environments. Let's discuss your challenges and explore how these technologies can support your organisation.

[Let's talk](#)

Authors



Annanda Rath