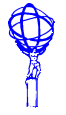
System Administration, Controls and CoordinationATLAS RBAC Administration Tool1.01DraftATLAS-TDAQ-2007-XXX16 April 2007CERN

ATLAS TDAQ



Requirements

Document Version:

Document ID: ATLAS-TDAQ-2007-XXX

Document Date:

Document Status:

Abstract

The document presents the user requirements for the ATLAS RBAC Administration Tool. They shall be the basis for the evaluation of the commercial products candidates for the ATLAS’ roles and policies administration. They shall be also the basis for the design and implementation of the tool to be developed for this purpose.

Institutes and Authors:

CERN: M. Leahu

Politehnica University of Bucharest: M. Leahu

Table 1 Document Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| **Title:** | ATLAS TDAQ Requirements | | |
| **ID:** |  | | |
| **Version** | **Issue** | **Date** | **Comment** |
| 1.0 | 1 | 16 April 2007 | Initial version |
| 1.0 | 2 | 17 April 2007 | Added requirement URNA02 |
| 1.0 | 3 | 11 May 2007 | Comments from Gokhan taken into account: the requirements URR20, URR21, URR22, URNA03.  Added requirements checklists. |

# Introduction

The ATLAS DAQ and DCS access control is based on users, roles and policies following the Role Based Access Control Model. While the users’ management is the responsibility of the System Administration, the roles and the access control policies have to be managed at a higher level to preserve the coherence of the ATLAS access control scheme. The shall be able to administrate the roles, the assignment of roles to users and the access control policies within the ATLAS experiment.

## Purpose of the document

This document presents the Requirements for the ATLAS RBAC Administration Tool of the ATLAS TDAQ/DCS System Administration, Controls and Coordination. They shall be the basis for the design and implementation of the ATLAS RBAC Administration Tool in the context of the ATLAS Trigger DAQ/DCS system.

## Glossary, acronyms and abbreviations

### Glossary

**Role Based Access Control**

An approach to restrict the system access to authorized users using the role information assigned to the users and the access policies based on roles and permissions.

**User**

A person or automated agent.

**Role**

Job function or job title within ATLAS experiment which defines an authority level.

**Senior Role**

The role A is senior for the role B if the role A inherits the role B.

**Junior Role**

The role B is junior for the role A if the role A inherits the role B.

**Permission**

Approval of a particular action to one or more resources in the ATLAS system.

### Acronyms and Abbreviations

|  |  |
| --- | --- |
| **AM** | Access Manager |
| **CERN** | European Laboratory for Particle Physics |
| **CNIC** | Computing and Network Infrastructure for Controls |
| **CRD** | Control Room Desktop |
| **DAQ** | Data AcQuisition system |
| **DCS** | Detector Control Systems |
| **DSD** | Dynamic Separation of Duties |
| **GUI** | Graphical User Interface |
| **RBAC** | Role Based Access Control |
| **SSD** | Static Separation of Duties |
| **XACML** | eXtensible Access Control Markup Language |

## References

1. Proposed NIST Standard for Role-Based Access Control  
   <http://csrc.nist.gov/rbac/rbacSTD-ACM.pdf>
2. Access Manager Requirements  
   <https://edms.cern.ch/document/484984/2>
3. XACML standard  
   <http://www.oasis-open.org/specs/index.php#xacmlv2.0>
4. CNIC Policy  
   <https://edms.cern.ch/document/584092/1.4>

# General Description

The NIST RBAC model [1] defines four access control model components:

* Core RBAC
* Hierarchical RBAC
* Static Separation of Duty Relations
* Dynamic Separation of Duty Relations.

The ATLAS experiment is implementing the Hierarchical RBAC (which includes the Core RBAC) in all the systems, but the necessity of constrained RBAC models (SSD, DSD) may occur in some complex and critical systems. In conclusion, all the models could exist in the ATLAS experiment at one moment in time and the administration tool shall be able to manage the access policies corresponding to each access control model component.

The elements for all the RBAC models are represented in the Figure 1. There are five basic data elements called users (USERS), roles (ROLES), resources (RES), and actions (ACT). The concept of roles relations is used to formulate policies. The relations are User Assignment (UA), Permission Assignment (PA) and Role Hierarchy (RH). They are many-to-many relationship, e.g. a user can be assigned to one or more roles and a role can be assigned to one or more users. Each session is a mapping of one user to possibly many roles, that is, a user establishes a session during which the user activates some subset of roles that he or she is assigned.

session  
role

user

session

Role Hierarchy

(RH)

Permission  
Assignment

(PA)

User   
Assignment

(UA)

Figure SSD and DSD within Hierarchical RBAC

The functions required to create and maintain the RBAC model components can be separated in three categories:

* *Administrative Functions*: creation and maintenance of element sets and relations for building the various component RBAC models
* *Supporting System Functions*: functions that are required by the RBAC implementation to support the RBAC model constructs (e.g., RBAC session attributes and access decision logic) during user interaction with an IT system
* *Review Functions*: review the results of the actions created by the administrative functions

The functionalities of ATLAS RBAC Administration Tool are split over three tool sub components according to the functional categories mentioned above:

1. **Administrative Component**
2. **Users Sessions Component**
3. **Review Component**

## Context of the ATLAS RBAC Administration Tool

The external systems with which the ATLAS RBAC Administration Tool interacts are presented in Figure 2. The databases with users’ information, services configuration and roles and access policies represent the central data repository used by the operating system and software applications.

The ATLAS RBAC Administration Tool should expose an interface to allow external systems to register for notifications events (e.g. access policy is changed and the external system must update their configuration).

The DAQ AM [2] interface with ATLAS RBAC Administration Tool is the set of access policies defined in XACML [3] format. The policies are stored in the database wherefrom the DAQ AM retrieves them for its internal use.

**SOFTWARE APPLICATIONS**

DAQ AM

DCS PVSS

**OPERATING SYSTEM**

Users

Management

Security

Mechanisms

**DATABASES**

Users, Groups

Services Configuration

Roles, Policies

**RBAC ADMINISTRATION TOOL**

Data flow

Notificationss

CRD

Figure ATLAS RBAC Administration Tool interraction with external systems

## General capabilities of ATLAS RBAC Administration Tool

The ATLAS RBAC Administration Tool shall provide the general functions required to create and maintain the RBAC model components (element sets and relations). Following is a brief description of these functions for each component:

* + **Core RBAC**
    - *Administrative Functions*: Create and administrate the element sets (USERS, ROLES, RES, ACT) and the relations (user-to-role assignment relation (UA), permission-to-role assignment relation (PA))
    - *Supporting System Functions*: Enable and disable the roles assigned to a user for the current user session.
    - *Review Functions*: Return the set of users assigned to a given role, return the set of roles assigned to a given user and other functions like return the permissions granted to a given role or user.
  + **Hierarchical RBAC** (includes the Core RBAC functions, therefore only the new functions are listed below)
    - *Hierarchical Administrative Functions:* Add/remove inheritance relationship between two existing roles, create new role and add it as immediate ascendant/descendant of an existing role.  
      **Note**: The role hierarchy is limited to a *tree* structure.
    - *Supporting System Functions*: Enable and disable the roles assigned *directly* to the user. The roles inherited by an enabled role are not *explicitly* enabled. It is up to the system enforcing the access policies to take into account or not the inherited roles.
    - *Review Functions*: The functions specified for the Core RBAC model including the roles inherited by a given role.
  + **SSD Relation** (includes the Hierarchical RBAC functions, therefore only the new functions are listed below)
    - *Administrative Functions*: Create and delete the SSD sets, add and delete a role from a SSD set.
    - *Review Functions*: Return the set of named SSD relations; return the set of roles associated with a named SSD role set.
  + **DSD Relation** (includes the Hierarchical RBAC functions, therefore only the new functions are listed below)
    - *Administrative Functions*: Create and delete the DSD sets, add and delete a role from a DSD set.
    - *Review Functions*: Return the set of named DSD relations; return the set of roles associated with a named DSD role set.

In addition to these functionalities, the ATLAS RBAC Administration Tool shall provide a GUI and command line tools.

## General constraints

The ATLAS RBAC Administration Tool shall function properly in the ATLAS system with no connection or dependency outside ATLAS system.

## General assumptions and dependencies

The ATLAS RBAC Administration Tool interacts with the other systems through the **databases**, but the databases administration is not its responsibility. It is assumed the databases are accessible 24/7 inside the ATLAS system.

The **user accounts** information necessary to associate roles to users is retrieved from the databases, but the user accounts administration is not part of the responsibilities of ATLAS RBAC Administration Tool.

## User characteristics

There are 2 categories of users: the administrators and the shifters. The administrators shall define the roles, the access policies and assign/revoke the roles to/from users. The shifters shall enable and disable the roles already assigned to users by the administrators.

# Specific Constraints, Assumptions/Dependencies, Use Cases and Requirements

## Constraints

**CO001 CNIC Policy Compliance**

The tool shall not break the security of the ATLAS Controls System which complies with the CNIC policy [4].

Note The tool may operate with the user accounts and their security is regulated by the CNIC policy.

**CO002 XACML Compatibility**

The access policies storage format shall be compatible with the XACML standard.

Note The constraint is because the DAQ AM processes the access policies in the XACML format.

### Constraints

**CO101 Organizational Roles**

The administrative organization of users in groups shall be reflected in the roles definition and roles hierarchy.

Note The detectors and sub detectors shall have the roles defined with their names.

**CO102 Functional Roles**

The level of expertise in a given area and the user’s function in that area shall be reflected in the roles definition and roles hierarchy.

Note The detectors experts and sub detectors experts shall have the roles defined with unique names.

## Assumptions and Dependencies

**AD001 Users accounts availability**

The user accounts in the ATLAS system shall be stored in a database which is available for interrogation 24/7.

Note The user accounts database should have a well defined interface for interrogations.

## Use Cases

The main use cases for each component are presented in the use case diagrams in the following paragraphs.

### Use Cases

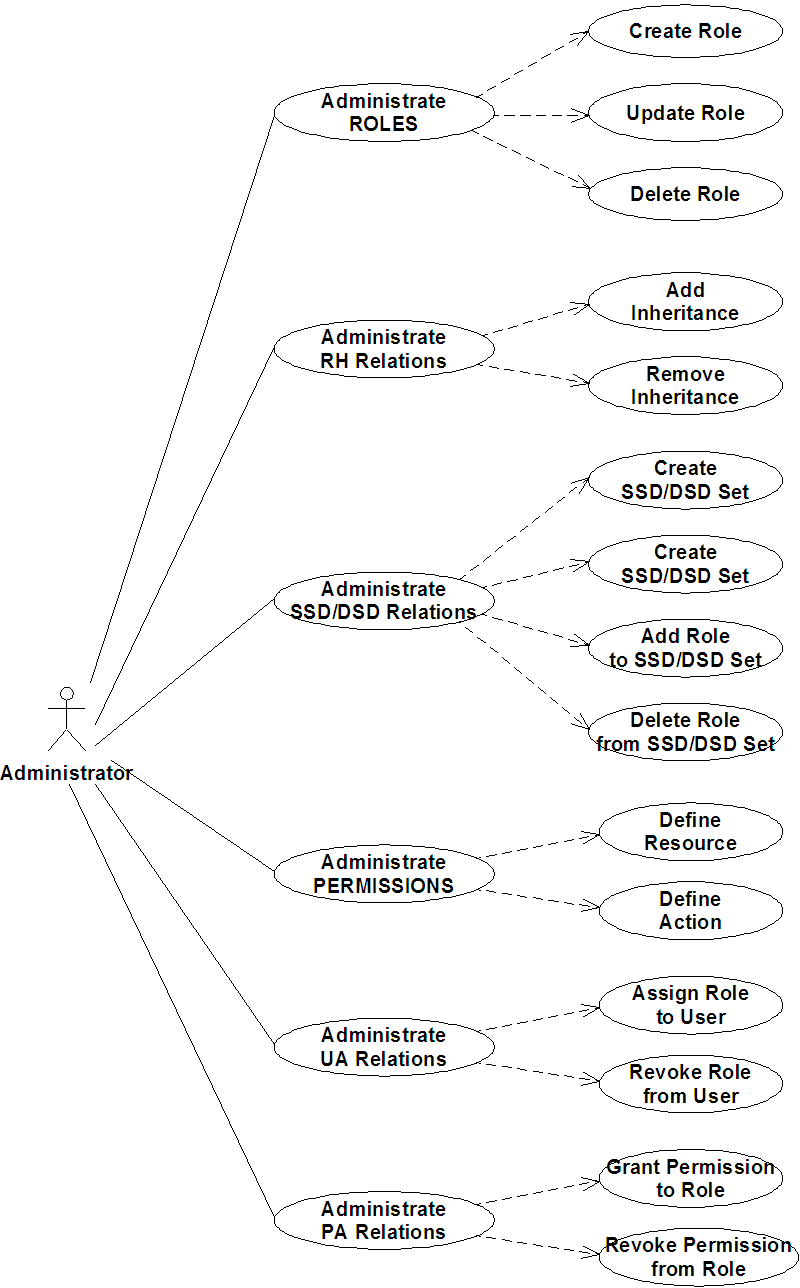


Figure Use Case Diagram for

### Use Cases

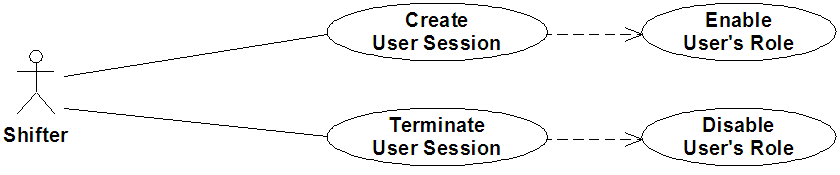


Figure Use Case Diagram for

### Use Cases

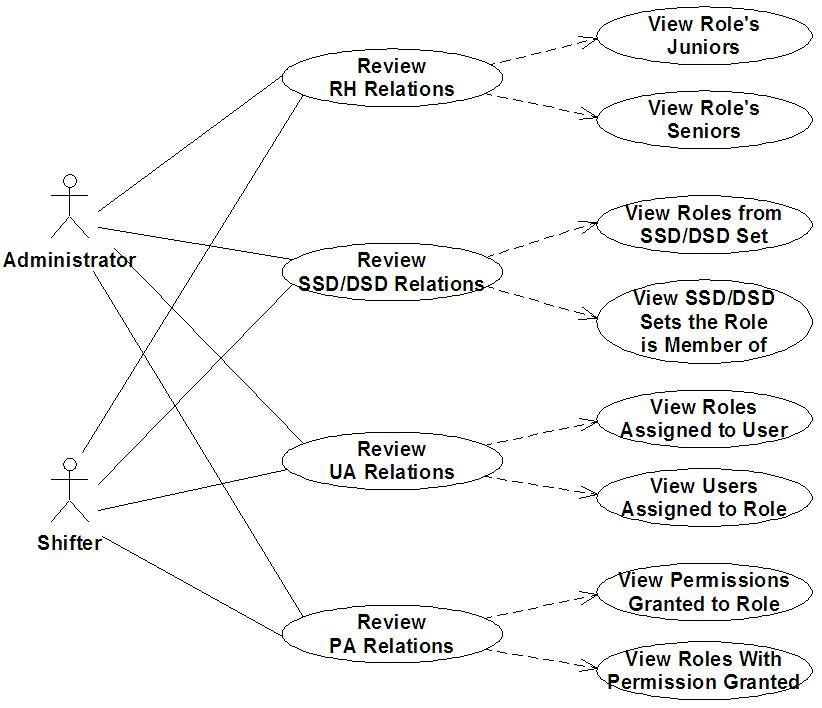


Figure Use Case Diagram for

## Functional Requirements

### Functional Requirements

URA01 Role Creation

The shall provide the means to create a unique role in the system.

Priority High

Note The role should have various attributes like the description, the creation date, the person responsible for it, etc.

URA02 Role Update

The shall provide the means to update the role attributes.

Priority High

Note The attribute *creation date* should be read only.

URA03 Role Deletion

The shall provide the means to delete a role from the system.

Priority High

Note The requirement URNA01 shall be met.

URA04 Role Inheritance Creation

The shall provide the means to establish a new immediate inheritance relationship (RH relation) between two existing roles.

Priority High

Note The requirement URNA01 shall be met.

URA05 Role Inheritance Deletion

The shall provide the means to delete an existing immediate inheritance relationship (RH relation) between two roles.

Priority High

Note If the role A inherits the role B and the role B inherits the role C, then the roles A and C have implicit inheritance relationship. The deletion of the inheritance relationship between the roles A and B shall not preserve the implicit relationship between the roles A and C.

The requirement URNA01 shall be met.

URA06 Senior Role Creation

The shall provide the means to create a new role and add it as an immediate senior of an existing role.

Priority High

Note The requirement URNA01 shall be met.

URA07 Junior Role Creation

The shall provide the means to create a new role and add it as an immediate junior of an existing role.

Priority High

Note The requirement URNA01 shall be met.

URA08 SSD Set Creation

The shall provide the means to create a named instance of an SSD relation. The SSD cardinality shall be set at creation time.

Priority Normal

Note The SSD relation is defined as a role set that includes two or more roles, and the cardinality as a natural number greater than one indicating a combination of roles that would constitute a violation of the SSD policy. For example, it may be required that no user may be assigned to three of the four roles representing the detector expert functions.

URA09 SSD Set Deletion

The shall provide the means to delete an existing SSD relation.

Priority Normal

URA10 SSD Role Member Addition

The shall provide the means to add an existing role to a named SSD role set.

Priority Normal

Note The requirement URNA01 shall be met.

URA11 SSD Role Member Deletion

The shall provide the means to delete a role from a named SSD role set.

Priority Normal

Note The requirement URNA01 shall be met.

URA12 DSD Set Creation

The shall provide the means to create a named instance of a DSD relation. The DSD cardinality shall be set at creation time.

Priority Low

Note The DSD relation is defined as a role set that includes two or more roles, and the cardinality as a natural number greater than one indicating a combination of roles that would constitute a violation of the DSD policy. For example, it may be required that no user may enable three of four roles already assigned to him.

URA13 DSD Set Deletion

The shall provide the means to delete an existing DSD relation.

Priority Low

URA14 DSD Role Member Addition

The shall provide the means to add an existing role to a named DSD role set.

Priority Low

Note The requirement URNA01 shall be met.

URA15 DSD Role Member Deletion

The shall provide the means to delete a role from a named DSD role set.

Priority Low

Note The requirement URNA01 shall be met.

URA16 Resource Definition

The shall provide the means to define a resource using the predefined resource types available in the ATLAS system.

Priority High

Note The resource types shall be defined in agreement with the sub systems that enforce the access policies. The resources and the actions are used to define permissions.

URA17 Action Definition

The shall provide the means to define an action using the predefined actions available in the ATLAS system.

Priority High

Note The action types shall be defined in agreement with the sub systems that enforce the access policies. The resources and the actions are used to define permissions.

URA18 Permission Definition

The shall provide the means to define a permission as a relation between resource and action.

Priority High

Note The permission shall have the meaning “the action is granted on the resource”. This is the “denied by default” access policy.

URA19 Role Assignment to Users

The shall provide the means to assign an existing role to a set of existing users (UA relation).

Priority High

Note The requirement URNA01 shall be met.

The requirement URNA02 shall be met.

URA20 Role Revocation from Users

The shall provide the means to revoke a *directly* assigned role from a set of users (UA relation).

Priority High

Note The roles indirectly assigned to users through the inheritance relation shall not be revocable.

The requirement URNA01 shall be met.

The requirement URNA02 shall be met.

URA21 Grant Permission to Role

The shall provide the means to grant a permission to an existing role.

Priority High

Note The requirement URNA01 shall be met.

URA22 Revoke Permission from Role

The shall provide the means to revoke a permission from a role.

Priority High

Note The requirement URNA01 shall be met.

### Functional Requirements

URUS01 User’s Role Enabling

The shall provide the means to enable a user’s assigned role.

Priority Normal

Note Only the roles *directly* assigned to the user can be enabled.

If a subset of roles assigned to the user is in the inheritance relationship, then only *one* role from the subset shall be enabled at one time.

The requirement URNA01 shall be met.

URUS02 User’s Role Disabling

The shall provide the means to disable a user’s assigned role.

Priority Normal

Note Only the roles *directly* assigned to the user can be disabled.

### Functional Requirements

URR01 View Role’s Juniors

The shall provide the means to view the role’s junior roles.

Priority Normal

Note The tool shall display on request the roles that are indirectly its juniors due to inheritance relationship.

URR02 Graphical Display of Role’s Juniors

The shall display graphically the role’s junior roles.

Priority Low

Note The tool shall display on request the roles that are indirectly its juniors due to inheritance relationship.

URR03 View Role’s Seniors

The shall provide the means to view the role’s senior roles.

Priority Normal

Note The tool shall display on request the roles that are indirectly its seniors due to inheritance relationship.

URR04 Graphical Display of Role’s Seniors

The shall display graphically the role’s senior roles.

Priority Low

Note The tool shall display on request the roles that are indirectly its seniors due to inheritance relationship.

URR05 View Roles from a SSD Set

The shall provide the means to view the roles member of a named SSD set.

Priority Normal

Note The tool shall display on request the roles that are indirectly seniors of the roles member of the named SSD set. Those roles are also in the SSD relation.

URR06 View Roles from a DSD Set

The shall provide the means to view the roles member of a named DSD set.

Priority Normal

Note The tool shall display on request the roles that are indirectly seniors of the roles member of the named DSD set. Those roles are also in the DSD relation.

URR07 View the SSD Sets a Role is Member of

The shall provide the means to view the named SSD sets an existing role is member of.

Priority Normal

Note The tool shall display on request the SSD sets its junior roles are member of. The role is also member of those SSD sets.

URR08 View the DSD Sets a Role is Member of

The shall provide the means to view the named DSD sets an existing role is member of.

Priority Normal

Note The tool shall display on request the DSD sets its junior roles are member of. The role is also member of those DSD sets.

URR09 View Roles Assigned to User

The shall provide the means to view the roles assigned to a user.

Priority Normal

Note The tool shall display on request the roles indirectly assigned to the user due to the inheritance relationships.

URR10 View Users Assigned to Role

The shall provide the means to view the users assigned to a role.

Priority Normal

Note The tool shall display on request the users assigned to the role’s seniors.

URR11 View Roles Enabled for User

The shall provide the means to view the roles enabled for a user.

Priority Normal

Note The tool shall display on request the roles indirectly enabled to the user due to the inheritance relationships.

URR12 View Roles Disabled for User

The shall provide the means to view the roles disabled for a user.

Priority Normal

Note The tool shall display on request the roles indirectly disabled to the user due to the inheritance relationships.

URR13 View Users with a Role Enabled

The shall provide the means to view the users with a given role enabled.

Priority Normal

Note The tool shall display on request the users with the role’s seniors enabled.

URR14 View Users with a Role Disabled

The shall provide the means to view the users with a given role disabled.

Priority Normal

Note The tool shall display on request the users with the role’s seniors disabled.

URR15 View Permissions Granted to Role

The shall provide the means to view the permissions granted to an existing role.

Priority Normal

Note The tool shall display on request the permissions granted to the role’s juniors.

URR16 View Permissions Granted to User

The shall provide the means to view the permissions granted to a user through his or her assigned roles.

Priority Normal

Note The tool shall display on request the permissions granted to the user through the role inheritance relationships.

URR17 View Actions Allowed on Resource for Role

The shall provide the means to view the set of actions a given role may perform on a given resource.

Priority Normal

Note The tool shall display on request the set of actions allowed to be performed through the role inheritance relationships.

URR18 View Actions Allowed on Resource for User

The shall provide the means to view the set of actions a given user may perform on a given resource.

Priority Normal

Note The tool shall display on request the set of actions allowed to be performed through the role inheritance relationships.

URR19 View Roles with Permission Granted

The shall provide the means to view the set of roles with a given permission granted.

Priority Normal

URR20 Search Resources

The shall provide the means to search the defined resources.

Priority Normal

Note The requirement URNA03 shall be met.

URR21 Search Actions

The shall provide the means to search the defined actions.

Priority Normal

Note The requirement URNA03 shall be met.

URR22 Search Permissions

The shall provide the means to search the defined permissions.

Priority Normal

Note The requirement URNA03 shall be met.

## Non-Functional Requirements

Performance Requirements

URPER01

The shall not affect at all the ATLAS system running performance.

Priority Normal

Note Since this tool changes only the state of roles during the system operational period, it should not affect the system performance.

Portability Requirements

URPOR01 Operating System

The shall be able to run successfully on a Scientific Linux CERN operating system.

Priority Normal

Note The Scientific Linux CERN version used will be version officially maintained by the CERN IT.

Interface Requirements

URI01 Graphical User Interface

The shall provide a graphical user interface for operating all the 3 components.

Priority Normal

URI02 Command Line Interface

The shall provide a command line interface for operating all the 3 components.

Priority Normal

Note The command line tools shall be developed in one of the Linux scripting languages.

Operational Requirements

URO01 Remote Operation

The shall be accessible remotely from anywhere in ATLAS system for operating all the 3 components using both the GUI and command line interface.

Priority Normal

Security Requirements

URS01 Self Access Control

The shall be protected with the RBAC mechanisms administrable by itself.

Priority Normal

Note The access policy for this tool specification is not subject of this document.

URS01 Operation Traceability

The shall provide a mechanism for operation traceability.

Priority Normal

Note All operations performed with the 3 components should be traceable for debug or supervision purposes.

Resource Requirements

URRES01 Hardware Requirements

The shall run successfully on the following hardware configuration:

#CPU Core:

CPU Freq:

Mem:

HDD:

Priority Normal

URRES01 Software Requirements

The shall run successfully on the Scientific Linux CERN operating system distribution with the software provided from CERN Linux Soft repository and any other software under Public Domain license.

Priority Normal

Note If the tool is purchased, the above requirements remain valid meaning no other software has to be purchased to ensure its functionality.

Documentation Requirements

URD01 User Manual

The user manual document shall be available with the description of steps to be followed to fulfil all the requirements in the current document.

Priority Normal

### Non-Functional Requirements

URNA01 Relationships Integrity

The functions shall preserve the integrity of the relationships RH, SSD, DSD, UA and PA.

Priority High

Note Every function that changes roles or relationships shall not violate the integrity of other relationships in the system.

URNA02 Selection Filters

The selection filters needed to generate sets of users shall accept wildcards.

Priority Normal

Note The wildcards shall include the “\*” character (stands for any characters) and “?” character (stands for any character).

URNA03 Search Filters

The search filters used to list the resources, the actions or the permissions shall accept wildcards.

Priority Normal

Note The wildcards shall include the “\*” character (stands for any characters) and “?” character (stands for any character).

# Requirements Checklist

Functional Requirements

| **Requirement ID** | **Priority** | **Fulfilled** | **Observations** |
| --- | --- | --- | --- |
| URA01 Role Creation | High |  |  |
| URA02 Role Update | High |  |  |
| URA03 Role Deletion | High |  |  |
| URA04 Role Inheritance Creation | High |  |  |
| URA05 Role Inheritance Deletion | High |  |  |
| URA06 Senior Role Creation | High |  |  |
| URA07 Junior Role Creation | High |  |  |
| URA08 SSD Set Creation | Normal |  |  |
| URA09 SSD Set Deletion | Normal |  |  |
| URA10 SSD Role Member Addition | Normal |  |  |
| URA11 SSD Role Member Deletion | Normal |  |  |
| URA12 DSD Set Creation | Low |  |  |
| URA13 DSD Set Deletion | Low |  |  |
| URA14 DSD Role Member Addition | Low |  |  |
| URA15 DSD Role Member Deletion | Low |  |  |
| URA16 Resource Definition | High |  |  |
| URA17 Action Definition | High |  |  |
| URA18 Permission Definition | High |  |  |
| URA19 Role Assignment to Users | High |  |  |
| URA20 Role Revocation from Users | High |  |  |
| URA21 Grant Permission to Role | High |  |  |
| URA22 Revoke Permission from Role | High |  |  |
| URUS01 User’s Role Enabling | Normal |  |  |
| URUS02 User’s Role Disabling | Normal |  |  |
| URR01 View Role’s Juniors | Normal |  |  |
| URR02 Graphical Display of Role’s Juniors | Low |  |  |
| URR03 View Role’s Seniors | Normal |  |  |
| URR04 Graphical Display of Role’s Seniors | Low |  |  |
| URR05 View Roles from a SSD Set | Normal |  |  |
| URR06 View Roles from a DSD Set | Normal |  |  |
| URR07 View the SSD Sets a Role is Member of | Normal |  |  |
| URR08 View the DSD Sets a Role is Member of | Normal |  |  |
| URR09 View Roles Assigned to User | Normal |  |  |
| URR10 View Users Assigned to Role | Normal |  |  |
| URR11 View Roles Enabled for User | Normal |  |  |
| URR12 View Roles Disabled for User | Normal |  |  |
| URR13 View Users with a Role Enabled | Normal |  |  |
| URR14 View Users with a Role Disabled | Normal |  |  |
| URR15 View Permissions Granted to Role | Normal |  |  |
| URR16 View Permissions Granted to User | Normal |  |  |
| URR17 View Actions Allowed on Resource for Role | Normal |  |  |
| URR18 View Actions Allowed on Resource for User | Normal |  |  |
| URR19 View Roles with Permission Granted | Normal |  |  |
| URR20 Search Resources | Normal |  |  |
| URR21 Search Actions | Normal |  |  |
| URR22 Search Permissions | Normal |  |  |

| **Requirement ID** | **Priority** | **Fulfilled** | **Observations** |
| --- | --- | --- | --- |
| URPER01 | Normal |  |  |
| URPOR01 Operating System | Normal |  |  |
| URI01 Graphical User Interface | Normal |  |  |
| URI02 Command Line Interface | Normal |  |  |
| URO01 Remote Operation | Normal |  |  |
| URS01 Self Access Control | Normal |  |  |
| URS01 Operation Traceability | Normal |  |  |
| URRES01 Hardware Requirements | Normal |  |  |
| URRES01 Software Requirements | Normal |  |  |
| URD01 User Manual | Normal |  |  |
| URNA01 Relationships Integrity | Normal |  |  |
| URNA03 Search Filters | Normal |  |  |
| URNA02 Selection Filters | Normal |  |  |

This document has been prepared using the Requirements Document Template provided and approved by the Atlas TDAQ and DCS Connect Forum. For more information, go to

<http://atlas-connect-forum.web.cern.ch/Atlas-connect-forum/>.

This template is based on the SDLT Single File Template that have been prepared by the IPT Group (Information, Process and Technology), IT Division, CERN (The European Laboratory for Particle Physics) and then converted to MS Word. For more information, go to http://framemaker.cern.ch/.