# Role Based Access Control System in the ATLAS Experiment

## Introduction
The complexity of the ATLAS [1] experiment motivated the deployment of an integrated Access Control System in order to guarantee safe and optimal access for a large number of users to the various software and hardware resources. Such an integrated system was foreseen since the design of the infrastructure and is now central to the operations mode. In order to cope with the ever growing needs of restricting access to all resources used within the experiment, the Roles Based Access Control (RBAC) previously developed [2] has been extended and improved.

The access control system regulates the operations that can be executed on data and resources to be protected. Its goal is to control operations executed by subjects in order to prevent actions that could damage or steal data and resources.

## System design
The Role Based Access Control (RBAC) system used in the ATLAS experiment takes the access decision for an individual user based on the roles the user possesses. The role determines which resources can be accessed and permission is being granted only if the user has the required role enabled. The core components of the RBAC system are:

- **users:** computing accounts associated with human beings or automated agents;
- **roles:** job functions or job titles which define an authority level;
- **resources:** object which supports a set of possible actions;
- **permissions:** approvals to perform an action.

## Implementation
Inside ATLAS a simplified RBAC model was implemented. Roles have been designed to have both an organizational (ATLAS subsystem or project) and a functional component (reflecting the expertise levels within a subsystem).

Permissions are attached to roles located at the bottom of a role hierarchy (like a task based organization). The roles assigned directly to users are at the top of the hierarchy. The two classes of roles are connected via intermediary roles, allowing for a fine grained and flexible permission allocation.

Global base roles are used as building blocks. These are not directly assignable to users and generic access policies are defined for them. More specific roles are assignable to users, inherit other roles including base roles not assignable to users and can get additional permissions.

Roles are defined in LDAP (Lightweight Directory Access Protocol) as NIS (Network Information Service) netgroups. This approach offers several advantages, including the ability to model a hierarchical structure and integration at the operating system / application level [3].

The Access Manager [4] is the component that implements the access management for Trigger and Data Acquisition (TDAQ) software. It has a client-server architecture and has been designed as a highly scalable system, capable of handling hundreds of requests in parallel.

## Integration of the RBAC system
In order to have a consistent security policy across all ATLAS subsystems a synchronization mechanism was implemented to integrate the RBAC policies with various other security components, including:

- the Detector Control System (DCS) Access Control;
- login restrictions to Windows machines;
- POSIX groups used at the filesystem level.

The synchronization mechanism is based on a monitoring process running on the LDAP provider server which sends notification to several synchronization processes whenever a role to user relation changes. After receiving a trigger the listener process connects to one of the LDAP servers, gets the updated user to role relationships and performs the required changes.

The full list of user enabled DCS-related roles (explicit and inherited) is passed to the DCS Access Control system to avoid the need for duplicating and synchronizing the whole role hierarchy.

## Policy Enforcement Point
The Control Room Desktops are customized with KIOSK [5] so that the available set of functions and applications is limited. The application execution is authorized by the Access Manager.

### Access Manager

**Policy Decision Point**

- **TDAQ Access Manager Server**
  - OS Level (sudo, PAM, Privileged protection)
- **LDAP**
  - LDAP provider (read/write)
- **LDAP consumers (read only)**
  - LDAP Cluster
  - Contains user account information, roles, role hierarchies and assignment of roles to users.

### Access Control

- **Configuration management of roles**
  - Role assignment and removal

## Policy Information Point
- **ATCN (ATLAS Technical & Control Network)**

### Access Control

- **Configuration management of roles**
  - Role assignment and removal

## List of authors

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>M. L. Balsen</td>
<td>Politechnical University Bucharest</td>
<td>Romania</td>
</tr>
<tr>
<td>M. Dobson</td>
<td>CERN, Switzerland</td>
<td>Switzerland</td>
</tr>
<tr>
<td>G. Lehmann Mottio</td>
<td>CERN, Switzerland</td>
<td>Switzerland</td>
</tr>
<tr>
<td>D. A. Scannechie</td>
<td>University of California at Irvine</td>
<td>USA</td>
</tr>
<tr>
<td>S. Schlenker</td>
<td>CERN, Switzerland</td>
<td>Switzerland</td>
</tr>
<tr>
<td>L. Filimonov</td>
<td>Petersburg Nuclear Physics Institute, Russia</td>
<td>Petersburg Nuclear Physics Institute, Russia</td>
</tr>
<tr>
<td>V. Khomoutnikov</td>
<td>Politechnical University Bucharest</td>
<td>Romania</td>
</tr>
<tr>
<td>I. Dumitru</td>
<td>Budker Institute of Nuclear Physics, Russia</td>
<td>Petersburg Nuclear Physics Institute, Russia</td>
</tr>
<tr>
<td>A. S. Zaytsev</td>
<td>Budker Institute of Nuclear Physics, Russia</td>
<td>Petersburg Nuclear Physics Institute, Russia</td>
</tr>
<tr>
<td>A. A. Korol</td>
<td>Budker Institute of Nuclear Physics, Russia</td>
<td>Petersburg Nuclear Physics Institute, Russia</td>
</tr>
<tr>
<td>A. Bogdantchikov</td>
<td>University of California at Irvine</td>
<td>USA</td>
</tr>
<tr>
<td>G. Avolos</td>
<td>University of Johannesburg, South Africa</td>
<td>Politechnical University Bucharest, Romania</td>
</tr>
<tr>
<td>G. L. Darlea</td>
<td>Politechnical University Bucharest</td>
<td>Romania</td>
</tr>
<tr>
<td>M. Twomey</td>
<td>University of Washington, USA</td>
<td>USA</td>
</tr>
<tr>
<td>F. Bujor</td>
<td>Politechnical University Bucharest</td>
<td>Romania</td>
</tr>
<tr>
<td>C. Caramacu</td>
<td>National Institute of Physics and Nuclear Engineering, Romania</td>
<td>Romania</td>
</tr>
</tbody>
</table>

## References

5. K. D. E. V., Darmstadt, Germany, "KIOSK", [Online], available: http://techbase.ksd.org/KDE_System_Administration/Kiosk/