Role of Identity and Access Management in Operational Technology Security

January 2024

pwc

Introduction

Cyber-threats and cyber-attacks are no longer limited to the digital world. As the silos between technologies and different sectors are disappearing, so too are the silos between various aspects of security.

As indicated by the International Energy Agency, Cyber attacks against the energy sector are on the rise. A recent example comes from PwC's tracking of and reports from Israel's and American government organizations about a threat actor using personas such as "Soldiers of Solomon''. This threat actor has been targeting the Israeli and American Water and Wastewater (WWS) Industry. The objective is to try to compromise the PLCs (Programmable Logic Controllers) that are part of the Unitronics Vision series. This is just one of the several threats in the sector, where attacks and their detection is underreported.

The purpose of OT security is to prioritize Safety, followed by Availability, Integrity, and finally Confidentiality – in that order. Conventional IAM principles do not directly apply to OT security – however, when tailored to meet OT requirements, IAM can help bridge this gap and protect infrastructure better.

Challenges around OT and its security

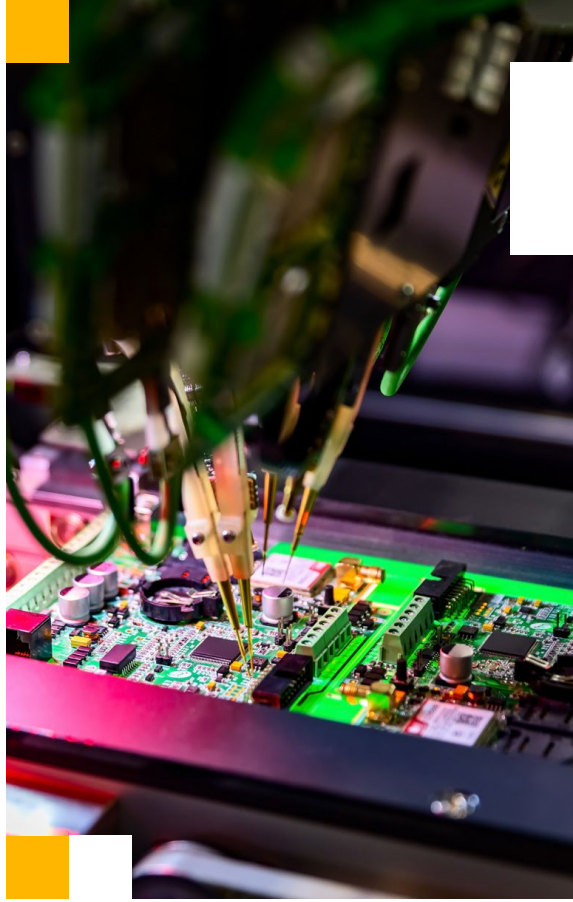
As all systems move towards a completely digital landscape, the need for an evolved approach towards security is becoming necessary. The critical infrastructure sector faces numerous challenges with respect to OT and cybersecurity.

- Use of shared-accounts and credentials, especially for critical infrastructure using legacy hardware/software
- OT systems have no or limited support for secure authentication and remote-access capabilities
- Connections between legacy systems and cloud infrastructure are not compliant with latest security standards
- Complications with patching and updating IT infrastructure due to high availability requirements
- Lack of policies and controls for providing secure access to 3rd parties.

Some of the prominent breaches of the OT security due to the compromised IAM include;

- **Maersk** – Compromised privileged account
- **Florida water treatment Plant** – Outdated OS and Ungoverned shared account
- **Colonial Pipeline Case** – Leaked password of a dormant account having access to VPN
- **Norsk Hydro** – Email infected ransomware
- **Tower Semiconductors** – Ransomware.

Some of the major breaches in the OT sector are due to the lack of management of identities and accesses. This should force the Cyber Security team to look into the identity and access management with more focus to identify the gaps and address before another severe disruption.



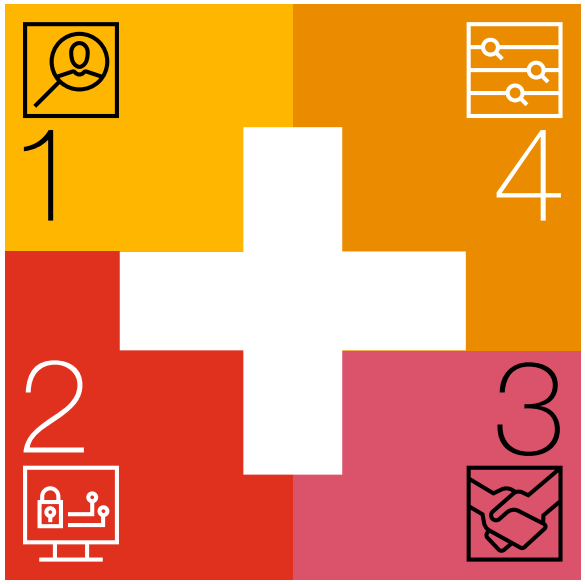
Key regulations governing the OT Security and IAM

Considering the severity of OT and its security around accesses, different governing bodies have formulated regulations and frameworks to reduce the OT security breaches, especially around the identities and accesses. Some of the more prominent include;

- **IEC – 62443** – A framework to address and mitigate security vulnerabilities in industrial automation and control systems (IACSs)
- NIST Frameworks – **NIST 800-82 ICS Security** and **NIST IR 8183 Cyber Security Framework for Manufacturing**
- **NCSC Ireland – OT Security Framework**

Understanding the IAM with the OT Context

Utilising the principles of Identity and Access Management in OT security and protecting critical infrastructure requires a modified approach. Various principles of logical security, such as Privileged Access Management, Zero trust, least privilege principle, and others, can help provide a greater level of security for OT systems.



1. Physical Access & Governance

Physical security is the first line of defense for the OT sector. All critical areas, control centers, as well as portable devices require physical access controls. Surveillance systems, including video surveillance, as well as monitoring as to how the granted access is used, are also key elements of this aspect.

2. Identity Governance & Administration

The OT sector must approach identity governance and administration with a centralized management system that focuses on context-based access management. The principles of Zero-Trust, Role & Attribute-based access control, as well as Segregation of Duties are key factors in enhancing identity security. In cases where digital access management is not feasible, appropriate physical security acts as a compensating control.

3. Access Enforcement

Authentication (verifying the identity of a user) and authorization (determination of the level of access) are the 2 pillars of access enforcement. Physical security can be further enhanced through biometric-based authentication. Multi-Factor Authentication (MFA), Single-Sign On (SSO), and Passwordless authentication for both human and non-human users (for example BOT IDs) can strengthen access control.

4. Monitoring and Reporting

Just-In-Time (JIT) and Just–Enough-Time (JET) help to reduce the risk caused due to standing privileges and ensuring that accounts only have the lowest administrative privileges possible which are strictly necessary to complete the tasks on-hand. Along with this, monitoring of access usage, periodic review and remediations of risk, and risk-score based evaluation would help organizations better address and report risk.

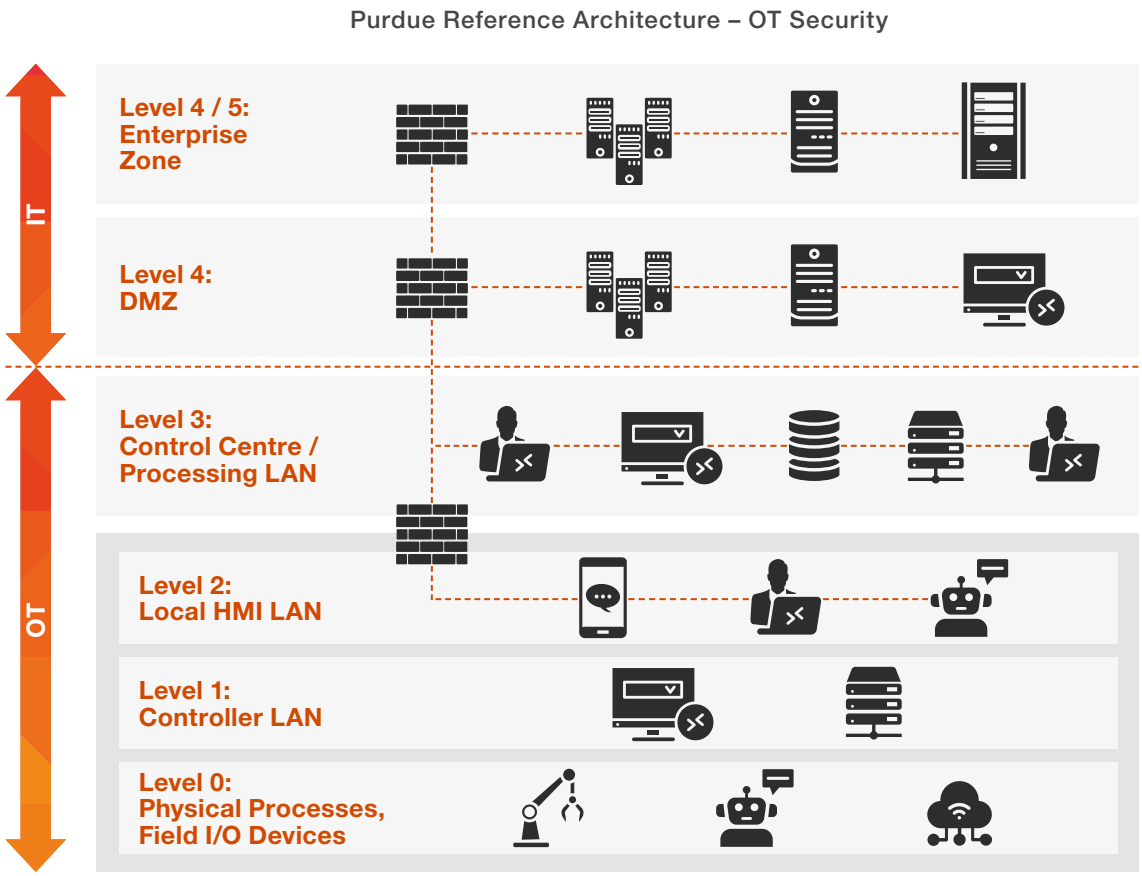
Applicability of IAM in OT Security

Any industrial control systems' security is divided between Information Technology (IT) and Operational Technology (OT), and maximum efficiency is gained through effective management of IT and OT.

Both IT and OT have their own cyber risks and lately, they are converging. With the advancement of Internet of Things (IoT), the convergence has accelerated in terms of process, technology and the integrations.

Though the security of both IT and OT is important, the priorities for both systems are different. In IT security, Confidentiality takes the precedence followed by integrity and availability, while in OT security, Availability and Integrity (along with Safety) takes precedence followed by Confidentiality.

A typical manufacturing environment is divided into zones to help automate the large-scale facilities. The security architecture for such an environment is described through purdue reference architecture.



Personas in action

- Privileged accounts (human / non-human)
- BOT IDs
- Regular human accesses
- Service accounts
- Server certificates

- Privileged accounts (human / non-human)
- BOT IDs
- Regular human accesses
- Service accounts
- Server certificates

- Human privileged accounts
- Regular accesses (servers)
- BOT IDs

- Service accounts
- BOT IDs
- Privileged accounts (human / non-human)

- BOT IDs
- Service accounts

Applicability of IAM

- Identity & Access lifecycle – JML automation
- RBAC, ABAC, SOD
- Access certification
- Authentication – MFA, Passwordless
- Authorization
- Privileged identity management
- Privileged access management

- Access certification
- Authentication – MFA, Passwordless
- Authorization
- Privileged identity management
- Privileged access management

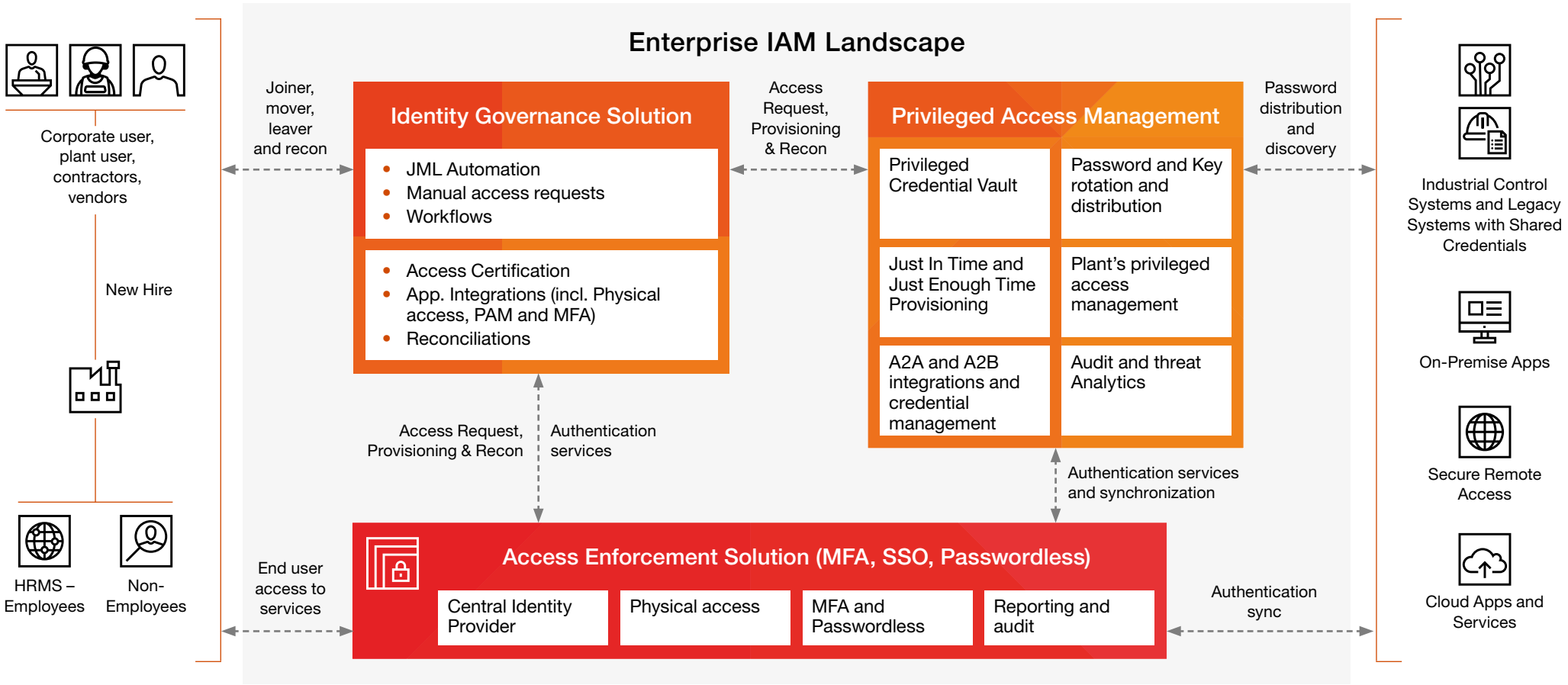
- Access certification
- Privileged Identity and access management
- Authentication – MFA
- Certificate Management

The interoperability of OT components, different personas and the applicability of IAM principles is handled through efficient IAM architecture and careful design of the use cases. In the following sections, the reference IAM architecture and some of the sample use cases are listed.

IAM Reference Architecture

In order to fulfill the IAM architectural requirements and address the key use cases for OT security, a sample IAM reference architecture is shown. The key use cases include that of end user's access and their lifecycle, automated JML process, access enforcement through MFA and SSO and the access governance to cover the access certification from the plant line manager and the remediation process.

Typical IAM Reference Architecture



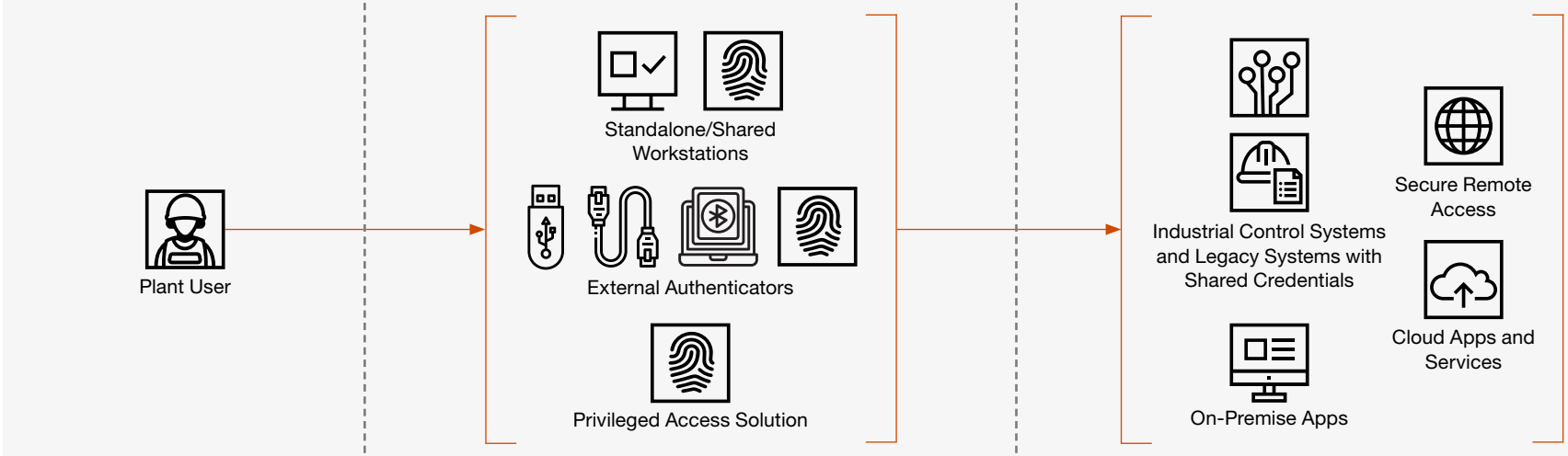
Sample Use Case Illustrations

Some of the sample use cases and user stories help us to visualize the action of the IAM architecture in the modern industrial / manufacturing plant.

Use Case: Water Plant Privileged User

Logging into critical plan machine through shared and privileged user ID.

Use Case: Accessing critical on-premise and cloud resources in a Water Treatment plant, through MFA and Privileged Access Management



- Registration – User and Devices
- Login using 1FA / 2FA with secure authentication factor

- Plant user logs into the resources using strong authentication
- The authentication mechanism is adaptive and risk-score based (dependent on type of resources accessed, access type, location of access etc.)
- The authentication is always the 2 factors (what you know and who you are)
- All the privileged sessions are through PAM system monitored and recorded
- All the authentications and authorizations are centrally managed and monitored

- Plant's resources are integrated through OIDC, SAML, Oauth 2.0, API-based technologies
- All the privileged sessions and logins are facilitated through PAM system
- All the sessions are centrally logged and monitored (and recorded wherever needed)
- All the critical and privileged sessions are Just In Time (JIT) and Just Enough Time based (JET)

Use Case: Water Plant Privileged User (continued)

Privileged Access Solution deals with the discovery, distribution and management of critical or high-risk accounts and accesses. Multi-Factor Authentication combined with the Privileged Access Solution provides increased security and compliance for OT-critical systems, such as ICS, SCADA, and others, in addition to corporate apps and cloud resources.

- Risk-based and adaptive authentication mechanisms, including MFA, step-up authentication, and risk-score based authentication
- Comprehensive monitoring and analysis of privileged access attempts and usage
- Central monitoring and management of all the involved entities (users, accounts, target systems, and access)
- JIT and JET to reduce permanent persistent access, ensuring that only the minimum level of access required for the task is provided for the appropriate time.

Use Case: Access Certification of Critical Accesses

Use Case: Access Recertification (including Privileged Access) for Employees and Third Party Resources in a Manufacturing Facility

Identity Governance Solution – Regular and Privileged

Actors –
Plant / Line manager

Accounts to certify –
Corporate Users, Factory/ Plant Employees, 3rd Party Resources, Service Accounts (Non-Human accounts)

- Initiate the access certification campaign
- The campaign request goes to individual actors like line managers, plant manager etc.

Industrial / Manufacturing Plant's critical apps

Applications/ Resources –
Individual/user workstations, internal applications (Payroll, HR, etc)

Critical Infrastructure –
Industrial Control Systems, SCADA Systems, Mainframes and Other High-Risk Systems

Cloud Applications and Services –
Including remote access for required infrastructure

- Certification campaign for the users who has access to all critical apps
- Certification actor would review the accesses of each applications
- The frequency of each type of apps differ as per the criticality
  - Corporate resources – Quarterly
  - Plant specific critical infrastructures – Bi-weekly / Monthly
  - Cloud Apps and services – Quarterly

Actors –
Plant / Line manager

- Certifying actors reviews the list of accesses across the resources
- Performs the action – Approve / Deny
- All the approved list of accesses stays and continue
- All the denied accesses undergo the suspension

Use Case: Access Certification of Critical Accesses (continued)

The Identity Governance Solution would include the recertification of both regular as well as privileged accounts and access. This includes accounts and access in the critical applications of the plant such as SCADA and other control systems, as well as corporate and cloud applications.

The certifying actors, who are the plant/line managers, supervisors, and system owners as per the case study are responsible for certifying the account access, and providing retain or remove (Approve/ Deny) decisions for the same. Any account and/or access that is denied by the certifying Actor is removed per the already established Access Removal/Modification procedure.

Key benefits of this campaign include:

- Retention of only the relevant and required accounts and access
- Identification of high-risk accounts such as those that are Dormant, Inactive, or Orphan Accounts
- Review of all the high-risk and critical Systems/ Applications including all accounts that have access to the same
- Improved governance and compliance.

Conclusion

Considering the criticality of OT, IoT and their security, along with the challenges around these aspects in any Industrial setup, the IAM principles in OT security is one of the key tenets to consider. With appropriate strategy, process and technology, the risks, the disruptions and the breaches arising due to shared credentials, privileged accounts breach and the data leaks due to stale accesses can be addressed.
Along with IAM principles, proper training and awareness among industrial users are equally important and critical in protecting valuable OT and IoT infrastructure.

pwc

www.pwc.ie