CERN
CH-1211 Geneva 23
Switzerland

the
Large Hadron Collider
project

LHC Project Document No.
LHC-C-ES-0007 rev 1.0

CERN Div./Group or Supplier/Contractor Document No.
AB-OP

EDMS Document No.
769302

Date: 2006-11-01

Functional specification

ROLE BASED ACCESS FOR THE ACCELERATOR CONTROL SYSTEM IN THE LHC ERA - REQUIREMENTS

Abstract

Given the significant dangers of LHC operations, access control to the accelerator controls network will be required. This document describes the requirements for Role Based Access (RBA) for the LHC & injectors controls systems.

Prepared by:	*Checked by:*	*Approved by:*
S. Gysin FNAL CD/AMR	**J. Wenninger AB/OP**	**P. Collier AB/OP**
K. Kostro AB/CO	**S. Page AB/PO**	**H. Schmickler AB/CO**
G. Kruk AB/CO	**E. Hatziangeli AB/CO**	**R. Bailey AB/OP**
M. Lamont AB/OP	**V. Kain AB/OP**	**S. Myers AB**
S. Lueders IT/CO	**K. Hanke AB/OP**	
W. Sliwinski AB/CO	**R. Schmidt AB/CO**	
P. Charrue AB/CO	**R. Steerenberg AB/OP**	

History of Changes

Rev. No.	*Date*	*Pages*	*Description of Changes*
0.1	2006-06-29	All	First draft
0.2	2006-08-01	All	Authors' review
0.3	2006-08-18	All	Revision for review
	2006-08-25	All	Submission for approval
1.0	2006-11-01	All	Version released

Table of Contents

1. INTRODUCTION 4
2. AUTHENTICATION AND AUTHORIZATION 4
3. ASSUMPTIONS 5
4. REQUIREMENTS 5
4.1 AUTHENTICATION REQUIREMENTS – A1 5
4.2 AUTHORIZATION REQUIREMENTS – A2 6
5. ISSUES AND QUESTIONS 9
6. CURRENT THOUGHTS ON THE DESIGN 10
7. USE CASES 10
7.1 OPERATOR (OP)/MACHINE PHYSISIST (MP) IN THE CCC 10
7.2 TIMEOUTS ON SETTINGS ENABLED AND APPLICATIONS AT THE TEVATRON . 10
7.3 ROLES AND PERMISSIONS 11
7.4 EXPERT INTERVENTION FROM REMOTE LOCATION DURING A PHYSICS FILL. 12
7.5 RBA AND MANAGEMENT OF CRITICAL SETTINGS 12
7.5.1 USE CASE – MAKING A CRITICAL SETTING FROM THE TRIM APPLICATION (LSA) 12
7.6 USE CASE: AUTHORIZATION FOR BATCH SETTINGS 13
8. SUMMARY 13
9. REFERENCES 13
10. GLOSSARY 14

1. INTRODUCTION

Role Based Access (RBA), also referred to as Role Based Access Control (RBAC) is an approach to restrict system access to authorized users. Within an organization, roles are created for various job functions. The permissions to perform certain operations ('permissions') are assigned to specific roles. Members of staff (or other system users) are assigned particular roles, and through those role assignments acquire the permissions to perform particular system functions.

RBA differs from access control lists (ACL's) used in traditional discretionary access control systems in that it assigns permissions to specific operations with meaning in the organization, rather than to low level data objects. For example, an access control list could be used to grant or deny write access to a particular system file, but it would not say in what ways that file could be changed. In a RBA based system an operation might be to create a 'credit account' transaction in a financial application or to populate a 'blood sugar level test' record in a medical application. The assignment of permission to perform a particular operation is meaningful, because the operations are fine grained and themselves have meaning within the application. [1]

The high level LHC control software (LSA [2]) needs to provide protection from unauthorized or accidental settings by users who should have only read permission or intend to only monitor data - possibly using the same applications that are used to modify settings.

The CNIC Working Group [3] has identified four use cases for accessing the LHC controls:

1) The operator in the CERN Control Centre

2) The expert from the office inside CERN

3) The expert from home

4) The expert from FNAL

For practical purpose the user at home, the user in the office inside CERN, and the one at a remote site are identical.

2. AUTHENTICATION AND AUTHORIZATION

In computer security, authentication is the process to verify the digital identity of the sender of a communication such as a request to log in. The sender being authenticated may be a person using a computer, a computer itself or a computer program.

To distinguish authentication from the closely related term authorization, the short-hand notations **A1 (authentication)** and **A2 (authorization)** are occasionally used.

The problem of authorization is often thought to be identical to that of authentication; many widely adopted standard security protocols, obligatory regulations, and even statutes are based on this assumption. However, more precise usage describes authentication as the process of verifying a person's identity, while authorization is the process of verifying that a known person has the authority to perform a certain operation. Authentication, therefore, must precede authorization. For example, when you show proper identification to a bank teller, you could be authenticated by the teller, and you would be authorized to access information about your bank accounts. You would not be authorized to access accounts that are not your own. [4]

Authentication can easily be separated from RBA, but since the LHC controls need both A1 and A2, they are both covered in this document. Keep in mind that these two functionalities can be separated at any time during design and implementation.

3. ASSUMPTIONS

For the purpose of this document, authentication is limited to the LSA framework. Authentication should be foreseen for some non-LSA applications such as the FESA explorer. There is no explicit authentication foreseen at this stage for expert applications using, say, LabView or Visual Basic.

4. REQUIREMENTS

4.1 AUTHENTICATION REQUIREMENTS – A1

No.	Requirement	Source	Priority
RA1-10	Encryption: the credentials used to authenticate the user shall be encrypted when sent over the network.	P.Charrue, Meeting, June '06	Critical
RA1-20	Hardware Independence: the method of authentication shall be independent of specialized hardware such as a card reader, finger print reader etc. This is such that a remote user does not have to purchase this hardware to gain access.	P.Charrue, Meeting, June'06	Critical
RA1-30	Quick and Simple: the operators must be able to log in quickly and easily. Therefore, the method of authentication must be straightforward for the users.	L.Mestre, Meeting, June '06	Critical
RA1-40	Authentication Method: authentication shall be done via user name and password from a personal CERN account (NICE, AFS, LDAP). The software should allow flexibility for future implementations of Kerberos and/or X.509 certificates.	M.Lamont, S.Gysin, S.Lueders, July '06	Critical
RA1-50	Single Point Authentication: outside of the CCC, the user shall have to log in only once to access all LSAs. Note: see RA1-70 and RA1-80 for login at the CCC	L.Mestre, Meeting June '06	Expected
RA1-60	Preserving LSA API: the LSA API business layer shall not change by the addition of the authentication.	L.Mestre, Meeting June '06	Critical
RA1-70	Authentication in the CCC: in the CCC, each island shall have a unique group login and password to gain access to the consoles in that island. The group logins are only used to access the physical machine, not to access individual software applications. Group logins are not valid outside of the CCC. Logging out, and loggin back in at the CCC consoles shall not be neccesary.	M.Lamont, S.Gysin , July '06	Critical
RA1-75	No extra authentication for the Console Manager in the CCC: when logging in at a CCC console with the dedicated group login and password, the Common Console Manager will start up without further login. This does not preclude starting the Console Manager under another account.	M.Lamont, S. Lueders, July '06	Critical
RA1-80	Critical Applications in the CCC: for a small number of	M.Lamont,	Critical

	critical applications, the operator in the CCC shall be required to login with her own credentials in addition to the generic login.	S.Gysin, July '06	
RA1-90	Timeout for Critical Applications in the CCC: for critical applications, there shall be a timeout to prevent accidental use, and to keep the integrity of the authentication.	M.Lamont, S.Gysin, July '06	Critical
RA1-95	Timeout expiry for inactive user: the timeout expires when there is no user activity for the set duration.	M.Lamont, S.Gysin, July '06	Critical
RA1-97	Timeout action for critical applications: upon timeout of a critical application, the writing priviledges shall be revoked and the application shall be locked down.	M.Lamont, S.Gysin, July '06	Critical
RA1-100	Critical Applications: the list of critical applications is fluid and whether or not an application needs further authentication shall be easy to change. All applications shall have the ability for further authentication, if required.	M.Lamont, S.Gysin, July '06	Critical
RA1-120	Timeout for non-critical applications: the non-critical applications shall have a configurable timeout. Upon the end of the timeout the application will exit.	M.Lamont, S.Gyisn, July '06	Optional
RA1-125	Timeout action for non critical applications: upon the end of the timeout the application will exit.	M.Lamont, S.Gyisn, July '06	Optional
RA1-130	Timeout Configuration: the timeout shall be configurable. For example: long during commissioning and MD, shorter during physics operation. Timeout will be configurable on a per application basis.	M.Lamont, July '06	Critical
RA1-140	Generic API for Role Based Access (RBA): to avoid duplication of RBA specific business logic in different applications and stay independent of changes to the data model, the RBA sofware shall provide a common, platform independent API to all the interested systems (LSA, CMW, FESA, ...)	W.Sliwinski, G.Kruk, July'06	Critical
RA1-150	RBA API information: the RBA API shall provide at least the following functionality: - authenticate a user - check user's role/privilege - list user's roles/privileges - create and manage a role	W.Sliwinski, G.Kruk July'06	Critical

4.2 AUTHORIZATION REQUIREMENTS – A2

No.	Requirement	Source	Priority
RA2-10	Safeguards for authenticated users: RBA shall be used for granting authority to read, monitor, and write to devices. RBA shall not grant the permission to make a setting when it is denied by Management of Critical Settings (MCS).	CNIC presentation, S.Lueders, M.Lamont, July '06 V. Kain, Oct.'06	Critical

RA2-25	Role Definition: a role is a named set of permissions. It defines the read, monitor, and write permissions for each device.	CNIC presentation, M.Lamont meeting June, '06	Critical
RA2-27	The following dependencies shall be respected in order to obtain authorization: USER: the user; DEVICE: the device to be acted upon: not every user has write-access to every device; MODE: the mode: depending on the accelerator mode, write-access might be inhibited; PERMISSION: the Engineer-in-Charge (EIC): general write-access must be authorized (esp. outside the CCC); LOCATION: the location: access rights are restricted when acting from home or a remote control room. For access from home, critical and non-critical settings can be distinguished. Thus Write Access permission represents a concatenation of authorisations: write_access = auth(user, device) * auth(mode) * auth(EIC) * auth(location) = role * auth(mode) * auth(EIC) * auth(location). Note: EIC = Engineer in Charge, EIC = 0 if remote, 1 if explicitly set. We do not have a clear understanding how the EIC will be implemented. Further discussion on this topic is needed. See use case 7.4	M.Lamont and S.Lueders, July '06	Critical
RA2-28	Activity Monitor: the Engineer in Change shall be able to monitor remote users and their activities.	S.Lueders, August '06	Expected
RA2-30	Accelerator Mode: the permissions for a role shall be able to be varied according to the mode of the accelerator (Injection, Ramping, Tuning, Collisions, and Shutdown). For example: With mode – could we imagine suspending authorisation. All modes with beam present imply lock out. Access/shutdown implies less restraint.	M.Lamont, July '06	Critical
RA2-40	Subject of authorization: it shall be possible to restrict access i.e. define access privileges for the following operations on each device property: read, monitor, and write. In practice, it is the write operation and exceptionally the monitor operation which will be restricted.	K.Kostro, S.Gysin, June '06	Critical
RA2-50	Default Role: when a user does not match any role, he is assigned the default role (Outsider). This role has no permissions to read, monitor, or write.	K.Kostro, S.Gysin, June '06	Critical

RA2-55	Default Device Permissions: if the device permissions for a role are not explicitly set, all write and monitor access shall be restricted, and read access shall be unrestricted.	K.Kostro, S.Gysin, June '06	Critical
RA2-60	Security Policy: management shall design, implement, and review an official security policy to determine the roles, locations, and accelerator modes. Management shall also define any restrictions as for the valid combination of the access control principles.	K.Kostro, S.Gysin, June '06	Critical
RA2-70	Access Privilege: access privileges shall be defined by the equipment owner in agreement with operations.	K.Kostro, S.Gysin, June '06	Critical
RA2-80	Role Administration: a software tool shall be deployed to administer the roles, locations, and accelerator modes.	K.Kostro, S.Gysin, June '06	Critical
RA2-90	Permission Administration: the permissions shall be defined during the design/deployment phase, and authorized administrators shall be able to edit the permissions at any time	K.Kostro, S.Gysin, June '06, M.Lamont July '06.	Critical
RA2-100	Permission Denial Notification: the user shall be notified when his actions have been rejected.	K.Kostro, S.Gysin, June '06	Critical
RA2-110	Permission Granularity: it shall be possible to define permissions for classes of equipment that are applicable to all members of the class.	K.Kostro, S.Gysin, June 2006, M.Lamont, July '06	Critical
RA2-112	Individual Override: there shall be a possibility to override device class permissions for a specific device.	M.Lamont July '06	Critical
RA2-115	Device Permission varies with Accelerator: there shall be the possibility to define a different set of permissions for the same device class on different accelerators.	K.Kostro, S.Gysin, June '06	Critical
RA2-120	Integration with Critical Settings Protection: RBA shall not interfere with the protection scheme implemented for critical settings.	LHC-CI-ES-0003	Critical
RA2-122	A request for making a change to a critical setting shall include the signature with the private key necessary to make the setting. (see Use Case 7.5.1)	V. Kain, Oct'06	Critical
RA2-125	One shall be able to submit settings to a batch operation for later execution. Unauthorized settings shall not be accepted at the time of submission. (see use case 7.6)	V. Kain Oct.'06	Critical
RA2-130	Logging/tracking: RBA shall keep track of all write actions (such as trim). It shall keep a log of the action stating the user name, the location, the day and time, the property and any parameters used to grant permission.	K.Kostro, S.Gysin, June '06	Critical
RA2-140	Archiving the Log: the action log shall be archived for a 'reasonable' time.	K.Kostro, S.Gysin, June '06	Expected

RA2-145	Performance: authorization shall be fast and shall not hinder the performance of the middle ware.	J. Wenninger, August '06	Expected
RA2-300	Granting/Revoking Access Temporarily: the Engineer in Charge or any authorized person shall be able to temporarily grant and revoke access to a person or a role. See the use case in CNIC document, shift leader giving write access section 6.5 [5] use case: debugging application	S.Lueders, July '06	Expected
RA2-310	Assuming a Role: a user shall be able to temporarily assume a pseudo role (such as sudo in Linux).		Desirable
RA2-320	Tailoring Applications to Roles: LSA applications shall have buttons grayed out or unavailable according to the role of the current user.		Desirable (can be delayed)

5. ISSUES AND QUESTIONS

1. One should be able to grant permissions on a device level, however, with 30,000 devices one should not have to grant permissions for each role and device. The appropriate grouping of devices has to be determined.
    a. Resolution: An obvious grouping for access control is accelerator. A use case would be that at the FESA design phase on a particular class of device it is decided that only LHC operation will be allowed to set property "Current". This would initially apply to all instances (devices) which implement this property as this class was designed for a specific accelerator (let's say the LHC). If we then want to reuse this class and deploy instances of the same class for the CNGS we would like allow only CNGS operation to set current on these new devices. We would then need different permission description for LHC and CNGS. The need for different permissions for devices of the same class on the same accelerators is not immediately apparent. However, by appropriate groupings this should be possible. We will start with a grouping by accelerator, if we need more granularity we can always refine the groupings.
2. Many authentication methods exist: Public Key Infrastructure, Kerberos, Login and Password, etc. Which we will implement is an open issue.
    a. Resolution: we will start with a simple encrypted login and password scheme, with built in flexibility to move to a more sophisticated approach in the future.
    b. The CERN Computer Security Team and IT/FIO, IT/IS groups have done evaluations of the authentication methods. Their findings will be a large consideration in this choice.
3. The Common Console Manager (CCM) is the window and configuration manager for each console. Usually the LSA applications are started from the CCM. How does the authentication integrate with the CCM?
    a. Resolution: In the CCC, the operators will be automatically logged into the consoles using a group login. No additional authentication at the CCM will be necessary. The login to the machine gives them permissions to start all LSA applications. Critical applications will require further authentication.
    b. NB: console authentication is different from application authentication.
4. From the experience of the super-power-cut of 29.07.06 : if authentication goes through database, should one foresee a procedure in case there are database problems? For example if you consider switching equipment ON/OFF as critical, one

may be totally blocked in case of database access problems. Remember that the LSA database was down for more than 24 hours on 29-30.07

a. Resolution: ??

6. CURRENT THOUGHTS ON THE DESIGN

The Spring frame work, which is used by LSA, provides a way to write authentication as an aspect oriented program. This means that all LSA applications use the same authentication and the credentials once authenticated can be shared by all LSA applications. A suitable tool for this is called Acegi. At this time we are thinking to use Acegi for LSA authentication.

We plan to implement the authorization in the CMW (Controls Middle Ware) layer, which is close to the front ends. All applications (not just LSA) will pass through CMW in order to access a device. (Some expert programs may have the ability to by-pass CMW and access the front-ends directly – a potentially dangerous loophole.)

We envision an Oracle database for mapping the users to roles and roles to permissions.

The RBA management application will most likely be written using Oracle forms or Java.

7. USE CASES

7.1 OPERATOR (OP)/MACHINE PHYSISIST (MP) IN THE CCC

The operator or the machine physicist enters the CCC and brings up several applications on multiple monitors and often multiple consoles. The MP will move around the CCC and share the use of software and consoles with others. Often an MP will delegate the operations of a specific application to the operator on shift. In this case it is prohibitive for the OP/MP to login on different consoles and switch user when the person executing the command changes.

For this case, a generic login on an island basis (LHCOP, or SPSOP) will be used.

For certain applications it is critical that the operator accept personal responsibility before changing a setting. In these cases, the operator will be asked to take the extra step to log in explicitly with her personal credentials. These 'critical applications' should also have a time out so that they do not linger unattended at a console (as well as the standard exit button).

This implies that there are a pre-configured set of 'critical applications' requiring LSA authentication.

If the generic login is used from any IP address other than the specific CCC-island, it shall not necessarily have the same permissions. As an AB/CO policy we may request that generic operator accounts are granted access only when used from the CCC. Outside of CCC, operators could be asked to use their 'private' logins.

7.2 TIMEOUTS ON SETTINGS ENABLED AND APPLICATIONS AT THE TEVATRON

There are two types of timeouts in the Tevatron [c/o Jim Patrick]:

– Setting enable timeouts for any application running on that console

Most of the time the setting activity that a non-Main Control Room (MCR) user is doing won't take long. The timeout greatly helps the situation where one would enable settings, "forget" they were enabled and some time later run a different possibly dangerous program.

– Application running timeouts. After a timeout period, the application is terminated. Most of the time a non-MCR user will want to look at an application for only a limited amount of time, then go off and do something else.

The timeout helps limit the amount of unnecessary I/O to front-ends. Note this timeout is purely based on application run time independent of whether there is any user activity or screen update activity (*for the LHC the timeout will be based on user activity*).

Both timeouts default to "forever" for the consoles in MCR, and smaller values for pretty much everyone outside the MCR. It is potentially very annoying to have timeouts in the MCR, especially in early phases of commissioning. You could set a timeout, and of course nothing is working well and just as it gets working you hit either the settings or application timeout and have to start over. In the MCR here, despite the availability of "comfort" displays (fixed displays in CERN language), many consoles are running other applications that people want to keep going most of the time. It would probably be annoying to have to periodically restart them.

In this approach the application would terminate so there is nothing additional to be done in RBA. This is good for technical reasons as currently CMW would take the client identity when it first established the connection to the device server. There is no concept of changing the identity of the client.

7.3 ROLES AND PERMISSIONS

Users are grouped into roles; one user can have several roles. The user's permissions are the union of all his roles' permissions.

Let's assume we have defined three roles:

LHC Operator: this role has the permission to change settings on LHC devices if the request comes from a CCC console, and the accelerator mode is such that the setting is allowed.

Remote Operator: this role has a large list of users, and settings are generally disabled.

LHC Expert: this role contains a list of users allowed to change settings using the critical applications.

Outsider: This is the default role for someone who does not fit any other defined role.

Case 1: Irene, who is on shift and uses one of the consoles of the LHC Island in the CCC. She logs in at the console using the group login. With these criteria, she is assigned the role **LHC Operator**.

Case 2: Mark, another shift leader, logs in from home into a terminal server using his personal credentials. Depending on which terminal server he logged into, he will be given a role of **XXX Operator** depending on which island he will work on (e.g. using different terminal servers for different islands). However when he tries to change a setting, the location reveals that he is not in the CCC and hence his request is rejected.

Case 3: Mark logs in at home using his own username. He is assigned the role **Remote User**. He chooses which console manager to run (SPS, PS, and LHC). He is not allowed to change any settings.

Case 4: Irene, who has already assumed the role LHC Operator in Case 1, is now opening a 'critical application'. She is prompted for a login and password. Which she answers with her personal credentials. She now assumes the role **LHC Expert**. Depending on the machine mode, she is able to change settings using the critical application.

Case 5: Guido logs in using his user name and password. His user name is not registered in any role, so he assumed the role of **Outsider**. As such he has no privileges. He realizes he has no access and sends a request to the Role administrator to add his name to the Remote User list.

7.4 EXPERT INTERVENTION FROM REMOTE LOCATION DURING A PHYSICS FILL.

Explicit permission shall be given by the EIC for a given role (e.g. RF expert) in mode PHYSICS for write access to a given RF device from a given remote LOCATION. During ACCESS mode, on the other hand, the role RF expert would have write access to RF device without the need for explicit authorisation from the EIC. (See RA2-30).

7.5 RBA AND MANAGEMENT OF CRITICAL SETTINGS

A critical setting is defined as the threshold on a device witch when exceeded triggers a beam dump. The thresholds are checked by the interlock system which will dump the beam when the readings exceed the critical setting.

Critical settings are mostly hard coded, but sometimes a critical setting needs to be changed remotely according to the accelerator state.

It is not surprising that for the critical settings a very strict additional authorization is desired. To address this need, the critical settings are managed with a private/public key encryption scheme. This has a dual purpose:

1) Authorization: only PKI encrypted settings are accepted. The encryption is checked at the device level, so that independent of the entry point, an unauthorized setting will be rejected.
2) guard against corruption : the PKI encryption will serve as a check against corruption

The "Management of Critical Settings" is documented in [6].

7.5.1 USE CASE – MAKING A CRITICAL SETTING FROM THE TRIM APPLICATION (LSA)

Below is a use case describing a person making critical setting. Verena, our authorized critical settings expert, is in the CCC. She is working on a console so she is assigned the role LHC Operator.

She opens the Trim Application to make a change to the TDI Setting, a critical setting with PKI protection.

The Trim Application is on the list of critical applications defined in the requirements above RA1-80. It requires Verena to login with her personal credentials. At this time she is assigned the role of "XXX Critical Settings Expert" by the authentication software.

Now, the Trim GUI shows her the list of critical settings she is allowed to change. Note that there are multiple groups of critical settings, she only sees the critical settings groups her role allows her to change. Note that critical settings can only be changed when the accelerator is in the 'no beam' state. If there were beam in the accelerator, Verena would not see any critical settings on her list (i.e. Trim does authorization).

She issues a command to change one of her settings. The Trim Application takes her private key and signs the setting command.

The FESA checks the signature against the public key and accepts or rejects the request. If accepted the setting is set, if rejected an error notice is sent and displayed at the Trim LSA.

7.6 USE CASE: AUTHORIZATION FOR BATCH SETTINGS

When deciding where in the architecture authorization should take place, one needs to consider that a collections of settings may be submitted at one time, stored to be executed at a later time. Settings are generated and written to a database and later sent to the hardware ("Drive Hardware"). This is done for example when the supercycle in the SPS is changed.

When a setting is executed in a sequence that depends on it's execution it is too late to raise an error during execution. An unauthorized setting should never make it into the database. Hence the setting needs to be authorized at the time it is submitted and at the time it is executed.

It may be worth debating what happens when the permission changes between submission and execution.

8. SUMMARY

Role Based Access (RBA) will be required in the LHC era to restrict accelerator system access to authorized users. In brief:

- We foresee 2 levels of authentication: at the console level with generic logins for each accelerator grouping in the CCC; at the application level for applications with potentially machine critical functionality.
- Authentication shall timeout where appropriate.
- Authorisation shall take into account: the user's role, the device, the machine mode, EIC authorisation and the user's location.
- Authorisation shall be implemented in the middleware.
- A generic API for Role Based Access shall be provided.
- The system shall be easily configurable with full logging of all actions performed.
- There will be a set of tools to allow easy visualisation, modification of the database of users, roles and permissions.

9. REFERENCES

[1] "Role Based Access Control", Wikipedia (http://en.wikipedia.org/wiki/Role_based_access_control)

[2] LHC Software Architecure, http://cern.ch/ab-project-lsa/

[3] "Security in the AB controls Infrastructure beyond CNIC", Pierre Charrue, ABMB – 20 March 2006

[4] "Authentication", Wikipedia http://en.wikipedia.org/wiki/Authentication

[5] Draft: "CNIC on Operators Accounts", Stefan Lueders

[6] "Management of Critcal Settings", V.Kain et. all LHC-CI-ES-0003 rev 1.0

10. GLOSSARY

Application lock down: the application is frozen, but the state of the application is preserved (example: Remote Desktop). The user can not continue until he authenticates himself again. Once the user is authenticated again, the state of the application is resumed.

Authentication: The process to verify the digital identity of the sender

Authorization: The process of verifying that a known person has the authority to perform a certain operation

CCC: CERN Control Centre

CCC Console: a computer located in the CERN Control Centre which has the controls software installed. This is not software, but a physical machine.

CCM: the Common Console Manager is the portal for the software applications. It is configured to run the applications for the particular accelerator.

Critical Application: these are applications on the critical application list. Any application can be labelled critical. If the application is on the critical list, the user, even when in the CCC, must log in with his personal credentials. The Sequencer, MCS, and trim are examples of critical applications.

Critical Setting:

The threshold on a device which when exceeded triggers a beam dump. The thresholds are checked by the interlock system which will dump the beam when the readings exceed the critical setting.

Device: the device to be acted upon.

EIC: the Engineer in Charge is the person responsible for the operation of the accelerator during a shift.

Location: the IP address of the CPU running the application. This is not the physical location of the user, but the IP address of the machine that is running the software.

Mode: the mode of the accelerator.

Permissions:

- **Read** = the ability to read data
- **Monitor** = the ability to receive continuous updates of data
- **Write/Set** = the ability to change the setting in an instrument

Role: a role is a named set of permissions

User: the person using the controls software