

*If you are using a printed copy of this procedure, and not the on-screen version, then you **MUST** make sure the dates at the bottom of the printed copy and the on-screen version match. The on-screen version of the Collider-Accelerator Department Procedure is the Official Version. Hard copies of all signed, official, C-A Operating Procedures are available by contacting the **ESSHQ Procedures Coordinator, Bldg. 911A***

C-A OPERATIONS PROCEDURES MANUAL

4.91 Configuration Management Plan for the C-A Access Controls System

Text Pages 2 through 8

Hand Processed Changes

<u>HPC No.</u>	<u>Date</u>	<u>Page Nos.</u>	<u>Initials</u>
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Approved: \_\_\_\_\_ *Signature on File* \_\_\_\_\_  
 Collider-Accelerator Department Chairman Date

A. Etkin, D. Passarello, J. Reich

## 4.91 Configuration Management Plan for the C-A Access Controls System

### 1. Purpose

This document describes the method by which the configuration of the C-A Access Controls System (ACS) hardware (which includes chipmunks, gates and locks), software, and documentation will be managed. The C-A Access Control System includes the AGS relay based system and the Particle Accelerator Safety System (PASS). These requirements supplement BNL's Standards Based Management System (SBMS) Engineering Design Subject Area, [C-A OPM 13.6.1, Preparation & Issuance of Engineering Documentation](#), and [C-A OPM 13.6.2, Configuration Management](#).

### 2. Responsibilities

- 2.1 The C-A Access Control Group (ACG) Leader is responsible for ensuring that all proposed ACS changes, including any modification of chipmunks and ACS hardware and software, are processed in accordance with this document, and the C-A Configuration Management program, [C-A OPM 13.6.2](#).
- 2.2 The Radiation Safety Committee (RSC), via the Access Control Physicists, is responsible for the review of all changes/modifications to ACS documentation, e.g. drawings, specifications, test procedures, in accordance with the Committee charge in [C-A OPM 1.10](#), Attachment 8.1.
- 2.3 Accelerator Systems Safety Review Committee (ASSRC), via the Access Controls Physicist, is responsible for the review of any design changes that affect the Oxygen Deficiency Hazard (ODH) monitoring or emergency ventilation system operation.

### 3. Prerequisites

All temporary changes shall be processed in accordance with [C-A-OPM 4.92, Control of Temporary Hardware Changes/Bypasses in the Particle Accelerator Safety System \(PASS\) and the Access Control System \(ACS\)](#).

### 4. Precautions

None

### 5. Procedure

- 5.1 The C-A Access Control Group (ACG) shall initiate drawings, specifications, test procedures, and other design documents, to present a verifiable engineering description of ACS (including chipmunks). These drawings/documents shall conform to appropriate C-A design and document control requirements.

## 5.2 Change Control Process

5.2.1 Proposed changes to ACS test procedures shall be documented and processed in accordance with [C-A OPM 1.4.3](#), Procedure for Implementing New, Revised, or Canceled, Permanent Procedures.

5.2.2 All proposed changes to ACS drawings and specifications shall be documented on the C-A Engineering Change Notice (ECN) form. The cognizant engineer shall review all proposed changes prior to submission of the ECN. Processing of the ECN shall be in accordance with the C-A Configuration Management Program, [C-A OPM 13.6.2](#), and the requirements listed below:

### 5.2.2.1 Review of Changes

**Note:**

The Access Control Physicists shall be informed of all changes to software and hardware (including chipmunks, gates and locks), which do not require an ECN, e.g. parameter changes, component substitution, and replacement.

- At the discretion of the Access Control Physicists, the ASSRC shall be consulted for modifications that affect the design/operation of ODH monitoring, or emergency ventilation system.
- The review shall determine whether the proposed change(s) suggest retraining of the Main Control Room (MCR) Operations staff, and/or other personnel, and determine any impacts to operation procedures.
- After the PLC(s) software modification(s) have been approved, the Access Control Physicists will apply a graded approach when determining the amount of safety function re-certification testing required.

5.2.3 The following steps shall be followed by ACG Leader and Quality Representative when replacing released PLC Code with revised code

- 5.2.3.1 The C-A ACG Leader shall
- Ensure that discs are marked as specified in 5.5.3.
  - upon placing the primary copy of the PLC code in the safe, initial/date the “ECN Incorporated By” line on the original ECN
  - update the safe logbook to reflect the addition of the revised PLC code

- forward the ECN with the secondary copy of the PLC code to the C-A QA Representative

#### 5.2.3.2 The C-A QA Representative

- upon placing the secondary copy of the PLC code in the safe, initial/date the “ECN Incorporated By” line on the ECN
- update the safe logbook to reflect the addition of the revised PLC code
- forward the original ECN to the C-A Documentation Control Group

5.2.3 A description of the change shall be put into the ACS Engineering Change Logbook.

5.2.4 If an approved change affects the current system test procedures, as determined by the C-A ACG Leader, the test procedure shall be revised in accordance with the [C-A OPM 1.4](#). Access Control Physicists review and concurrence is required on all revised test procedures.

### 5.3 Functional Test of Changes to the System

5.3.1 Prior to routine use of modified code; test procedures that adequately describes the functional test of any hardware (including chipmunks), or software modification shall be submitted for review to the Access Control Physicists, by the C-A ACG Leader. These test procedures shall facilitate the recording of test results and provide objective evidence of test result review. The Maintenance Panel View Display (PVD) is exempt unless it contains command code.

- At the discretion of the Access Control Physicists, specific test results may be recorded in the ACG System Work-In-Progress Logbook. All test results which are recorded in the ACG System Work-In-Progress Logbook shall be reviewed by the ACG Leader and Access Control Physicists.

5.3.2 If during functional testing, a mechanical repair, which is a replacement by an identical device/component, must be made that would not require changes to the released drawings, specifications, test procedures, or other design documents, the functional testing shall proceed. A record of the repair shall be maintained by the ACG Leader. The Access Control Physicists shall be informed of the repair by the C-A ACG Leader, and a determination on whether supplemental testing is necessary shall be made by them.

## 5.4 Hardware Securities and Labeling

- 5.4.1 All ACS enclosures shall be secured with the same lock/key combination. Copies of the enclosure key shall be sequentially numbered. A set of maintenance keys shall be kept in the ACG Leader office. The ACG Leader may issue keys to personnel who are authorized to access the ACS enclosures.
- 5.4.2 All the keys and spares for the locks that secure the ACS hardware enclosures shall be accounted for. The spare keys shall be kept by the ACG Leader in the lockbox.

**Caution:**

Spare CA keys cannot be issued without consultation with the RSC Chair, or designee, or C-A ESSHQ Management. Unauthorized use of a spare key could result in a grave danger to the user and will prompt disciplinary action.

- 5.4.3 Except for the operational CA, Sweep and S keys in the key tree in the Main Control Room, and the maintenance keys kept in the safe, the spare CA and S keys, shall be kept by the Access Control Physicist in a lockbox.
- 5.4.4 The enclosures, critical devices, wiring, interlocked chipmunks, etc., shall be appropriately labeled with Orange Tags so as to identify them as part of ACS.
- 5.4.5 Any operational software or hardware (including chipmunks), found to deviate from the approved design basis, shall be recorded in the ACS Trouble Logbook and be reported within 24 hours, to the RSC Chairman, or designee, the C-A ACG Leader, and ESSHQ Associate Chair. The deviation shall be evaluated by the Facility Manager for DOE reportability, as appropriate.

**Caution:**

If a deviation from the approved design is present, then unsafe operation of the system may occur. RS LOTO of the area per [C-A-OPM 9.1.16](#) shall be required until a review is conducted by the RSC.

- 5.4.6 During accelerator operations, the Operations Coordinator may give permission for the C-A ACG Leader, or designee, to unlock equipment racks, or the 911B security area containing PLC devices, for the limited purpose of inspection. Access shall be limited to only one PLC Division cabinet at a time. During cryogenic only operation, the C-A ESH Coordinator, Associate Chair for ESSHQ, or designee, shall give

permission to access the aforementioned enclosures for the purpose of inspection. During times of non-operation, access may be supervised by the C-A ACG Leader.

- 5.4.7 The safe in the office of the C-A ACG Leader, contains a set of Sweep and CA keys, whose purpose is to facilitate PASS system test procedure execution. During accelerator shutdown, after confirmation of appropriate RS LOTO, or during maintenance periods, after confirmation by the duty Operations Coordinator of RS LOTO, the C-A ACG Leader may remove these keys for the duration of active testing. During cryogenic only operations, when testing is expected to take place within RHIC cryogenic areas, the approval of the C-A ESH Coordinator, or Associate Chair for ESSHQ, or designee, is also required. When any key is removed/returned to the safe, it shall be logged in the Safe Logbook. This logbook shall be provided by the C-A ACG Leader.

## 5.5 Control of Documentation and Software

- 5.5.1 Upon authorized release by the C-A ACG Leader, the PLC source code, and relevant documentation, shall be maintained per the requirements of this document. A Release History Log shall be maintained by the C-A ACG Leader.
- 5.5.2 The original development software and PLC source code, shall be maintained by the C-A ACG Leader. All manufacturer supplied development software disks shall be stored in the fire retardant safe in the office of the C-A ACG Leader.
- 5.5.3 A primary and secondary copy of the PLC source code shall be maintained. The primary and secondary disks shall be write-protected and conspicuously marked with file name, date, revision number, and check sum. The location of the primary and secondary copies are as follows: 1) The primary copy shall be secured in a fire retardant safe in the office of the C-A ACG Leader, 2) The secondary copy shall be secured in a fire retardant safe in the C-A Quality Assurance Office.

The C-A ACG Leader and the Quality Assurance Representative shall not permit the disks to be removed from either safe without permission of the RSC Chairman, or designee, or the C-A Department Chairman, or designee. When system software disks are removed/returned to either safe, it shall be logged in the safe logbook.

- 5.5.4 Control of released drawings and the State Tables shall be maintained by the C-A Design Room, with copies made available in TIFF format.

## 5.6 Control of Special PASS Test Equipment

Except for standard tools, voltmeters, etc., any dedicated devices which could degrade functionality that are needed for system testing; i.e., special jumper/clips, mechanical door switch bypasses, etc., shall be:

- Predefined in the respective test procedure.
- Kept in the C-A ACG Leader's safe.
- Verified they are back in the safe via a signature on the appropriate test procedure by the C-A ACG Leader or designee.

## 5.7 An ACS System Trouble Logbook shall be maintained to track problems discovered during the test and operational phases of ACS.

5.7.1 Problems found during testing of ACS shall be tracked by entering them in the Logbook. Marginal or compilation notes made in the Test Procedure sheets for problems that require correction shall be transcribed into the Logbook.

5.7.2 Problems found during ACS operation shall be immediately reported as required in 5.4.5. Problems shall also be entered in the Logbook.

**Caution:**

If a deviation from the approved design is present, unsafe operation of the system may occur. RS LOTO of the area per [C-A OPM 9.1.16](#) may be required until a review is conducted by the RSC.

5.7.3 Each entry in the Logbook shall be assigned a unique tracking number.

5.7.4 For facilitation of tracking and auditing, the first page(s) of the Logbook shall consist of an index which lists all problems by tracking number and their current dispositions.

5.7.5 Only one copy of the Logbook shall exist, and it shall be in the custody of the C-A ACG Leader. It shall be his responsibility to keep the Logbook current, and to ensure that all pertinent entries are made, tracked and corrected.

**6. Documentation**

- 6.1 ACS Engineering Change Logbook
- 6.2 Baselined Schematics, State Tables and Ladder Diagrams
- 6.3 ACS System Release History Logbook
- 6.4 ACS System Work in Process Logbook
- 6.5 Safe Logbook
- 6.6 ACS System Trouble Logbook

**7. References**

- 7.1 [SBMS, Engineering Design](#)
- 7.2 [C-A OPM 13.6.1, Preparation & Issuance of Engineering Documentation.](#)
- 7.3 [C-A OPM 13.6.2, Configuration Management.](#)
- 7.4 [C-A OPM 9.1.16 Lockout/Tagout for Radiation Safety.](#)
- 7.5 [C-A-OPM 4.92 Control of Temporary Hardware Changes/Bypasses in the Particle Accelerator Safety System \(PASS\) and the Access Control System \(ACS\).](#)
- 7.6 [ES&H Standard 1.5.3](#)

**8. Attachments**

None