Enhanced Beam Line Access Restrictions Definitions and Use Cases

Scott McPhillips
Stanford Synchrotron Radiation Laboratory
scottm@slac.stanford.edu

August 26, 2002

Contents

1 Introduction

The beam line is a complex system, and many people with different job functions interact with it on a daily basis. Therefore the potential exists for the individual users of the system accidentally overstepping the bounds of their job function and interfering with the work of another system user.

In addition, the beam line control system is built on a network interface, and provides the user of the system the ability to interact with the beam line from nearly anywhere in the world. Although this in itself is good, the user of the system from a remote environment must again limit their own activities and somehow determine (from their remote location) that the way that they are using the system is safe. With the current system, each person using the beam line must be educated in the whole system, and be willing to restrict their own activities. Ideally, the beam line itself would limit the user's activities based on the following four factors:

1. Restrictions added to each user's account.

2. The physical location of the console that the Blu-Ice client is being displayed on.

3. Restrictions placed on the device that the user is trying to interact with.

4. The state of the beam line's hutch door.

This document introduces all of the restrictions that can be placed upon a device and relates these restrictions to the permissions that can be given to a user account. Example use cases are provided to show a subset of the possible restrictions that can be defined.

2 Actors

2.1 Beam Line Configuration Database

This database contains all of the accounts and restrictions for the users that are able to log in to Blu-Ice. It also contains a list of computers and consoles that are recognized by the DCSS system.

2.2 Beam Line Administrator

A 'Beam Line Administrator' has privileges to change the Beam Line Configuration Database and is able to modify the list of users allowed to log into DCSS using Blu-Ice.

The administrator is also able to enter computer host names into the database and classify their displays.

2.3 Hutch Door

The software will be able to detect when the hutch door is closed. It is illegal to close the hutch door with a human inside the hutch.

The hutch door status will be used by the software to determine whether or not a device can be used.

2.4 The Active and Passive Blu-Ice Clients

The software only permits one Blu-Ice client to be in control of the beam line at a time. The Blu-Ice currently in control of the beam line is referred to as the 'Active client'.

A Blu-Ice client that is not in control is called a 'Passive' client.

2.5 Computer Consoles

The location from which the Blu-Ice client logs in to DCSS is important in deciding what devices the client can control. There are three categories that can be applied to a Blu-Ice user's location: 'In-Hutch', 'Local Console', and 'Remote Console'. The Blu-Ice client will announce what computer console it is displaying on during the authentication procedure with DCSS. DCSS will check the Beam Line Configuration Database to determine the location of the console and limit the client's activities according to the rules discussed in this document.

2.5.1 In-Hutch Console

The list of 'In-Hutch' consoles will be limited to the console that is available within the hutch. Any Blu-Ice client logging in from the 'In-Hutch' console will be allowed to become the 'Active Client.' A user at the In-Hutch console should be aware of the conditions at the beam line and will be accepting full responsibility for moving motors.

Table 1: Combined user permissions

Blu-Ice User Account Type	Staff Permissions	Roaming Permissions
Local Scientist	NO	NO
Roaming Scientist	NO	YES
Local Staff	YES	NO
Roaming Staff	YES	YES

2.5.2 Local Console

A display immediately outside the hutch will probably fall into the 'Local Console' category. Any Blu-Ice client logging in from a 'Local Console' will be allowed to become the 'Active Client.'

2.5.3 Remote Console

Any display not listed in the 'Beam Line Configuration Database' will automatically be considered remote. A user that is remote must have the 'Roaming' capability turned on for their account in order to become the 'Active Client' from this type of console.

2.6 Blu-Ice user

A Blu-Ice user is a person with an SMB Unix account whose account name has been entered into the database by the 'Beam Line Administrator'. The restrictions the administrator puts upon the user decides the role that the user can fill. The administrator must be capable of placing a user into one of the following categories: 'Local Scientist', 'Roaming Scientist', 'Local Staff', or 'Roaming Staff.' The four categories could be achieved with two Boolean values in the database. This would allow the administrator to enable/disable 'Roaming' permissions and enable/disable 'Staff' permissions for each account. Table 1 shows how to combine the permission bits to obtain the four types of user accounts.

2.6.1 'Roaming' permissions for Blu-Ice users

A user account with the 'roaming' permissions turned on will be capable of starting Blu-Ice from a 'Remote' console and becoming the 'Active Client.' An account without this privilege will only be able to become the 'Active Client' from a console defined as a 'Local' or 'In-Hutch' console.

2.6.2 'Staff' permissions for Blu-Ice users

An account with 'staff' permissions is capable of interacting with a device at the level determined by the 'staff' permissions associated with a device.

An account *without* 'staff' permissions is only able to interact with a device at the level determined by the 'scientists' permissions on the device.

2.7 Beam Line Device

A device may be a motor, shutter, ion chamber, scripted device, scripted operation, or any other entity that is under the control DCSS. The restrictions placed on a device is defined on a per device basis.

Each device will have two independent sets of permissions: one for 'staff' accounts, and another for 'scientist' accounts.

Through a device's configure window in Blu-Ice, 'staff' Blu-Ice users can enable the following permissions on each device:

1. Outside Closed Hutch
2. Inside Open Hutch
3. Outside Open Hutch Local
4. Outside Open Hutch Remote
5. Passively Accessible.

Because the permissions are listed in the order of increasing ease of access to a device, the software may be implemented such that selection of a less restrictive permission will automatically select all of the more restrictive permissions as well. For example, selecting the 'Outside Open Hutch Remote' permission will also automatically add 'Outside Open Hutch Local', 'Inside Open Hutch' and 'Outside Closed Hutch.' permissions to the device as well.

In addition, the software may automatically provide at least the same permissions to 'staff' as permitted for 'scientists'.

The permissions will be discussed in order of increasing of access.

2.7.1 No Permission

Not selecting any permissions for a device prevents use of the device. It is possible to not give any permissions to 'scientists' while enabling permissions for staff.

2.7.2 Outside Closed Hutch

If it is safe for a device to be accessed while the hutch door is closed, the device can be given the 'Outside Closed Hutch' permission. If this is the most permissive setting for this device, then the hutch door must be closed to access the device.

2.7.3 Inside Open Hutch

A Blu-Ice user may use a device with the 'Inside Open Hutch' permissions from the 'In-Hutch' console.

Setting the 'Inside Open Hutch' permission for a device would be useful for devices that are recognized as completely safe to operate while being observed directly by the person interacting with the device. The operator in this case can easily evaluate the complete state of the hutch and verify that no-one is standing in the way of a motor's path.

2.7.4 Outside Open Hutch Local

A Blu-Ice user at a 'local' console may use a device with the 'Outside Open Hutch Local' permissions while the hutch door is open. Setting this as the highest level of permission for a device is useful for devices recognized as safe to operate while the state of the hutch is known by a local user interacting with the device (e.g. no-one is inside). This category can be used on beam lines where the local consoles are positioned such that it is easy to observe the state of the beam line.

Without the 'Outside Open Hutch Local' permission, a Blu-Ice user interacting with the device from a 'local' console will be unable to use the device while the hutch door is open.

2.7.5 Outside Open Hutch Remote

An operator may use the 'Outside Open Hutch Local' device with the hutch door open from a 'remote' console if the Blu-Ice user has 'roaming' permissions.

Setting this permission for a device is useful for devices recognized as safe to operate regardless of the current state of the beam line.

This permissions should be reserved for motors that are limited in strength, restricted to limited paths of motion, or are isolated from human contact.

If this permission is *not* enabled, the hutch door must be closed to interact with the device from a 'remote' console.

Table 2: Can the user become the 'Active Client'?

	In-Hutch	Local Console	Remote Console
Local Scientist	YES	YES	NO
Roaming Scientist	YES	YES	YES
Local Staff	YES	YES	NO
Roaming Staff	YES	YES	YES

2.7.6 Passively Accessible

The software usually forces the Blu-Ice user to first become the 'Active Client' before interacting with the device. However, for devices with the 'Passively Accessible' permission, a Blu-Ice client will be able to interact with the device, regardless of whether or not the client is 'active' or 'passive'. This also implies that users *without* 'roaming' permissions will still be able to interact with this device from a 'remote' console because they do not first need to become the 'Active Client'.

Simultaneous requests to move a motor without this permission would be handled on a first come, first served basis. An attempt to move a motor that is already moving will fail, and the command will need to be issued again after the current move is complete.

3 Use Cases

3.1 Becoming the Active Client

A user must become the 'Active Client' to interact with any motor that does not have the 'Passively Accessible' permission. Whether or not a client is able to become the 'Active Client' depends upon the console on which the Blu-Ice client is displaying as well as the Blu-Ice user's privileges. Table 2 shows the conditions for which the different Blu-Ice users are able to become the 'Active Client'.

3.2 Classifying gonio_phi

Gonio_phi is a device that the scientists need interact with in order to perform their experiments. The device requires no safety precautions.

Through Blu-Ice, the device is given 'Outside Open Hutch' permissions for both 'staff' and 'scientists' as shown in Table 3.

Table 4 shows the capabilities that a user has while issuing commands to this 'gonio_phi' device.

Table 3: Device permissions for 'gonio_phi'

Permission	Scientist	Staff
Outside Closed Hutch	YES	YES
Inside Open Hutch	YES	YES
Outside Open Hutch Local	YES	YES
Outside Open Hutch Remote	YES	YES
Passively Accessible.	NO	NO

Table 4: Can a Blu-Ice user move 'gonio_phi'?

	In-Hutch	Local Console	Remote Console
Local Scientist	YES	YES	NO
Roaming Scientist	YES	YES	YES
Local Staff	YES	YES	NO
Roaming Staff	YES	YES	YES

3.3 Classifying detector_z

Detector_z is a device that the scientists need interact with in order to perform their experiments. The device does require some safety precautions, because it moves a heavy detector on a track. However, the device moves slowly and is very safe to operate if the user is operating the device from the 'In-Hutch' console. Staff members may also be able to operate the device safely from immediately outside the hutch. It is always safe to operate this device remotely if the hutch door is closed.

The device is given permissions to operate 'Inside Open Hutch' for 'scientists' and 'Outside Open Hutch local' for 'staff' as shown in Table 5.

Table 6 shows the capabilities that a user has while issuing commands to this 'detector_z' device.

3.4 Classifying the Optics Motors

The optics motors are devices that the staff members move while aligning the beam line. Once the beam line is aligned, the non-staff should not be able to move these motors.

The devices are completely safe to move because they are not accessible to human contact.

The devices are given 'Outside Open Hutch Remote' permissions for 'Staff' and no permissions for 'scientists' as shown in Table 7.

Table 8 shows the capabilities that a user has while issuing commands

Table 5: Device permissions for 'detector_z'

Permission	Scientist	Staff
Outside Closed Hutch	YES	YES
Inside Open Hutch	YES	YES
Outside Open Hutch Local	NO	YES
Outside Open Hutch Remote	NO	NO
Passively Accessible.	NO	NO

Table 6: Can the Blu-Ice user move detector_z?

	In-Hutch	Local Console	Remote Console
Local Scientist	YES	YES (If hutch door closed, otherwise NO)	NO
Roaming Scientist	YES	YES (If hutch door closed, otherwise NO)	YES (If hutch door closed, otherwise NO)
Local Staff	YES	YES	NO
Roaming Staff	YES	YES	YES (If hutch door closed, otherwise NO)

Table 7: Device permissions for optics motors

Permission	Scientist	Staff
Outside Closed Hutch	NO	YES
Inside Open Hutch	NO	YES
Outside Open Hutch Local	NO	YES
Outside Open Hutch Remote	NO	YES
Passively Accessible.	NO	NO

Table 8: Can the Blu-Ice user move optics Motors?

	In-Hutch	Local Console	Remote Console
Local Scientist	NO	NO	NO
Roaming Scientist	NO	NO	NO
Local Staff	YES	YES	NO
Roaming Staff	YES	YES	YES

to the 'Optics Motors'.

3.5 Classifying the Robot Sample Mounting Operation

The robot is a device that the scientists may need interact with in order to perform their experiments. The device requires some safety precautions because it moves a fast robot arm with a wide range of motion. Scientists should probably be outside the hutch while the robot is mounting and dismounting samples.

However, staff members will need the capability to work with the robot within the hutch, and are familiar with the robot's range of motion and speed.

The device is given 'Outside Closed Hutch' permissions for 'scientists' and 'Inside Open Hutch' permissions for 'staff' as shown in Table 9

Table 10 shows the capabilities that a user has while issuing commands to the robot.

Please note that Blu-Ice software will only be able to add to the restrictions already placed on SSRL's robot by the hardware interlock system.

3.6 Classifying the Robot Calibration Operations

Calibrating the robot is a process that non-staff should not be allowed to attempt.

The operation does require some safety precautions, because it moves a

Table 9: Device permissions for sample mounting robot.

Permission	Scientist	Staff
Outside Closed Hutch	YES	YES
Inside Open Hutch	NO	YES
Outside Open Hutch Local	NO	NO
Outside Open Hutch Remote	NO	NO
Passively Accessible.	NO	NO

Table 10: Can the Blu-Ice user perform sample mounting operations?

	In-Hutch	Local Console	Remote Console
Local Scientist	NO	YES (If hutch door is closed)	NO
Roaming Scientist	NO	YES (If hutch door is closed)	YES (If hutch door is closed)
Local Staff	YES	YES (If hutch door is closed)	NO
Roaming Staff	YES	YES (If hutch door is closed)	YES (If hutch door closed)

fast robot arm with a wide range of motion. Therefore, it would be unwise to attempt this operation from a remote location if the hutch door is open.

However, staff members will need the capability to work with the robot within the hutch, and are familiar with the robot's range of motion and speed.

The device is given 'Inside Open Hutch' permissions for 'staff' and no permissions for 'scientists' as shown in Table 11.

Table 12 shows the capabilities that a user has while issuing commands to the robot.

3.7 Classifying Preset Camera Positions

A camera with pan/tilt/zoom is placed within the hutch. The camera provides the capability to move to preset positions. It does not have the capability of moving to a position that would provide a view to something that is restricted (e.g. keyboard or monitor). The camera itself is small and unable to hurt anyone during its movement. Requesting a move of the camera would not affect other users of the system or interrupt data collection.

In Blu-Ice the pan/tilt/zoom motors are configured with a 'Passively Accessible' permission for both Staff and Scientists as shown in Table 13.

Table 11: Device Permissions for calibrating the robot.

Permission	Scientist	Staff
Outside Closed Hutch	NO	YES
Inside Open Hutch	NO	YES
Outside Open Hutch Local	NO	NO
Outside Open Hutch Remote	NO	NO
Passively Accessible.	NO	NO

Table 12: Can the Blu-Ice user calibrate the robot?

	In-Hutch	Local Console	Remote Console
Local Scientist	NO	NO	NO
Roaming Scientist	NO	NO	NO
Local Staff	YES	YES (If hutch door closed, otherwise NO)	NO
Roaming Staff	YES	YES (If hutch door closed, otherwise NO)	YES (If hutch door closed, otherwise NO)

Table 14 shows the capabilities that a user has while issuing commands to this unrestricted device.

3.8 Classifying preset camera positions for staff camera

A camera with pan/tilt/zoom is placed outside the hutch. It has the capability of moving to a position that would provide a view to keyboards and monitors.

Requesting a move of the camera would not affect other users of the system or interrupt data collection.

In Blu-Ice the devices allowing camera movement are configured with 'Staff' permissions set at the 'Passively Accessible' level as shown in Table 15. No permissions are enabled for the 'scientists'. Table 16 shows the capabilities that a user has while issuing commands to this device.

3.9 Configuring Devices

Configuring a device is treated as a special interaction. Regardless of the category of the device, the User must be 'Staff' and the client must be the 'Active Client' to attempt the configuration.

Table 13: Device permissions for camera.

Permission	Scientist	Staff
Outside Closed Hutch	YES	YES
Inside Open Hutch	YES	YES
Outside Open Hutch Local	YES	YES
Outside Open Hutch Remote	YES	YES
Passively Accessible.	YES	YES

Table 14: Can a Blu-Ice user interact with the camera?

User Type	In-Hutch	Local Console	Remote Console
Local Scientist	YES	YES	YES (doesn't need to become the 'Active Client')
Roaming Scientist	YES	YES	YES
Local Staff	YES	YES	YES (doesn't need to become the 'Active Client')
Roaming Staff	YES	YES	YES

Table 15: Device permissions for staff camera.

Permission	Scientist	Staff
Outside Closed Hutch	NO	YES
Inside Open Hutch	NO	YES
Outside Open Hutch Local	NO	YES
Outside Open Hutch Remote	NO	YES
Passively Accessible.	NO	YES

Table 16: Can a Blu-Ice user interact with the staff camera?

	In-Hutch	Local Console	Remote Console
Local Scientist	NO	NO	NO
Roaming Scientist	NO	NO	NO
Local Staff	YES	YES	YES (doesn't need to become the 'Active Client')
Roaming Staff	YES	YES	YES

Table 17: Can the Blu-Ice user configure a device?

User Type	In-Hutch	Local Console	Remote Console
Local Scientist	NO	NO	NO
Roaming Scientist	NO	NO	NO
Local Staff	YES	YES	NO
Roaming Staff	YES	YES	YES

Table 17 shows the capabilities that a user has while trying to configure a device.

3.10 Allowing 'non-staff' to calibrate motors

For motors that are determined to be safe to calibrate, such as 'gonio_phi', a scripted operation could be written and given the 'Inside Open Hutch' permission for 'scientists'. This operation could set the motor position (for gonio_phi only) on behalf of the user, thus bypassing the restrictions on configuring a motor. This will allow the experimenter to calibrate the motor, while protecting them from accidentally changing other important parameters, like the motor's scale factor settings.

3.11 Forcing 'non-staff' to use a scripted device

Scripted devices are motors that are a combination of motors whose relationship is defined by a script. It may be desirable to block a 'child' motor of a scripted device and only allow non-staff to work with the highest level parent script. This is possible by giving all of the children motors permissions for 'staff' only, while giving permissions for 'scientists' to the parent motor.

4 Document Version Information

Initial Release