EP3

Raise Your Security Level of User Access Control

- Why your user access control needs enhancement
- IEC62443 SL2 – ‘unique’ and ‘unified’
- What is role-based access control and how
- Challenges and solutions

User access control

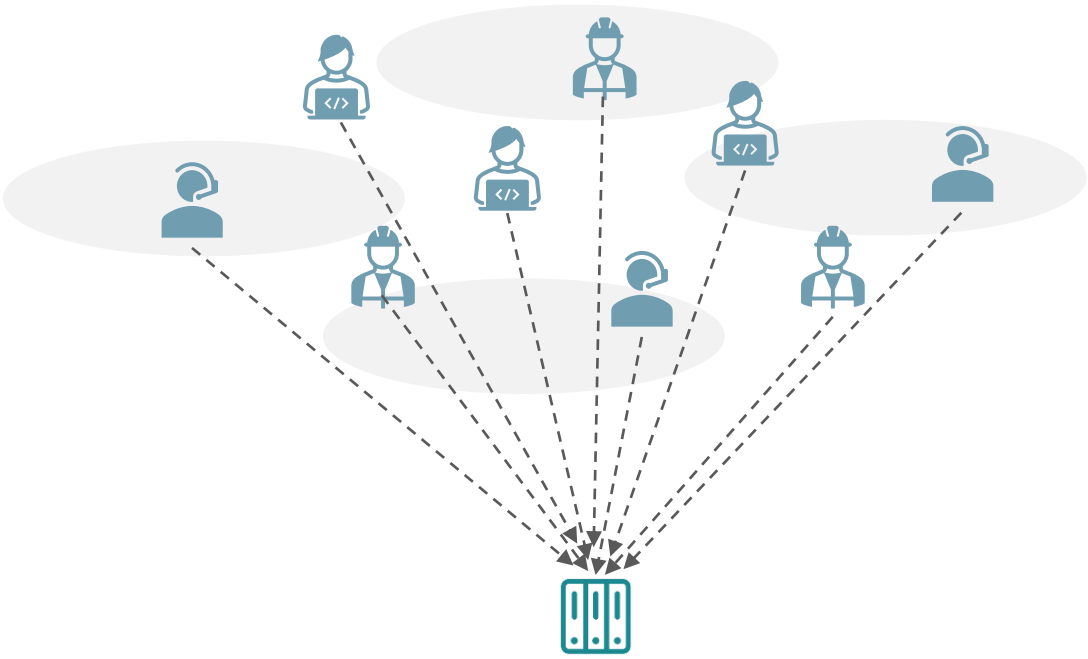
Authentication & Authorization

PHOENIX CONTACT
INSPIRING INNOVATIONS

User access control

Why Your UAC Needs Enhancement

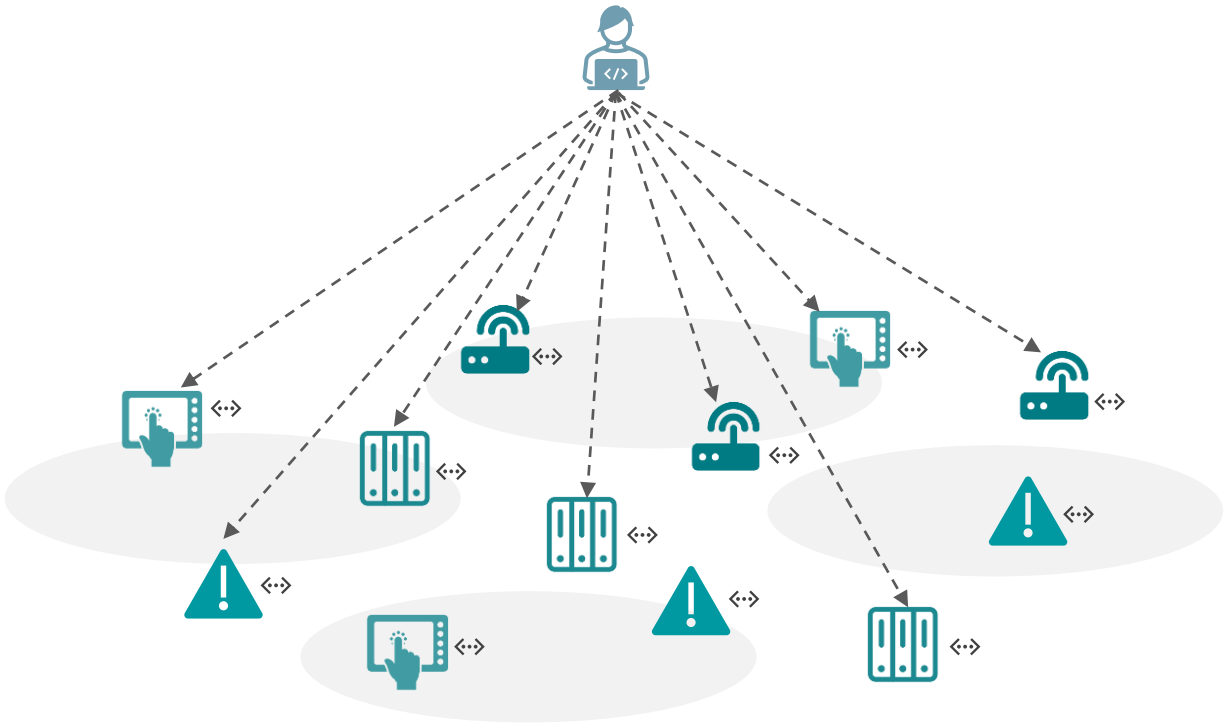
- Username and password are shard among the users (not unique)
  - Not secret
  - Not accountable
  - Not distinguishable (users and permissions)
  - Not revokable (former employees, etc)
  - …



User access control

Why Your UAC Needs Enhancement

- Username and password are stored in each component (not unified)
  - Either too many, or the same
  - Hard to manage (add/delete/edit/lock)
  - Not scalable
  - …



OT security standard

IEC62443

General	1-1 Technology, concepts, and models	1-2 Master glossary of terms and abbreviations	1-3 System security compliance metrics	1-4 System security lifecycle and use case	1-5 Rules for IEC62443 profiles	1-6 Application of the 62443 standards to industrial IoT
Policies & Procedures	2-1 Requirements for an IACS security management system	2-2 Security protection rating	2-3 Patch management in the IACS environment	2-4 Requirements for IACS solution providers	2-5 Implementation guidance for IACS asset owners	
System	3-1 Security technologies for IACS	3-2 Security risk assessment for system design	3-3 System security requirements and security levels			
Component	4-1 Secure product development lifecycle	4-2 Technical security requirements for IACS components				

OT security standard

IEC62443

IEC62443-2-4 Security Program

SP.01	Solution Staffing
SP.02	Assurance
SP.03	Architecture
SP.04	Wireless
SP.05	SIS
SP.06	Configuration Management
SP.07	Remote Access
SP.08	Event Management
SP.09	Account Management
SP.10	Malware Protection
SP.11	Patch Management
SP.12	Backup/Restore

IEC62443-3-3 and IEC62443-4-2 Fundamental Requirements

FR1.	Identification And Authentication Control
FR2.	Use Control
FR3.	System Integrity
FR4.	Data Confidentiality
FR5.	Restricted Data Flow
FR6.	Timely Response To Events
FR7.	Resource Availability

IEC 62443-2-4

SP.09 – Account Management

		Requirement Description
SP.09.01	**BR**	The service provider shall have a process that can be performed for the asset owner to support the following: 1) the administration of a single, integrated data base, which may be distributed or redundant, for defining and managing user and service accounts, 2) the creation of accounts for authorized users only, 3) the configuration for decentralized access to this data base for the management of accounts, 4) administration of decentralized enforcement of the account settings (e.g. passwords, operating system privileges, and access control lists) defined in this data base.
SP.09.02	**BR**	The service provider shall have a process that can be performed for the asset owner to create and maintain unique accounts for users.

IEC 62443-3-3

FR 1 – Identification & Authentication Control

		SL 1	SL 2	SL 3	SL 4
SR 1.1	Human user identification and authentication	✓	✓	✓	✓
RE 1	Unique identification and authentication		✓	✓	✓
SR 1.3	Account management	✓	✓	✓	✓
RE 1	Unified account management			✓	✓
SR 1.4	Identifier management	✓	✓	✓	✓
SR 1.5	Authenticator management	✓	✓	✓	✓

IEC 62443-3-3

FR 2 – Use Control

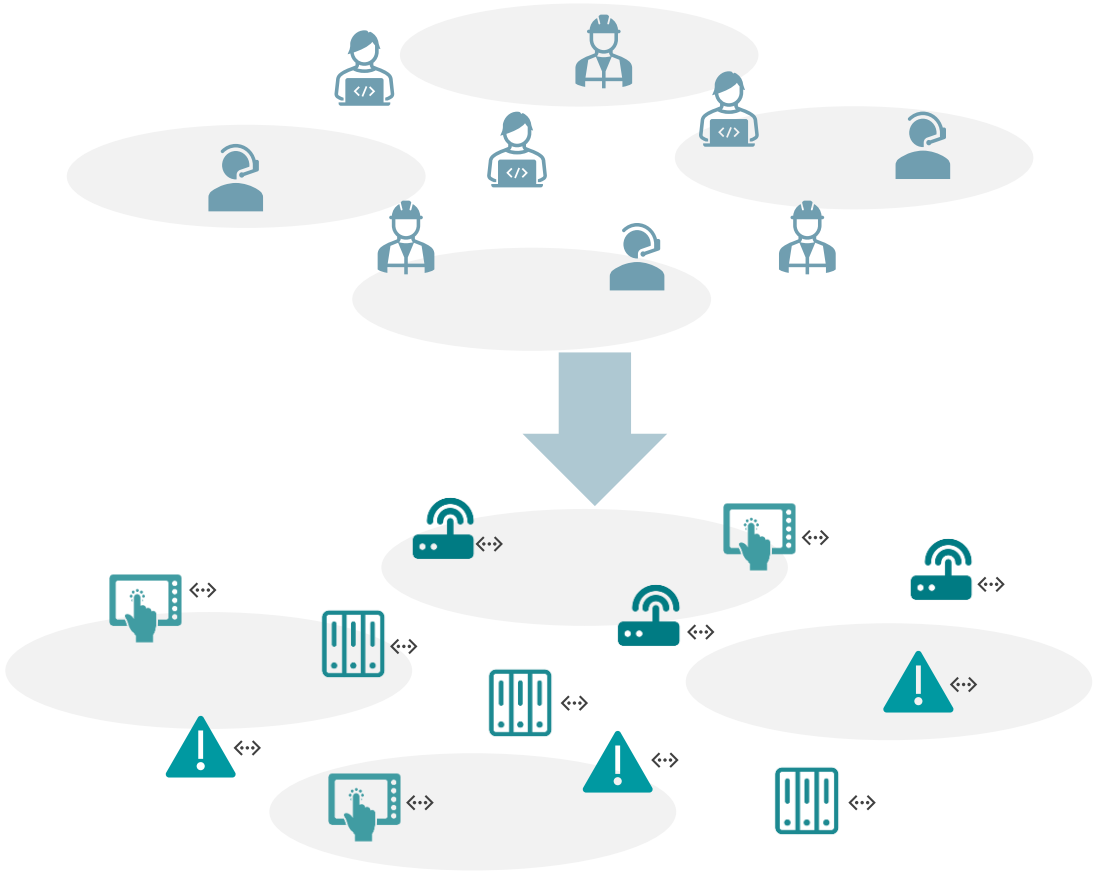
		SL 1	SL 2	SL 3	SL 4
SR 2.1	Authorization enforcement	✓	✓	✓	✓
RE 1	Authorization enforcement for all users		✓	✓	✓
RE 2	Permission mapping to roles		✓	✓	✓

IEC 62443

Raise Security Level of Your UAC

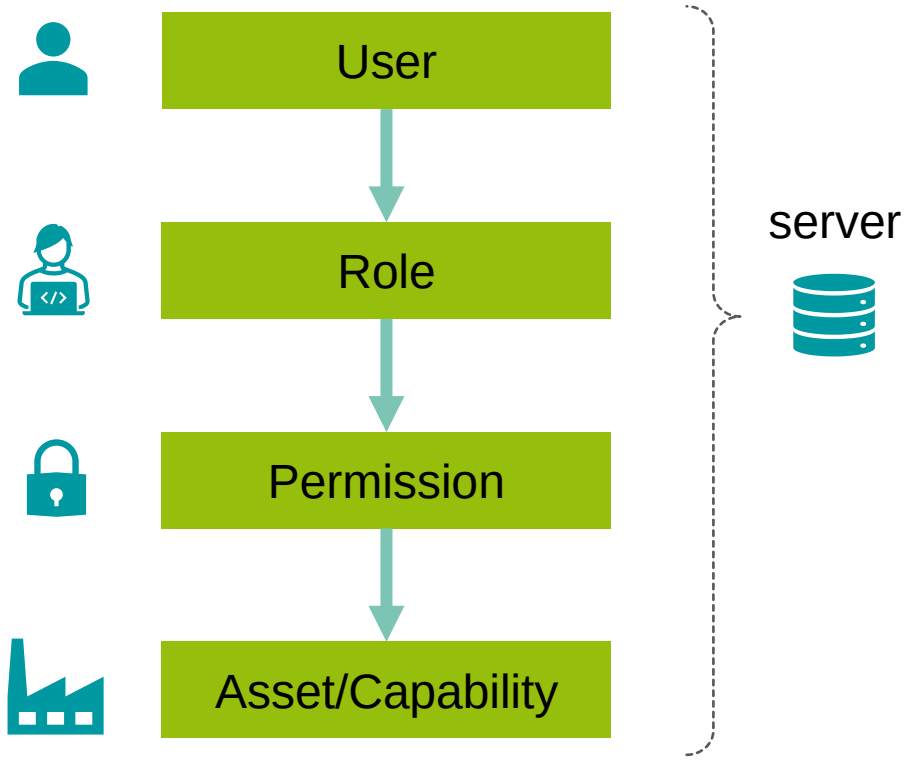
- Authentication
  - Unique identification and authentication
  - Unified account management

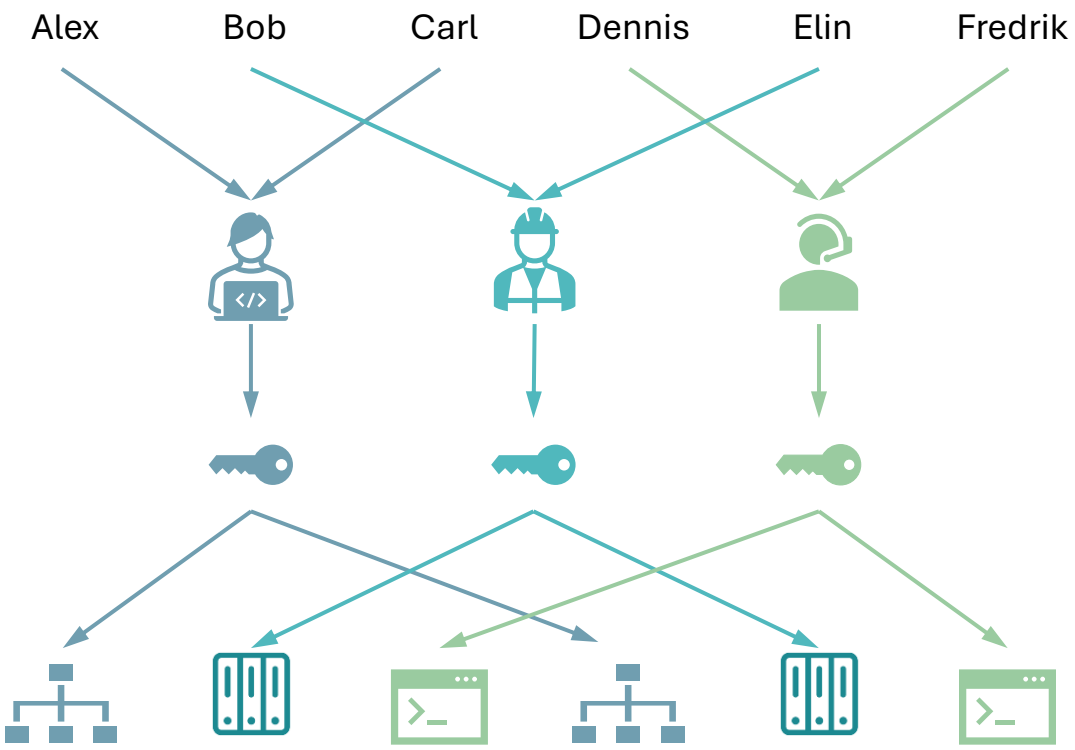
- Authorization
  - Enforcement for all users
  - Permission mapping to roles



Role-based Access Control

RBAC Explained



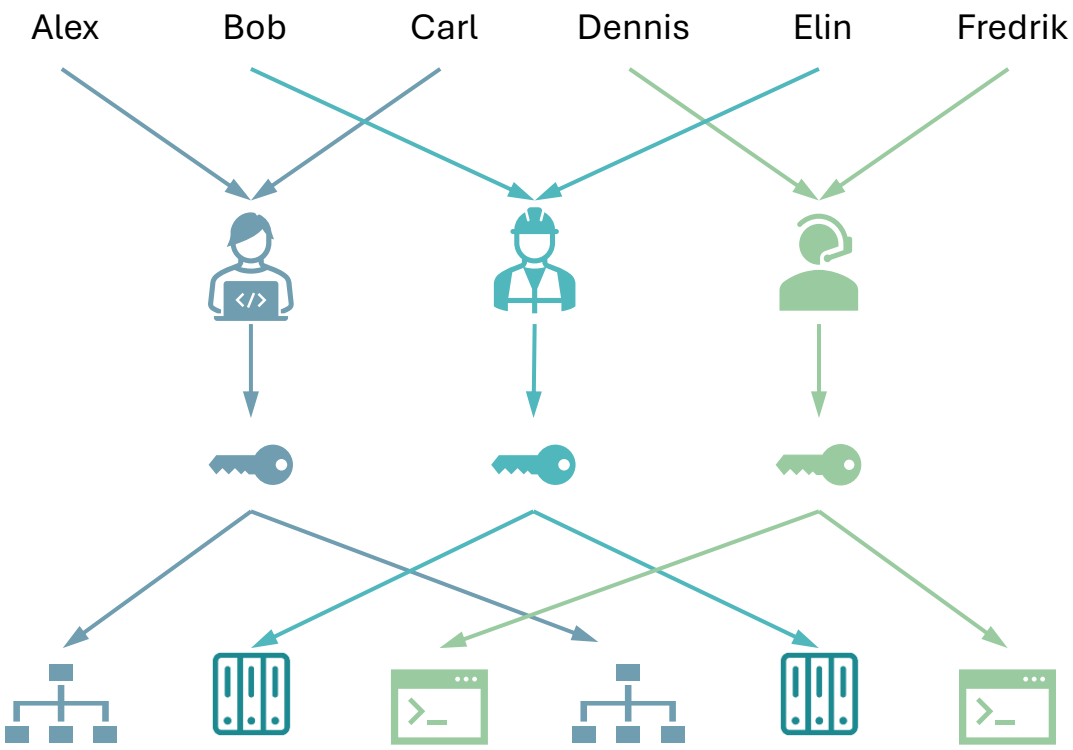


PHOENIX CONTACT
INSPIRING INNOVATIONS

Role-based Access Control

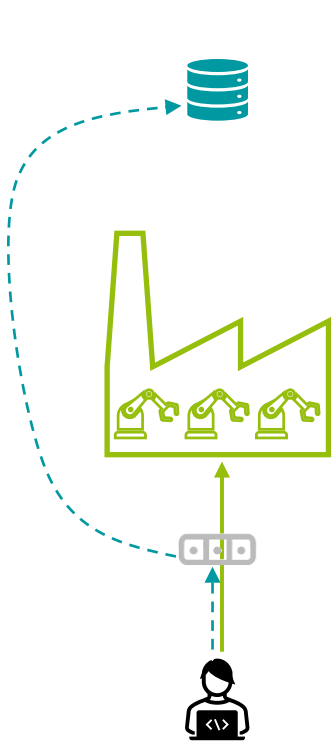
Benefits

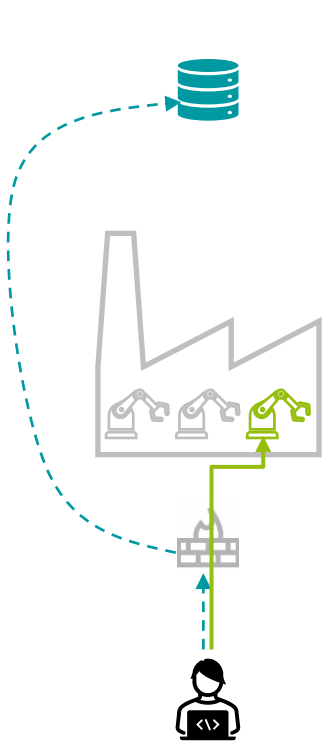
- Reduce complexity. Focus on roles-permissions, instead of individuals-assets/capability
- Add a user to a role; remove a user from a role; lock a user; change a user from one role to another; play multiple roles
- Simple, scalable, and secure

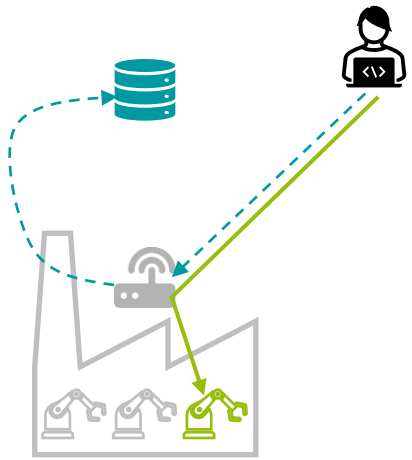


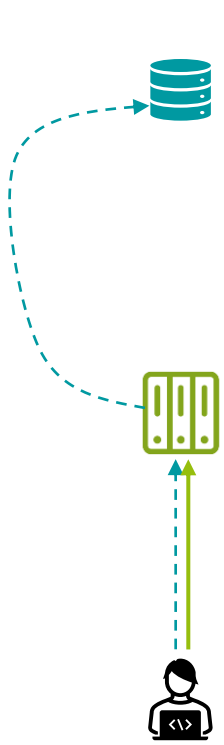
Common Scenarios

System	Sub-system	Remote Access	Component





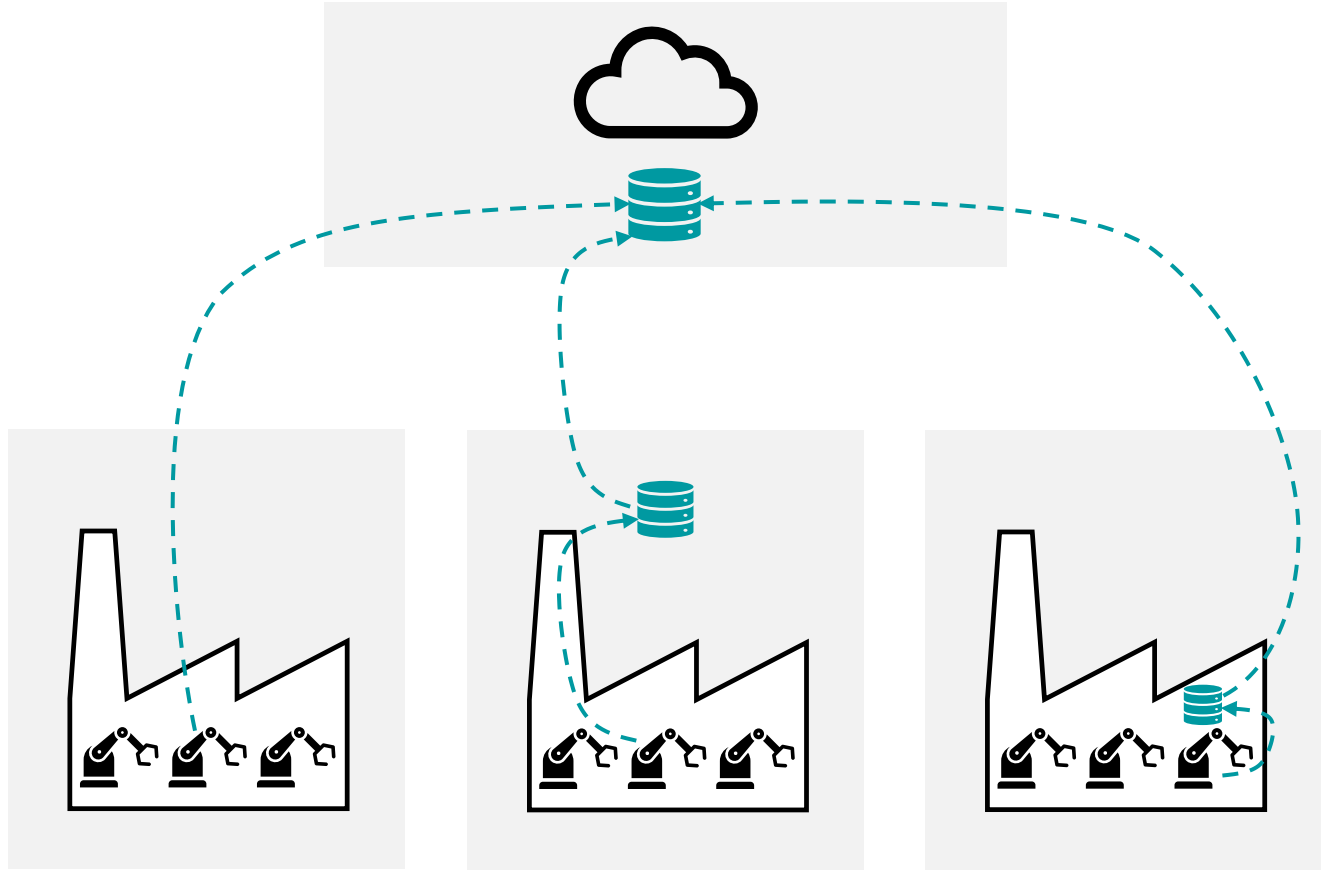




Role-based Access Control

Challenges

- Not all industrial components support RBAC
- Options and integration: RADIUS, LDAP, TACACS+, …
- Roles & Permissions
  - Asset owner
  - Service provider
  - Machine vendor
- Architecture
  - Centralized, distributed, redundant, proxy



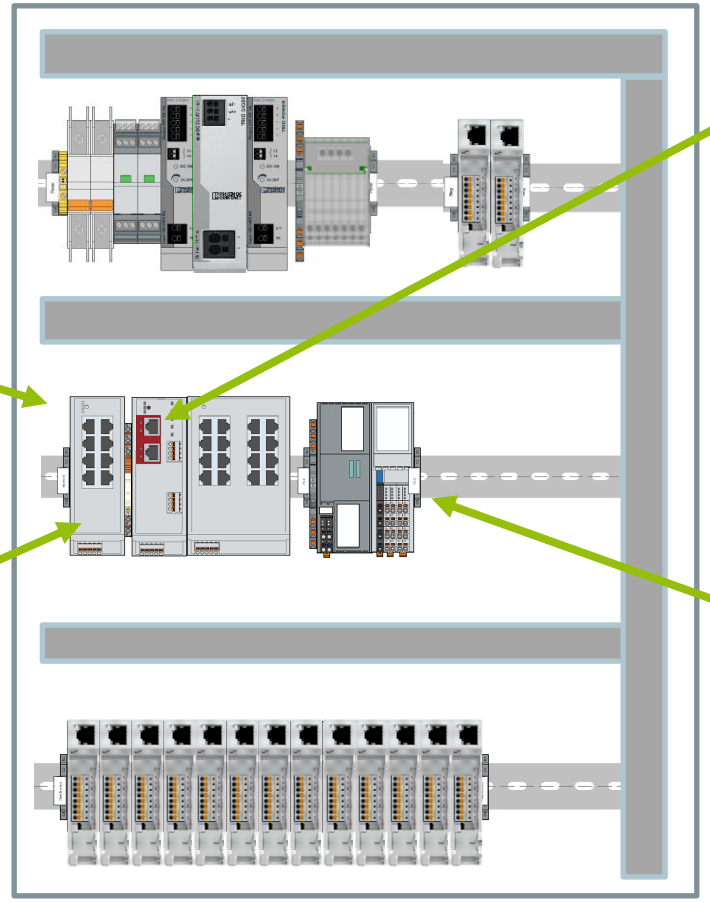
Role-based Access Control

Phoenix Contact Solution

Solution of networking, automation, safety with cybersecurity

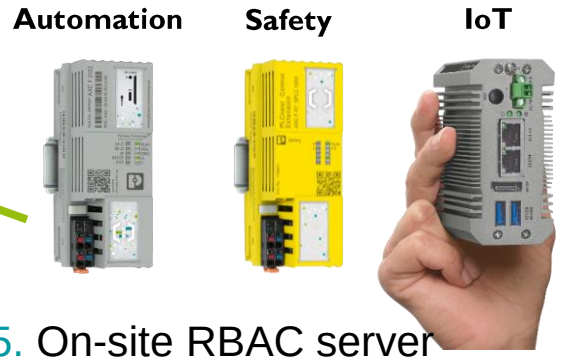
1. Role-based user access control to the components

2. Role-based user access control to the system (network)



3. Role-based user access control to sub-system

4. Role-based user access control for remote access

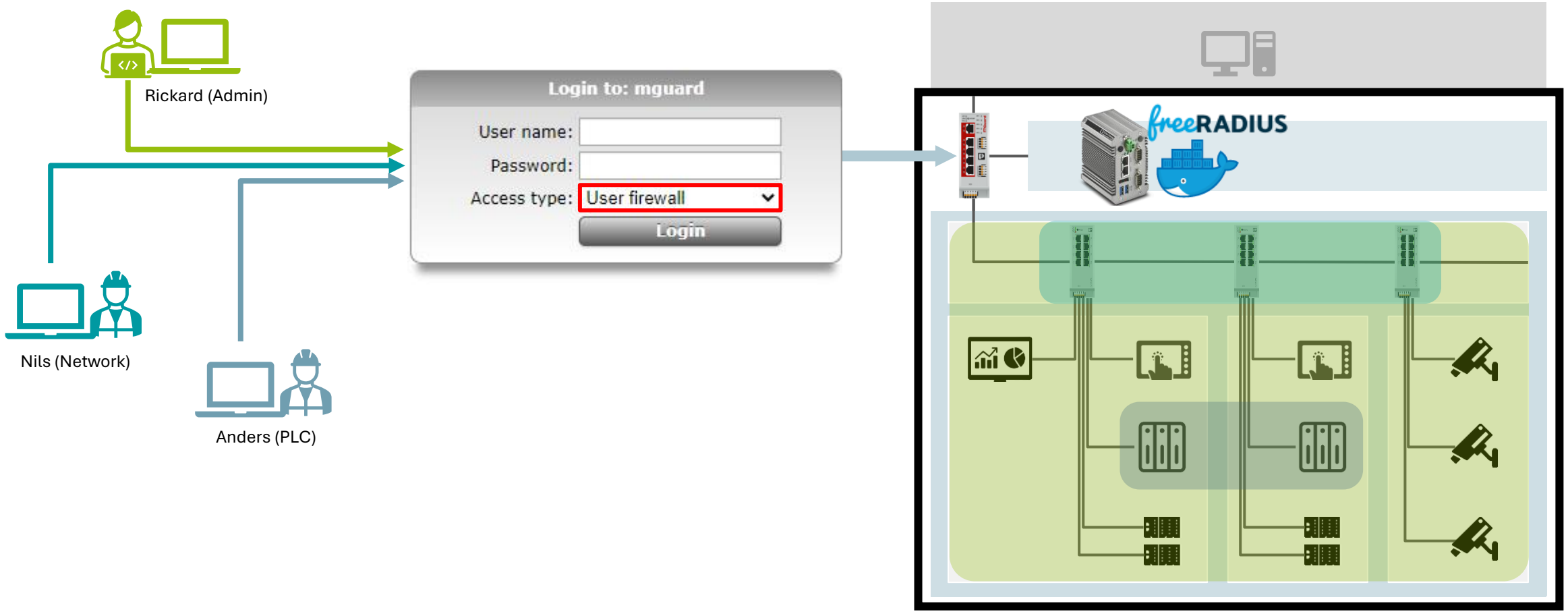


5. On-site RBAC server

PHOENIX CONTACT
INSPIRING INNOVATIONS

Role-based Access Control

Live Demo



PHOENIX CONTACT
INSPIRING INNOVATIONS

Be Aware

- Access control shall not prevent the operation of essential functions.

  Functions that are required to maintain health, safety, the environment (HSE) and availability for the equipment under control

  Loss of protection, loss of control, loss of view, etc

Raise your security level of user access control

Summary

- User access control is a fundamental requirement according to IEC62443-4-2, IEC62443-3-3, IEC62443-2-4
- Avoid sharing username/password or storing username/password on each component
- Unique identification and authentication, unified account management
- About Role-Based User Access control: benefits, considerations, architecture …

Thank you

PHOENIX CONTACT
INSPIRING INNOVATIONS