# Role Based Access Control for LHC devices

Suzanne Gysin - FNAL on behalf of the RBAC team

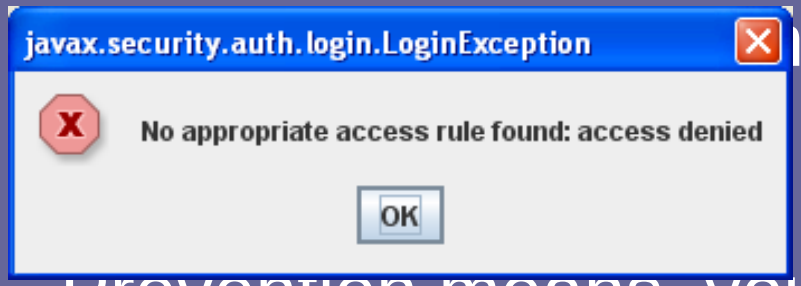
# Motivation: Machine Safety

- The energy stored in the LHC magnets and beam is enormous.
- The potential for crippling machine damage is a serious concern
- CERN has developed a multi-pronged approach for machine safety
  - Hardware Protection
    - LHC Beam Interlock System
    - Powering Interlock System
  - Software Interlock system
  - Role Based Access
    - Prevents unauthorized access to settings
    - Provides logging to detect errant settings

# Role Based Access Control

RBAC is software to prevent:

1. A well meaning person from doin
   thing at the wrong time.

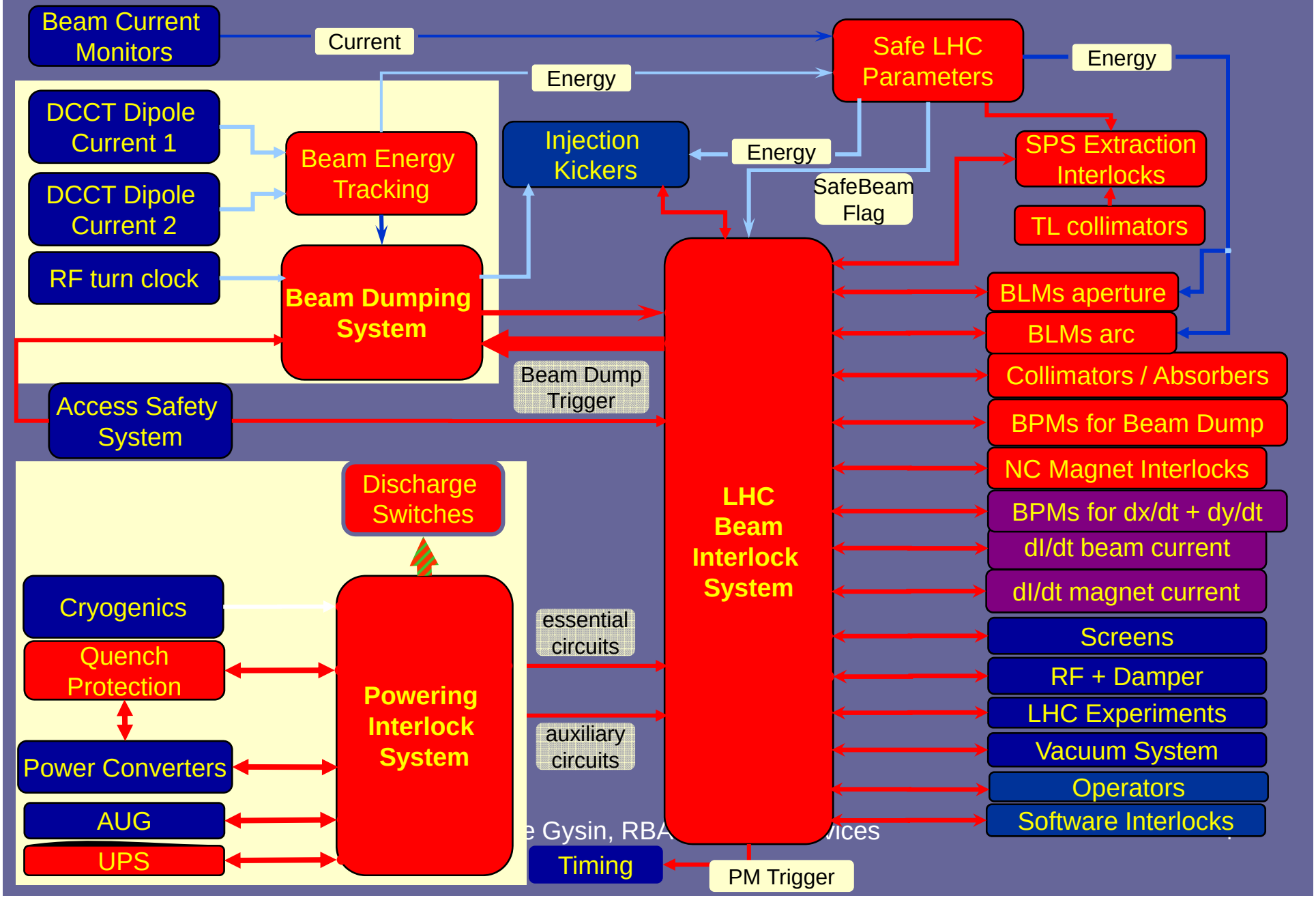




from doing anything,

Prevention means, you will see an error dialog.
They are annoying but, you'll press OK and the world moves on without any consequences.

On the other hand, you could trigger the Machine Protection System …

# Machine Protection Systems and (HW) Interfaces



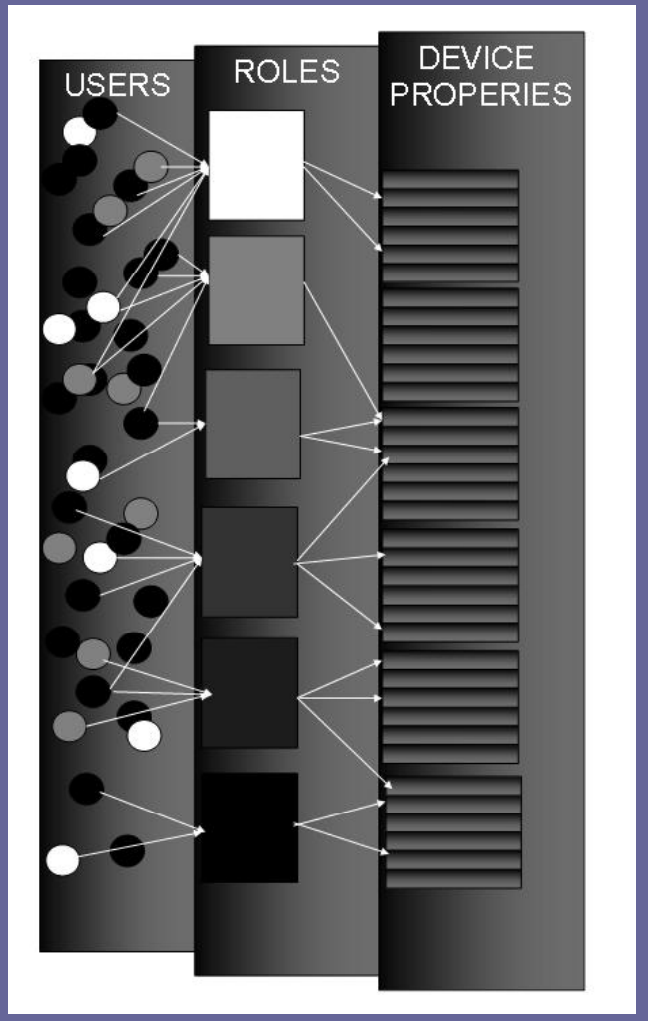
# Motivation Summary

1. Machine Safety
   - Energy stored in the LHC is enormous
   - RBAC protects from crippling machine damage
   - RBAC prevents invoking machine protection system
2. Machine Performance
   - Don’t mess with a fine tuned system
   - Access denied during certain machine states
3. Settings logger
   - Hardware and Software commissioning
   - Sequencer typo debugging

# How does it work?

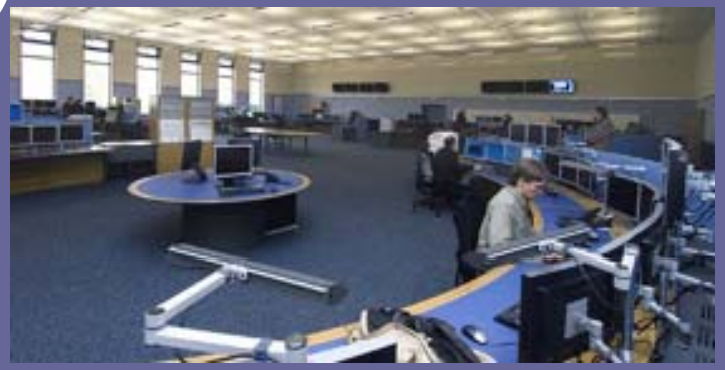
- RBAC works by giving people roles and assigning the roles permissions to make settings.

- Terminology
- Defining roles
- Defining permissions



# Role Based Access Control (RBAC)

- What is a ROLE?
  - A role is a job function within an organization. Examples: LHC Operator, SPS Operator, RF Expert, BPM Developer …
  - Roles are defined by the instrument designers in a security policy.
  - A user may have several roles



# Current List of Roles (26)

**Access-Rule-Maker**
BI-Expert
BT-Developer
BT-Equipment-Expert
BT-Expert
BT-Piquet
Critical-Property-Admin
FMCM-Expert
LHC-EIC
LHC-Operator
LabView-Developer
MCS-BPGCNGS
MCS-LHCCollCalibration
MCS-Test
MCS-Test2
OP-Daemon
PO-Calibrator
PO-Configurer
PO-FGC-Expert
PO-FGC-User
PO-GW-Expert
PO-Superuser
RBA-Developer
RF-LHC-PowerExpert
**Role-Maker**
Temporary

# Users Receive Roles

- Each role has one or more role administrators.
- The role admin is responsible for adding and removing users from a role.
- Role-Maker is a role that has the permission to make other roles.
- Users are identified by the NICE user name.

Partial list of users and their roles (52)

| | |
|---|---|
| BI-Expert | BDISOFT |
| BI-Expert | JJGRAS |
| BI-Expert | LJENSEN |
| BI-Expert | MPERYT |
| BI-Expert | NPELOV |
| BT-Developer | CARLIER |
| BT-Developer | NMAGNIN |
| BT-Developer | TMUELLER |
| BT-Developer | VERHAGEN |
| BT-Expert | CARLIER |
| BT-Expert | TMUELLER |
| BT-Expert | VERHAGEN |
| BT-Piquet | AANTOINE |
| BT-Piquet | FCASTRO |
| BT-Piquet | NVOUMARD |
| BT-Piquet | OLIVIERI |

# Controlling Access

- What is being accessed?
  - CMW device properties (power converters, collimators, kickers, etc.)
- What type of access?
  - get: the value of a property once
  - monitor: the property continuously
  - set: the value of a property
- Device Properties are protected with Access Rules.

# Access Rules

**Access rules**

row(s) 1 - 15 of more than 500 Next

| ID | CLASSNAME | PROPERTY | DEVICENAME | DEVICEGROUP | ROLE | APPLICATION | LOCATION | OP_MODE | ACCESS_MODE |
|---|---|---|---|---|---|---|---|---|---|
| 1 | LhcMKIkick | Setting | - | - | LHC-Operator | - | CCC-LHC | - | set |
| 2 | LhcMKIkick | Setting | MKI.UA23.KICK | - | BT-Equipment-Expert | - | BT-UA23 | - | set |

- Specify the property, role, location, access type
- If there is no access rule for a property, it is not protected (default)
- One access rule protects a property against all other roles
- Each device class has a rule administrator. It is his responsibility to add and remove access rules for the class.
- There is an Access-Rule-Maker (role) who has permission to create new rule administrators.
- Currently there are over 10,000 access rules

# A1 and A2

- A1 = Authentication : NICE, X.509
- A2 = Authorization: Role to make the setting

# Token and Access Maps

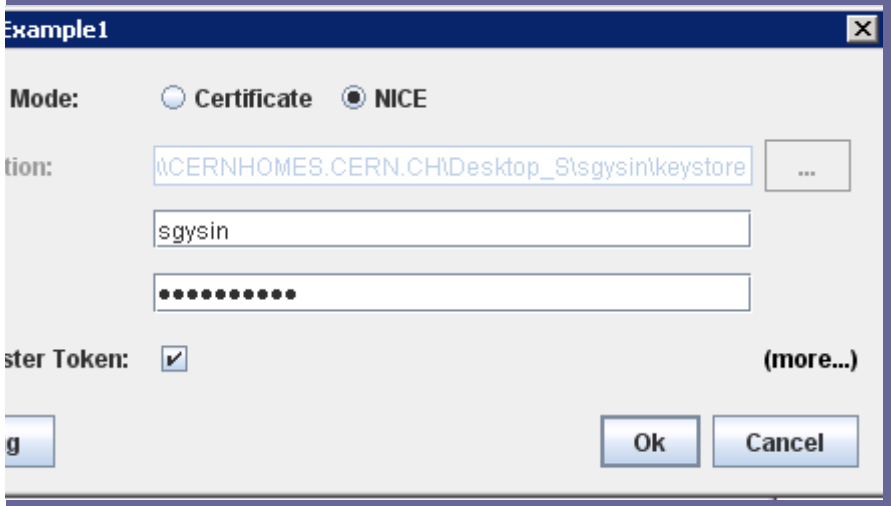
- RBAC Token (A1)
  - Proof of authentication
  - Holds information for authorization: roles, location, application
  - Digital signature
- Access map (A2)
  - Access maps are text files on the front ends
  - They are built from the database table holding all access rules
  - Contain the subset of access rules for a specific server on the front end
  - Read into memory for fast permission checks
  - Verify digital signature with RBAC public key
    - token came from the RBAC server
    - Token contents have not been altered
  - Check the expiration time

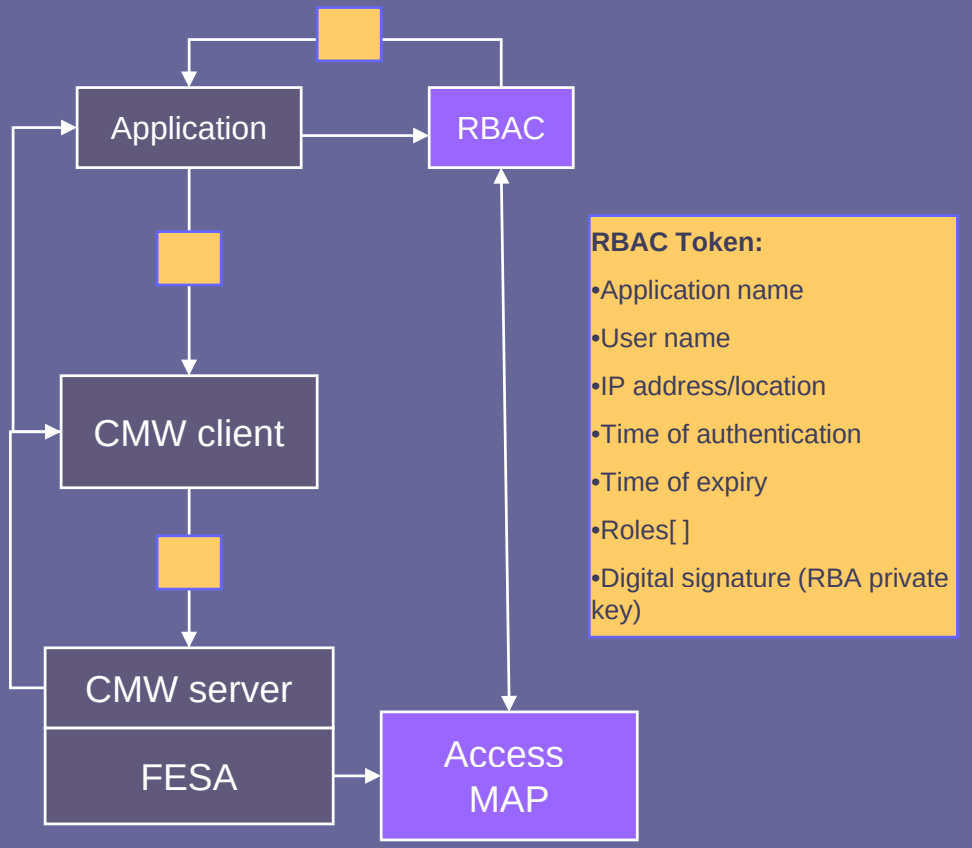
# High Level Design

A1:

- User requests to be authenticated.
- RBAC authenticates user via NICE user name and password
- RBA returns token to Application

A2:



# Performance Test Results

Tests were executed on a 400 MHz. Linux Power PC.

1. Size of access map

   The difference in performance of the access map search between 20 rules and 2000 rules is 0.02 ms.

2. Logging requests

   The overhead of logging each request into a log file is 0.003 ms.

3. Token verification

   The key size is the most contributing factor. A DSA 1024 bit key takes 5 ms. to verify. A RSA 512 bit key takes 0.15 ms. an order of magnitude different.

   Verifying the token, i.e. the signature and expiration time, of the RBAC token takes 2 ms.

# Many Special Features

- Authentication by Location: an access rule can limit the access on a location basis. Locations are set in the database on a host address basis.
- Authorization by application: an access rule can limit the access for applications.
- Role Picker: a user may pick a specific role if multiple roles are available
- Generate and manage public and private keys for Critical Settings
- Token Log (currently over 3000), keep track of who receives tokens.
- Load balancing (2 RBAC servers)
- Web interface for browsing and editing roles and rules
- Access map builder by class, server, and front end
- Application timeout: authentication timeout for an application.
- Role timeout: authentication timeout for a specific role (temporary role)
- Single Sign-on: once logged into one application, the others pick up the token.

# Participation in Requirements and Design

- **Requirements:**

- ***Prepared by:***
- **S. Gysin FNAL/ LAFS**
- **K. Kostro AB/CO**
- **G. Kruk AB/CO**
- **M. Lamont AB/OP**
- **S. Lueders IT/CO**
- **W. Sliwinski AB/CO**
- **P. Charrue AB/CO**

- ***Checked by:***
- **J. Wenninger AB/OP**
- **S. Page AB/PO**
- **E. Hatziangeli AB/CO**
- **V. Kain AB/OP**
- **K. Hanke AB/OP**
- **R. Schmidt AB/CO**
- **R. Steerenberg AB/OP**

- ***Approved by:***
- **P. Collier AB/OP**
- **H. Schmickler AB/CO**
- **R. Bailey AB/OP**
- **S. Myers AB**

- **Design:**

- ***Prepared by:***
- **P. Charrue AB/CO**
- **V. Baggiolini AB/CO**
- **W. Gajewski AB/CO**
- **S. Gysin FNAL/ LAFS**
- **V. Kain AB/OP**
- **K. Kostro AB/CO**
- **G. Kruk AB/CO**
- **R. Gorbanosov AB/CO**
- **S. Page AB/PO**
- **M. Peryt AB/CO**
- **A. Petrov FNAL/LAFS**
- **C. Schumann**
- **W. Sliwinski AB/CO**
- **N. Stapley AB/CO**

- **Design:**

- ***Checked by:***
- **E. Hatziangeli AB/CO**
- **K. Hanke AB/OP**
- **M. Lamont AB/OP**
- **S. Lueders IT/CO**
- **R. Schmidt AB/CO**
- **R. Steerenberg AB/OP**
- **J. Wenninger AB/OP**

- ***Approved by:***
- **P. Collier AB/OP**
- **H. Schmickler AB/CO**
- **R. Bailey AB/OP**
- **S. Myers AB**

# Documents and Meetings

- EDMS requirement document
- EDMS design document
- Vertical Slice Test Jan. 18th
- Formal review by CERN Feb. 16th
- Production release with load testing
- Weekly meetings
- Participate in CNIC
- Source code in CVS package: accsoft-security-rba
- Users Guide
- All information is on RBAC wiki:

: http://wikis.cern.ch/display/LAFS/Role-Based+Access+Control

# Usage and Status

- Current load:
  - 25 roles
  - 94 user/roles assignment
  - > 10,000 rules
  - > 140,000 token since May'07

- Andrey Petrov and I are supporting RBAC remotely.
- No direct network access is a severe handicap and cuts productivity by 40%.
- AB/CO plans to initiate a security policy
- Expect usage to grow fast in the next 6 months.

# At ICALEPCS'07

- Poster sessions
  - Tuesday TPPA04 (overview what you just saw here)
  - Tuesday TPPA12 (authentication: Andrey Petrov )
  - Wednesday WPPB08 (authorization: Wojciech Gajewski)