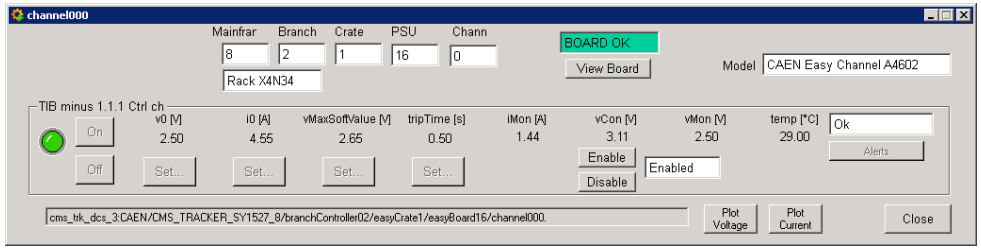
Centralized configuration of Role-Based authentication in JCOP Framework

ICALEPCS 2015, Melbourne Australia
5th Control System Cyber-Security Workshop

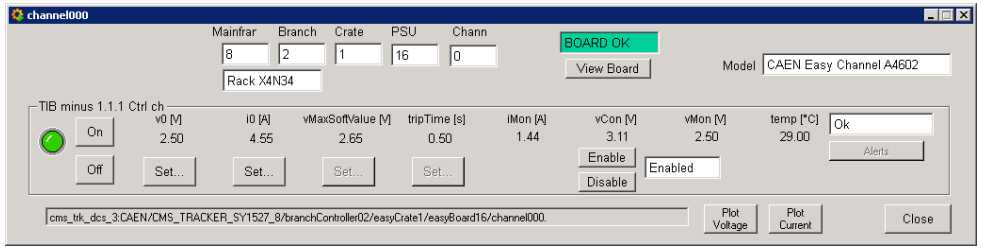
Lorenzo Masetti
Piotr Golonka

Access Control for Control System HMIs

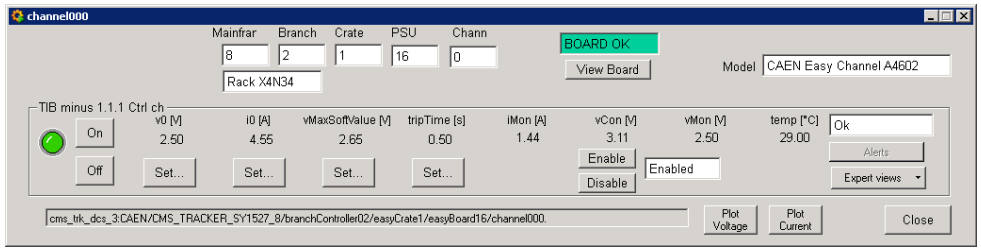
- Ensures the protection from non-malicious actions at the UI level
  - Other levels (e.g. ctrl scripts) are not protected by this feature



Operator:
Can not switch on from this panel



Detector Expert:
Can switch on and change some settings



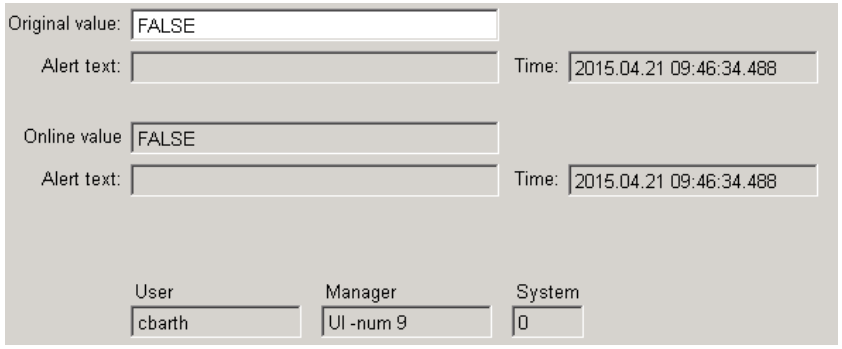
DCS Expert:
Can switch on and change all settings

Requirements

- CERN applications require rather frequent changes to user permission and a flexible authorization model
- Access Control Configuration needs to be replicated in many distributed systems
- Proper user/group (role) management tools are required → Role-Based Access Control (RBAC) model
- **Central persistent configuration of user rights and privileges**

Integration with WinCC OA Access Control

- WinCC OA provides a basic implementation of access control
  - Good for mid-scale industrial applications, not for CERN
- JCOP Access Control built on top of native WinCC OA mechanism
  - Can profit for activity logging and system-integrity protection from WinCC OA

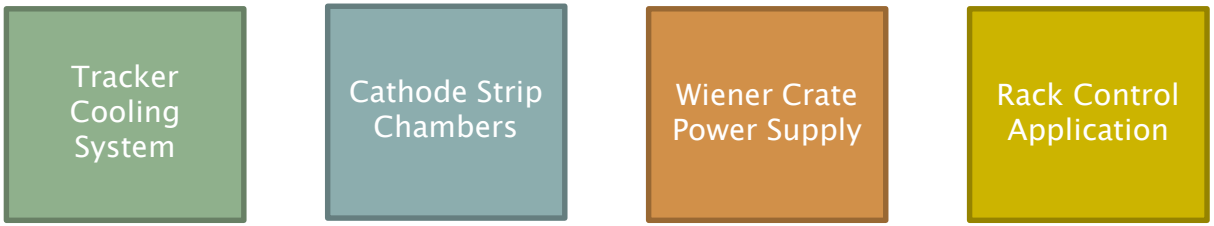


Access Control Configuration is complex

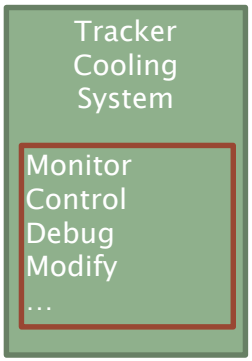
- Additional tools are needed to assist with the setup and storage of the configuration data
- WinCC OA is not the best environment to develop and deploy these tools
  - We need to reuse existing user database and existing authorization
  - Better to use existing and well-tested interfaces that users are familiar with
- Authorization, authentication and user management can be completely delegated to existing identity management tools that are shared with other applications outside the control system.
  - This was initially developed for users and groups
  - Now the complete configuration data including domain and privileges can be imported from external sources

Domains and Privileges

- Large Number of subjects need to be protected by access control
  - Large number of permissions to be defined in the system
- Domain is an entity (physical, conceptual or organizational) that needs to be protected:



- Within a domain we define a set of privileges corresponding to the specific domain

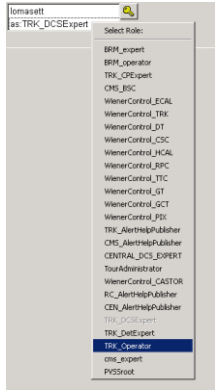


Access Right → Domain:Privilege

e.g. TrackerCooling:Control

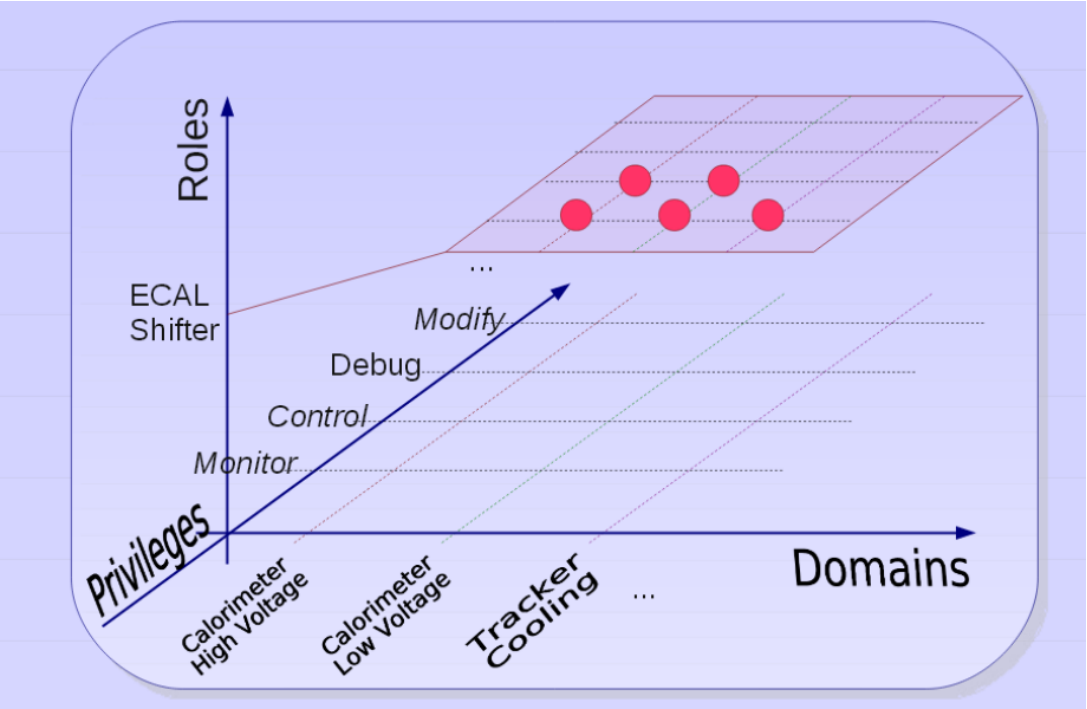
Role-Based Model

- Permissions (access rights) are granted to a *role*
- Users are assigned certain roles and gain the access right of their role(s)
- Roles correspond to Groups in WinCC OA terminology
  - Users belong to groups and gain the permissions defined for the groups they belong to
- The model has to be extended for Hierarchical RBAC
  - Role A that contains roles B and C inherits the permissions from B and C (plus the ones explicitly granted).
- Dynamic Separation of Duties
  - Strict role checking mode
  - Users need to explicitly select the role that they want to take to get their rights
  - Disabled by default but used in CMS



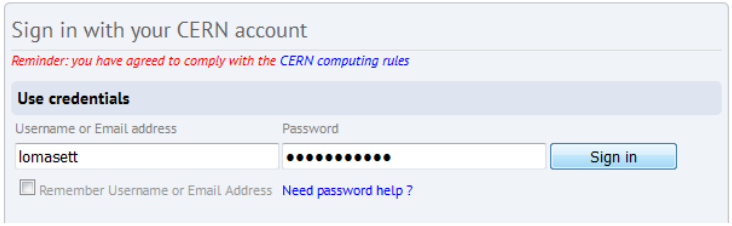
Advantages of this approach

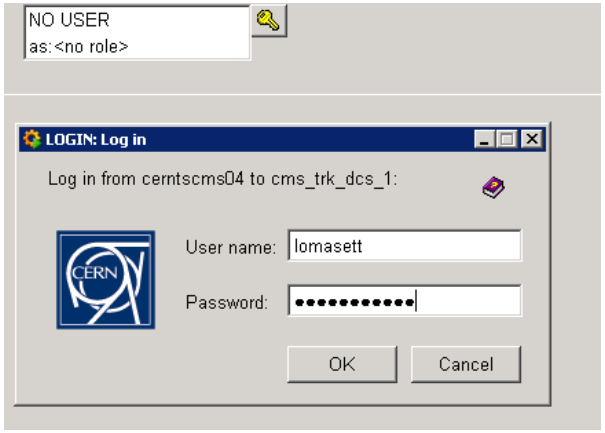
- Promote generic approach in defining access rights rather than fine-grained device-oriented approach
- Flexibility in configuration: it is easy to grant new rights to a role



Authentication

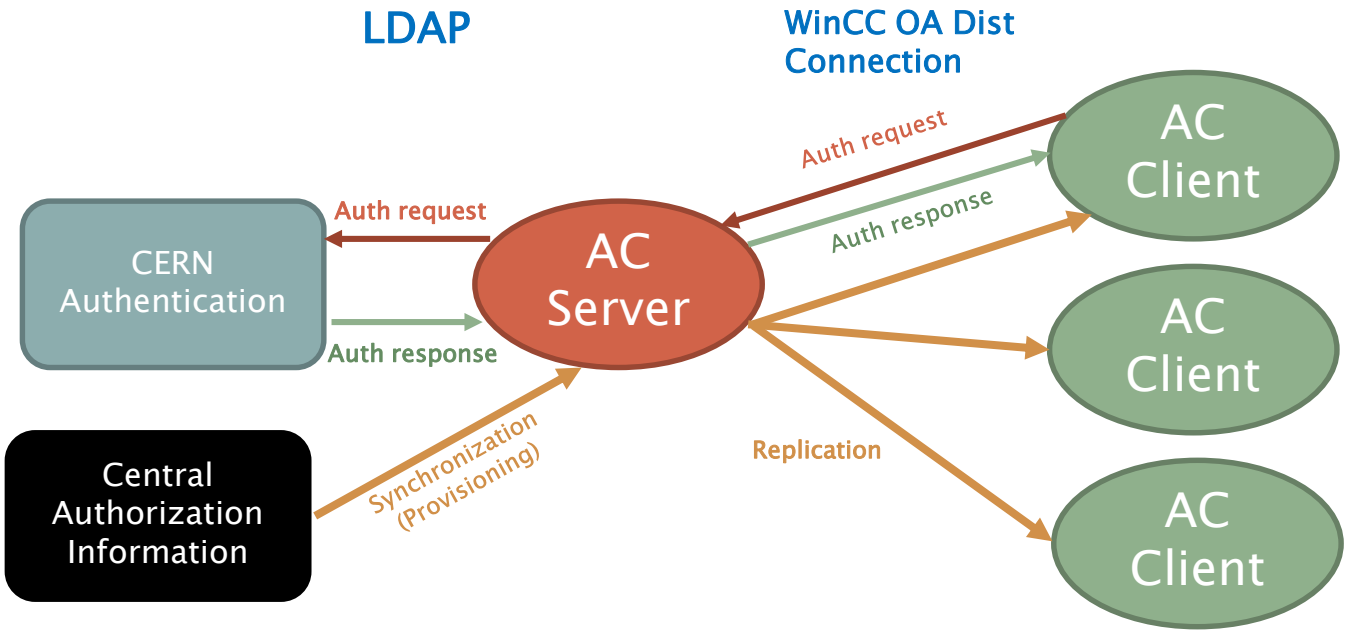
- Requirement: log in using the same credential used in CERN central services
- LDAP protocol used to authenticate against CERN Active Directory server
- Authentication with CERN cards is possible, using RFID card readers





Deployment to Large Distributed System Network

- The Access Control Server
  - Runs as a WinCC OA script in a central project connected to all others
  - Acts as a proxy server for authentication
    - It uses LDAP and returns the result to the clients
- Propagates all the changes in the users / groups / domain configuration or privileges mapping

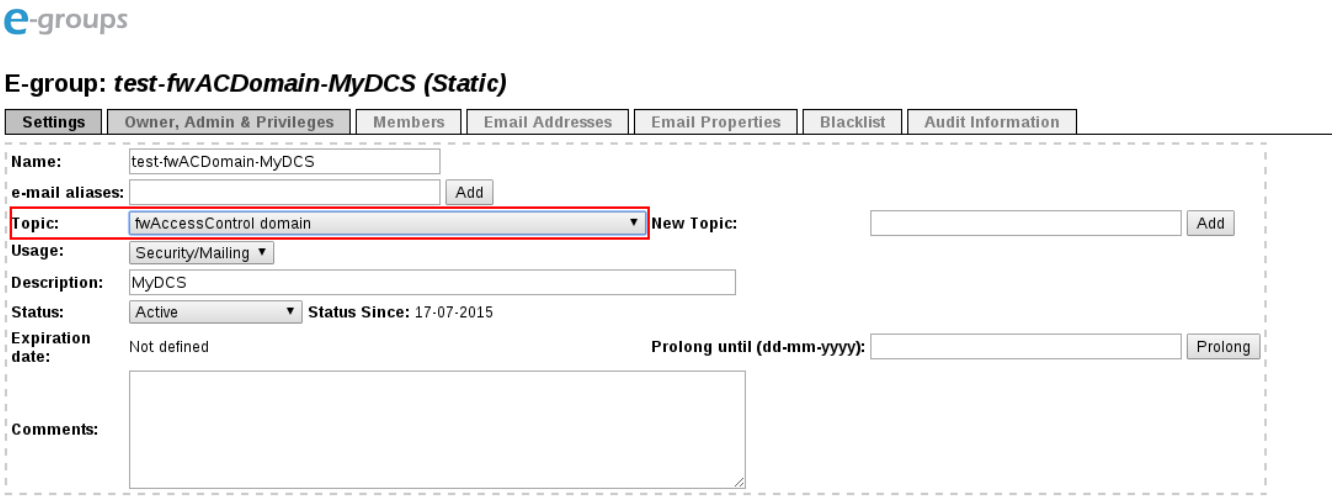


Full configuration from LDAP

- Synchronization process retrieves from LDAP
  - User names and user information (email, GSM, etc.)
  - Groups (Roles)
  - Group membership
  - Domain
  - Privileges
  - Mapping of Privileges to Roles
- This allows rebuilding the complete WinCC OA application from scratch and have its access control configured automatically
- Administration of rights delegated to external tools
- Possibility of automatic definition of group membership (e.g. synchronized with the shifts)
- Synchronization process typically scheduled to run periodically

E-group based synchronization

- Full configuration of WinCC OA based on a hierarchy of nested groups
- **E-group:** main interface to manage groups at CERN published via LDAP.
- E-groups can contain other e-groups.
- The e-groups are used for different purposes, differentiating by **topic**:
  - **fwAccessControl_configuration**: root e-group containing the full configuration information
  - **fwAccessControl_domain:** the e-group defines a domain
  - **fwAccessControl_privilege:** the e-group defines a privilege
  - **fwAccessControl_role**: the e-group defines an access control role
  - **No Topic**: a normal group of users



Full Configuration from LDAP