ACIS Design Compliance with Principal Accelerator Safety Interlock Design Requirements

Martin Knott

December 2004

Table of Contents

---

1 Introduction

Prior to and during the design of the APS's Access Control Interlock System (ACIS), an effort was made to insure that the design complied with the relevant DOE and ANL requirements as well as those set forth in other recognized documents then in circulation. A paragraph-by-paragraph listing of the requirements (in some cases, recommended practices) and the corresponding ACIS design features was compiled for use by the review committees then in place. This tabulation was incorporated in the APS Safety Analysis Document (SAD) as Appendix A.

With the evolutionary changes that have occurred to the APS and to the documents referenced, some of the details of these compliances have evolved as well. It has been decided to maintain the SAD as a "living" document, editing it in close time proximity to the evolving APS. Since Appendix A depicted the ACIS's original design compliance to an also-evolving set of documents, it was decided to remove Appendix A but to retain it as a reference document. This LS Note now contains that set of original design compliances.

As the APS and the ACIS continue to evolve, the changes made will be subject to internal review and approval and will always be subject to the requirements set forth by the DOE and ANL.

2 Compliance with Accelerator Safety Interlock Design Requirements

2.1 Accelerator Safety Order 5480.25 Guidance for an Accelerator Safety Program, September 1, 1993

Section I.F.2.a: Choice of Relay-Based or Computer-Based System

(1): Considerations for computer-based systems:

The selection of a programmable-logic controller (PLC) computer-based system for the ACIS was based on numerous initial input/output requirements, the complexity of the logic (support for multiple operating modes, independent operation of the accelerators), testing/maintenance requirements, flexibility in changing the system's configuration, and overall reliability.

The linac/PAR, the synchrotron, and the storage ring must operate independently, allowing personnel to occupy an area while its neighbors have beam. For testing requirements, dedicated PLC systems are used in each area.

The ACIS will be controlled from the Main Control Room. A hard-wired system would require long control lines with inherent noise problems. PLCs are designed for distributed control in harsh control environments.

A rough comparison was made between relay-based and PLC-based control systems (available from J. Forrestal, ASD Controls). It was found that PLCs had a lower failure rate than mil-spec relays for "equivalent" control functions for systems having a few hundred relays.

(2).(a): Software and hardware validation and verification:

The software and hardware used in the ACIS is validated and verified by direct hardware test suites. Every aspect of the ACIS is tested by this mechanism. An example of the test suite for the linac can be found in document ASD/PROC/ACIS/LINAC-0008 (see DCC document 210603-00012). In addition to periodic testing, the running software is continually monitored by performing a checksum on the code in random access memory. This checksum is constantly monitored for validity and also displayed for operator verification.

(2).(b): Modularity:

The linac/PAR, synchrotron, and storage ring have their own independent ACIS. One or more systems may be isolated from its neighbors for maintenance or testing. Partitions between systems which provide radiological isolation are independently monitored by adjacent ACISs.

(2).(c): Redundancy:

Two electrically independent and redundant PLCs are used in each ACIS, called Chain A and Chain B. Each chain enables the operation of equipment in each area to accelerate or maintain beam. Critical devices such as beam shutdown stations, access door status switches, partition hardware, radiation monitors, etc., are interfaced to both chains through separate contacts.

Possible common-mode failures of the software are mitigated by designing each program differently to the same control specification. Ancillary functions (such as monitoring the tunnel search or displaying system status) is programmed in only one chain to force diversity.

(2).(d): Isolation and configuration control:

The ACISs are only used to provide radiation protection for personnel. Equipment and machine protection is furnished by other systems.

When operating, the paths to the program area of the PLCs are physically disabled by key-operated switches on the PLC processors. At the end of the certification process, the program's checksum is recorded and the program is stored on an on-board EE-PROM. At power-up, this program is automatically loaded into the processor's memory. The checksum is then manually checked to match the expected version before the ACIS is put into service. As the PLC executes its program, the checksum is automatically calculated. At the end of each calculation, the computed checksum is compared with the expected value. Any difference trips the ACIS.

Physical keys and software passwords are required to gain access to the processor's memory. Only authorized personnel are allowed to modify the program. Modifications require complete re-certification.

An APS ASD policy is in place defining configuration control procedures.

(2).(e): Staff qualifications:

Several members of the APS ASD Controls Group have extensive experience with PLCs. PLCs are used in other divisions of the Laboratory, and personnel are available on an as-needed basis for consultation.

Section I.F.2.b: Technical Design

(1): Fail-safe design:

All protective functions are designed for fail-safe operation. Safe conditions require energized circuits or active pressure. The ACISs are not "fault-tolerant," e.g. any detected fault removes permissives from the controlled equipment.

(2): Redundancy:

No single failure renders the ACIS unsafe. All critical devices are duplicated in each chain.

(3): Component protection:

Safety circuit wiring is in dedicated cable trays or conduit. When cables leave trays, they are protected in conduit. When ACIS cables share a common signal tray, they are physically separated from other cables. All ACIS equipment is in tamper-alarmed racks or enclosures.

(4): Critical devices:

The following table illustrates the ACIS philosophy of at least two critical devices being controlled redundantly by the system.

	Chain A	Chain B
Linac	Klystron 1 Modulator	Klystron 1 rf Drive
	Klystron 2 Modulator	Klystron 2 rf Drive
	Klystron 3 Modulator	Klystron 3 rf Drive
	Klystron 4 Modulator	Klystron 4 rf Drive
	Klystron 5 Modulator	Klystron 5 rf Drive
	DC Gun High Voltage	DC Gun Pulser
	RF Gun Kicker	
LEUTL	Beamline Pitch-up Magnet	Beamline Pitch-up Magnet
	Beamline Pitch-level Magnet	Beamline Pitch-level Magnet
	Beamline Beam Stop	Beamline Beam Stop
PAR	Quadrupole Magnets	Quadrupole Magnets
	Main Dipole Magnet	Main Dipole Magnet
	RF (both systems)	RF (both systems)
Synchrotron	Main Dipole Magnet	Main Dipole Magnet
	Quadrupole Magnets	Quadrupole Magnets
	Sextupole Magnets	Sextupole Magnets
	Correctors	Correctors
	RF	RF
Storage Ring Zone-F	Main Dipole Magnet	Main Dipole Magnet
	Quadrupole Magnets	Quadrupole Magnets
	Sextupole Magnets	Sextupole Magnets
	Correctors	Correctors
	RF (four systems)	RF (four systems)
Storage Ring Zones A-E	Quadrupole Magnets (by zone)	Quadrupole Magnets (by zone)
	Sextupole Magnets (by zone)	Sextupole Magnets (by zone)
	Correctors (by zone)	Correctors (by zone)
	Main Dipole Magnet (via Zone-F)	Main Dipole Magnet (via Zone-F)
	RF (via Zone-F)	RF (via Zone-F)

Each critical device feeds a status signal back to the ACIS indicating compliance with the trip directive.

(5): Shutdown mechanisms:

ASD procedures (e.g., "Linac/PAR ACIS Operational Procedures," ASD/PROC/ACIS/ LINAC-0001) specifically prohibit using the Beam Permit Select keyswitch for routine shutdown of equipment.

(6): Configuration control:

All ACIS components including relay racks, cable trays, conduits, interconnection boxes, beam shutdown stations, door release boxes, and output contactors are clearly labeled with bright yellow labels which clearly mark the device as being part of the ACIS and call for contacting the ACIS system manager for information about the device. All drawings containing ACIS functions are identified as such. The ASD policy on ACIS configuration and control is stated below.

"All pieces of equipment, devices and wiring which the Access Control and Interlock System (ACIS) uses to disable the production of radiation shall be considered an extension of the Accelerator Access Control and Interlock System. The devices to be covered by this policy include power interrupters, switches, etc., which will be used to disable RF modulators, Diplole [sic] supplies, E-guns, low level RF amplifiers etc. This equipment will be subject to the following rules:

"**1.0** The initial physical implementation of the safety circuit will require the approval of the Controls/Interlock group management, the Accelerator Operations management and the Accelerator Systems Division ESH representative as well as the management of the ASD group responsible for producing the device.

"**2.0** The safety circuit will be considered an extension of the ACIS; therefore, any change to the circuit will require the approval of the Controls/Interlock group management, the operations management and the Accelerator Systems Division Safety representative as well as the management of the ASD group responsible for producing the device.

"**3.0** All such devices, wiring, etc. shall be identified on the drawings for the controlled device with the following words:

> "This drawing contains Access Control and Interlock System Components. Any changes to this drawing must be approved by Controls/Interlock group management, the operations management and the Accelerator Systems Division ESH representative as well as the management of the ASD group responsible for producing the device.

"**4.0** Physical wiring, devices and components involved in the ACIS will be marked inside the equipment. Care will be taken to separate and protect interlock wiring and devices from possible tampering. All devices and wiring will be clearly distinguished from other devices and wiring by special signs, colors and protection devices.

"**5.0** Where equipment exists or is being constructed under contract the changes shall be retrofitted as soon as practicable."

When a software release of the ACIS has been tested and approved by ASD management, no further changes to the software are permitted. A password will be entered by the ASD Associate Division Director for Controls and Diagnostics into the source code and the PLC code at this point. Two identical diskettes for each PLC, chain A and chain B, containing the complete source code as generated by the commercial PLC design software and identified with a unique checksum number as generated by the PLC while running the tested and approved code will be placed under APS Document Control Center jurisdiction. The diskettes will be write-protected using the intrinsic diskette mechanism and further protected with the PLC password system. A complete set of ladder logic diagrams, input/output tables, wiring diagrams, and hardware configuration drawings will also be placed under APS Document Control Center jurisdiction.

If a new release of ACIS software is required for any reason, the following steps must be performed:

- An ACIS change request document will be generated specifying the changes along with the reasons for the changes.
- The ACIS oversight committee will review and approve the suggested modification.
- The ACIS systems manager will obtain a copy of the write-protected, controlled diskettes from the Document Control Center, load the software, and verify the checksum.
- The verified reference software will be copied to the PLC development system hard disk drive under its existing name and subsequently copied to a new project name using the commercial PLC software development tools.
- The changes will then be implemented on the new project software.
- The revised software will be compared to the reference software using the commercial PLC development software **compare** function.
- The change diagrams and revised test plan will be reviewed by the ACIS review committee. If the committee approves, the complete test procedure will be rerun.
- If the test procedure is successful, the software configuration management will be followed with the revised software.

(7): Modular design:

Components of the PLC systems and radiation monitors are of modular design for easy expansion and replacement. ACISs may be isolated for independent testing and maintenance (see I.F.2.a.(2).(b)).

(8): Testing:

Each ACIS may be shutdown for testing while adjacent ACISs are operational.

(9): Independent review:

Independent reviews of the technical design were held in November 1992 and June 1993. Fault analyses of system components and procedures are in progress. Reviews of the software and test procedures are performed before each ACIS becomes operational.

Section I.F.2.c: Personnel Exclusion Areas

(1): Emergency shut-off devices:

Beam shutdown stations (BSSs) are located in all tunnels. BSSs are spaced a maximum of 30 m apart and in blind areas.

(2): Emergency exit/entrance mechanisms:

All access doors are equipped with crash bars on the interior side which break the circuit to the magnetic lock. Likewise, emergency entrance buttons are located on the outside of the doors.

(3): Signs:

Signs are provided indicating entrances to exclusion areas. Displays are provided indicating the state of the ACIS at each access door. The BSSs also have indicators for ACIS status (SAFE, TEST, and SEARCH).

(4): Search procedures:

Exclusion area searches are incorporated into the ACISs. Search confirmation buttons must be pressed in a predetermined order which verifies the searcher's visit to every area of the tunnels. If tunnel security is violated in an already searched area, the search must begin again.

Audible and visual warnings are given before the ACIS transits to the Beam Permit Mode.

(5): Limited entry:

A Controlled Access Mode is provided which allows personnel into the tunnel without requiring a search before returning to Beam Permit Mode. Personnel in the tunnels while the ACIS is in the Controlled Access Mode are required to carry controlled access keys. These keys prevent the ACIS from entering Beam Permit Mode until they are all returned to their keybank.

Section I.F.2.d: Testing of Interlocks

(1): Periodic testing:

The performance of each ACIS will be verified before it is placed in operation and at a minimum of every six months thereafter, or whenever the configuration or software is

modified.

(2): Written test procedures:

Written test procedures, e.g., ASD/PROC/ACIS/LINAC-0008 (see DCC document 210603-00012), exist to ensure a complete functional test of the interlock system. A check sheet is provided with this document. This functional test exercises all system inputs and verifies response determines the integrity of each interlock chain, and tests the system "end to end."

At least once during the tests, equipment controlled by the ACIS will be disabled by tripping the system. End-to-end testing is incorporated into the test procedures, e.g., it will be verified that trips originating from the furthest point "down stream" shuts off the linac equipment.

All input and output devices will be individually tested. Redundant input devices will be independently tested, e.g., it will be demonstrated that each device can trip the ACIS if the second device is not exercised.

The integrity of redundant interlocks will be explicitly tested.

Feedback mechanisms will be in place to test the action of the critical components. For example, the status of the output relays which interface to the accelerator controlled equipment is fed back to the PLC. If a mis-state is detected (for example, a relay is on when it is told to be off) the ACIS trips.

(3): Modification and maintenance:

Replaced components will be tested to verify all parts of the ACIS which are dependent on those components work properly. Applicable sections of the test procedure will be re-checked.

Section I.F.2.e: Documentation

(1)-(5): Documentation:

Documentation will be maintained with audible records consisting of:

1. Each ACIS's functional requirements, description, software, and block and wiring diagrams.
2. Operating instructions.
3. Test procedures, test results, and maintenance logs.

Section I.F.2.f: Administrative Controls

(1)-(3): Administrative procedures:

APS administrative procedures will define:

1. Configuration controls for the physical and software aspects of the ACIS including

the change review process.

2. Authorized personnel responsible for the ACIS and the review process.
3. Special interlock bypass procedures if required.
4. Testing procedures, including lock-out of systems under test conditions.
5. Operating instructions.

2.2 SLAC 327 Health Physics Manual of Good Practices for Accelerator Facilities, 1988

Appendix B: Safety Interlock Report, Computers For Personnel Safety Systems:

RECOMMENDATIONS:

Pg. 91, para. 5: Selection of computer-based vs. hard-wired interlock system criteria, items 1 & 2:

Same criteria as in the Accelerator Safety Order, 5480.25, section I.F.2.a.(1).

Pg. 92: Hardware requirements:

1. Minimum hardware requirements:

The injector ACIS is constructed using well-proven industrial grade PLC components. The system is fully redundant with two completely independent interlock chains each of which de-energize the injector equipment independently. Independence is carried all the way from duplicate sensors to the devices which interrupt the radiation-producing devices. The ACIS is a completely dedicated system whose program resides in ROM as well as in RAM. The running software is continually monitored by performing a checksum on the code in RAM. This checksum is constantly monitored for validity and also displayed for operator verification. Watchdog timers are used to monitor program execution.

2. Dedicated systems:

The PLCs in the ACIS are dedicated to providing personnel safety interlocks. Status information is sent to the APS control system (EPICS), but EPICS has no control inputs to the ACIS.

3. Program storage:

The ACIS programs reside in battery backed-up RAM in the PLCs. The also reside in on-board EEPROMs. The EEPROM program is loaded into the PLCs RAM at power up.

The executive programs for the PLCs are stored on EEPROM.

4. Watchdog timers:

External watchdog timers are used on the PLC processor crates and all remote crates which interface to critical accelerator equipment. These timers must receive constant pulses from the PLCs. If a transition is not seen within a 4-s window, the watchdogs time out and drop power to the relays which enable the accelerator equipment. The watchdogs are monitored by each opposite chain, e.g. the watchdogs in Chain A are monitored by Chain B and vice versa. If a chain detects a failed watchdog, the interlocks for that chain also trip.

The PLCs also incorporate internal watchdogs. The first monitors the user's program. If the program fails to execute, this watchdog causes a processor fault which de-ener-

gizes all outputs. The time-out period for this watchdog is set by the user (default value is 500 ms). The second is a hardware check performed by the PLC every 10 ms to verify the validity of the data bus lines. A failure shuts down the processor and all outputs are de-energized.

Pg. 93: Software requirements:

1. Staff qualifications:

Same comment as for 5480.25 section I.F.2.a.(2).(e), Staff Qualifications.

Fault tolerant programming:

The ACIS programs are not "fault tolerant" in the classical sense. Any fault removes the enables from the controlled equipment.

Software hazard analysis:

The ACIS hardware and software will be independently reviewed before they are placed in service.

2. Configuration control:

Same comments as for 5480.25 section I.F.2.a.(2).(d), Isolation and Configuration Control.

3. Software common mode failures:

Different programs exist for each chain. Both chains monitor and control life safety devices. Chain A performs the additional tasks of monitoring tamper devices, displaying ACIS status, and supervising the search tour.

Pg. 94: Testing:

Same comments as for 5480.25 section I.F.2.d, Testing of Interlocks.

Operator override:

The control room consoles will have manual shutdown buttons which will remove primary power from the PLC processors.

Section 2.5: Interlocks And Warning Devices:

Pp. 21-22, para. 3 and 4, List of basic hardware equipment and administrative procedure requirements of an interlock system:

The ACIS has all listed equipment.

Pg. 22, para. 3, Interlock Design:

Component reliability:

Component reliability and system redundancy are prime drivers of the ACIS design. The system is fully redundant with two completely independent interlock chains each of which de-energize the injector equipment independently. Independence is carried all the way from duplicate sensors to the devices which interrupt the radiation-producing devices. Uninterruptible power supplies supply power to the system so that it is inde-

pendent of the AC power mains. All components used in the tunnel are insensitive to the levels of radiation which will reach their location.

Pg. 22, para. 4 and 5, Fail-safe design:

Same design criteria as in 5480.25 section I.F.2.b, Technical Design.

Pg. 23, para. 1, System type selection:

Redundant system has already been selected for the ACIS.

Pg. 23 para. 2, Cable protection:

ACIS cables are protected in cable trays and/or conduit. Radiation-resistant cables are used.

Pg. 24, para. 1, Equipment protection:

All PLC hardware is installed in tamper-alarmed racks. Beam shutdown station enclosures are tamper-alarmed.

Pg. 24 para. 2, Provision for testing:

Each ACIS may be individually brought off-line for testing. Self checking features are built into the PLC hardware and software. The use of jumpers is minimized. See also comments for 5480.25 section I.F.2.d: Testing of Interlocks.

Pg. 24 para. 3, Radiation monitors:

Neutron and gamma radiation monitors are provided around the linac/PAR, synchrotron, and storage ring. The balance of the storage ring has, at least, gamma detection near the ratchet wall doors. Each monitor independently interfaces to both interlock chains. The gamma detector has a "heartbeat" generated by background radiation. The neutron detector is supplied with a "heartbeat" source. Monitor failures are also monitored by the ACIS. Analog output signals are interfaced to the APS control system, EPICS.

Each monitor has local visual and audible alarms when radiation levels exceed preset levels.

The detectors will be calibrated before they are put into service and annually thereafter by ESH.

Pg. 24, para. 5 - 7, Pg. 25, para. 1 and 2, Features of an Interlock System:

See comments for 5480.25, section I.F.2.c: Personnel Exclusion Areas.

Pg. 25, para. 3, Search buttons:

Search buttons which must be hit in a predetermined order are provided on the beam shutdown stations in the tunnels.

Pg. 25, para. 4, Warnings:

Audible and visual warnings are provided and must be activated before beam is turned on.

Pg. 25, para. 5, Violations:

Any exclusion area violation resets the ACIS to its lowest state (Restricted Access) and

requires a complete search of the area before beam can be restarted.

Pg. 25, para. 6, pg. 26, para 1, Controlled entry:

See comments for 5480.25, I.F.2.c.(5): Personnel Exclusion Areas, Limited Entry.

Pg. 26, para. 2 - 4,

Not applicable or already covered by the ACIS hardware or procedures.

Pg. 27, para. 1, Safe entry conditions:

In the Controlled Access Mode, the door lock is under the control of the control room operator. The door can only be opened if the operator releases the lock. The operator must hold the release button all of the time the door is opened; if the door is detected open and the button is not being pressed, it is assumed that control of the tunnel is lost and a search is required.

Pg. 27, para. 2, Routine shutdown:

Procedures demand that the beam be turned off or partition devices be activated before the ACIS is brought out of the Beam Permit Mode.

Pg. 27, para. 3, Documentation:

See comments for 5480.25, I.F.2.e, Documentation.

Pg. 27, para. 4 and 5, Administrative procedures and configuration control:

See comments for 5480.25 section I.F.2.f, Administrative Controls.

Pg. 27, paras. 6 and 7:

See comments for 5480.25 section I.F.2.d: Testing of Interlocks.

2.3 NBS Handbook 107, ANSI N43.1 Radiological Safety in the Design and Operation of Particle Accelerators, 1979

Section 3.3: Safety Systems

3.3.1.4: Materials and Workmanship:

Cables installed in tunnels have radiation-resistant insulation. Tampers are provided on all enclosures housing critical equipment.

3.3.1.5: Redundant and fail-safe design:

See comments for 5480.25, sections I.F.2.a, Choice of Relay-Based or Computer-Based System and I.F.2.b, Technical Design.

3.3.1.6: Barriers:

All exclusion areas are enclosed in shielded tunnels. Areas are locked to prevent access.

Section 3.4: Accelerator Controls And Interlock Systems

3.4.1: Access to controls:

Keys are required to operate the ACIS.

3.4.2 thru 3.4.4:

See comments for 5480.25 section I.F.2.b, Technical Design.

3.4.5: System reset after trips:

If the ACIS trips, a search is required of the exclusion area before the system can be restarted. All trips are “latched” and must be reset by the ACIS manager or designee.

3.4.6: Exclusion area access:

All access doors to the exclusion area are equipped with access controls.

3.4.7: Scram switches:

See comments for 5480.25 section I.F.2.c, Personnel Exclusion Areas.

Section 3.5: Warning Devices

3.5.1: Warning devices at entrances to exclusion areas:

Indicators are used to display ACIS status at the entrances to the exclusion areas. Red strobe lights, located immediately inside the access doors (visible through a window), are on whenever the ACIS is in the Beam Permit Mode.

3.5.2: Temporary barriers:

Not used with the ACIS.

3.5.3: Audible and visual warnings:

See comments for 5480.25 section I.F.2.c, Personnel Exclusion Areas.

3.5.4: Radiation monitors:

Neutron and gamma radiation monitors are provided around the linac/PAR, synchrotron, and storage ring. The balance of the storage ring has, at least, gamma detection near the ratchet wall doors. Each monitor independently interfaces to both interlock chains. The gamma detector has a "heartbeat" generated by background radiation. The neutron detector is supplied with a "heartbeat" source. Monitor failures are also monitored by the ACIS. Analog output signals are interfaced to the APS control system, EPICS.

Each monitor has local visual and audible alarms when radiation levels exceed preset levels. The monitors and detectors will be calibrated before they are put into service and annually thereafter by ESH.

Section 3.6: Reliability Tests

See comments for 5480.25 sections I.F.2.d, Testing of Interlocks and I.F.2.e, Documentation.

2.4 Argonne ES&H Manual, Radiological Control Procedure, Chapter 5-16 Radiation Safety Interlock Systems

INDEPENDENT SAFETY REVIEW OF INTERLOCK SYSTEMS:

Pg. 4, para. 3-4, Drawings of new interlock systems...

> ACIS drawings are currently reviewed at the Group and Associate Division Director level before construction begins. All drawings are required to be under document control prior to the operation of any ACIS-controlled system. The ASD Radiation Safety Policy Committee (chaired by the ASD Division Director) must approve all revisions to any ACIS functionality, including the affected drawings. ESH membership will be offered on this committee.
>
> The ASD Radiation Safety Policy Committee (chaired by the ASD Division Director) must approve all revisions to any ACIS functionality. This committee membership does not include as members those responsible for system designs or modifications. ESH membership will be offered on this committee.

Pg. 4, para. 5, Interlock systems must be documented....

> All ACIS systems are required to have a complete set of approved and document-controlled drawings, written and approved functional descriptions, and written, approved, and document-controlled test procedures prior to validations and use.

DESIGN REQUIREMENTS:

Pg. 4, para. 6, The decision as to....

> All APS in-tunnel areas are considered to be in the Table 1 category of >100 rem MCI-I. All of the requirements listed in Table 1 for this category are incorporated in the APS shielding and ACIS designs. Independent design review committees (all non-APS) are used to review and approve the interlock systems.

Pg. 4, para. 7, Emergency shut-off devices....

> Such devices are provided which are clearly visible, unambiguously labeled, and readily accessible.

Pg. 4, para. 8, Because of the ....

> All ACIS components of of the highest quality and workmanship. The designs are as failure proof (or, at least fail-safe) as possible. Most components are contained in locked and tamper-monitored enclosures which will cause system trips if opened.

Pg. 4, para. 9, Fail-safe designs...

> Fail-safe analysis is part of all system design and component choice decisions during the ACIS design phase. Redundant devices for critical functions and redundant equipment shutdown methods are used throughout.

Pg. 4, para. 10, Maximum reliance....

Maximum reliance is made on bulk shielding. All doors are both locked and redundantly interlocked. Radiation monitors are tied to beam-shutdown actions, but not to protect against serious, in-tunnel exposure. No electronic surveillance systems are used.

HARDWARE REQUIREMENTS (if interlocks are required):

Pg. 5, para. 1, Computer-based systems....

Cross-chain checking is done at two levels: Final trip decisions are communicated to enhance the chances of shutdown success, since both chains are independently capable of the shutdown action. Watchdog timers triggered by each chain's continuous functions are checked by the redundant chain and a trip produced in response to a detected failure.

Pg. 5, para. 2, Safety system components....

All ACIS components, ACIS-dedicated cable trays, and ACIS cables in other trays are labeled. All cabling is contained in ACIS-dedicated cable trays or conduits, or when routed elsewhere, are given an added protective covering and labels.

Pg. 5, para. 3, Interlocks shall be....

In accordance with DOE Order recommendations, all relevant procedures prohibit use of the ACIS for routine shutoff of controlled equipment. Only emergency situations are exempted from these prohibitions.

Pg. 6, para. 1, There must be two redundant methods....

The ACIS design includes three redundant methods to monitor all personnel access maze doors, two implemented with PLC logic and a third consisting of a simple hard-wired chain. Entry systems employing heavy moving shield masses are mechanically locked and employ two of the redundant chains. All switches are mounted on the "safe side" of the door or require removal of a steel shroud for access. All redundant methods are able to force the particular accelerator facility into a safe condition.

Pg. 6, para. 2-3, If a key interlock tree is used....

Any key of the APS Controlled Access Key banks (APS terminology for a key tree) will, if removed, will place the related facility into a safe condition, and will prevent it from restarting. All ACIS keys are controlled as to procurement, maintenance, and custodianship (which is outside of the ANL locksmith office).

Accidental grounding will short the related power supply and cause all controlled equipment to be disabled (tripped). The introduction of outside electronic signals depends on the nature and placement of the signals, but of the many scenarios studied, all resulted in safe failures. For example, multiple signal introductions are required to influence all but the final components located within the controlled equipment.

Pg. 6, para. 4-5, In those areas where....

The ASD practice is to employ at least two primary devices to prevent beam transmission or generation. Status monitoring is used on all primary and failure mode devices.

In most cases, two or more failure mode devices are employed to prevent the generation of radiation.

The enclosure interlock status (actually the ACIS mode) is displayed at each maze door entrance. Entry systems employing heavy moving shield masses do not have such displays, but are mechanically locked and are not used for routine or remote-controlled access.

Pg. 6, para. 6, When an interlock....

All trip conditions require resetting to occur at the position where the trip originated, whether by requiring a re-search/secure process, or the resetting of a mechanical or electrical device.

Pg. 6, para. 7, A scram switch, pull-chain, or....

The Beam Shutdown Stations (BSSs) employ a clearly visible and unambiguously labeled mushroom button which will disable all ACIS-controlled equipment. The maximum distance to the nearest BSS is 15 meters and audible warnings are issued for one minute. The mushroom button must be manually reset and restarting of the accelerator system always requires a thorough search/secure of the entire area containing the BSS.

Pg. 6, para. 8, If beam-off controlled access....

Beam-off access is the only access mode supported at the APS. All access doors provide interlock-based tripping of any radiation-producing systems. The key tree has an identical affect on all radiation-producing systems.

Pg. 7, para. 1, There shall be hardware to require....

The ACIS-controlled search/secure operation forces the search to proceed in a fixed sequence and forces visits to all areas of the tunnel. Out-of-order sequences will abort the process, and maximum search time limits are imposed to insure non-interference with the process.

Pg. 7, para. 2, An announcement or other....

An audible warning is issued prior to all transitions from access condition to beam-on operation and last for one minute. Any exit or shutdown button actuation will terminate the warning, display “SAFE” at all BSSs, and require a re-search/secure process. Consideration is being given to supplementing the audible warning devices with pre-recorded voice messages.

Pg. 7, para. 3-4, In order to minimize....

The four APS ACIS systems are nearly identical in mission, operation, and function. The first system, the Linac/PAR ACIS, predated ANL Radiological Control Procedure 5-16 and was the model from which the other three APS systems were modeled and upon which all subsequent improvements were made.

The Accelerator Systems Division of the APS has in place the ASD Radiation Safety Policy Committee, chaired by the division director. This committee is responsible for the ACIS functionality and any subsequent changes.

SOFTWARE REQUIREMENTS:

Pg. 7, para. 5, Verification and validation of software....

DOE Order 1330.1C, Attachment 1, paragraph 2i indicates that "Verification and validation procedures for both acquired and developed software" is an element of a software management methodology. The verification and validation of software during its development cycle requires that at each definable development phase, the output of that phase fulfills the requirements of the previous phase. The ACIS software development phases and their inter-phase verification processes are:

1. Development of a requirements document: This document is reviewed at the Group and Associate Division Director level for conformance to accepted accelerator operation and safety practices.
2. Development of a functional specification: This document is reviewed at the Group and Associate Division Director level to insure that it supports the requirements of the previous phase - the requirements document.
3. Design of supporting databases: As the hardware interfaces are developed, detailed information databases are developed to support the later ladder-logic development. All of the aspects of the functional specification are checked to insure that the database will fulfill the ACIS mission.
4. Development of the detailed ladder-logic: This is the actual software development stage and is done incrementally, with each definable section checked for proper operation with the interface hardware and proper utilization of the database. The actual ladder-logic functions are checked against the functional specifications where applicable.
5. Development of a validation test procedure: This procedure is developed, written, reviewed, and approved at the Group, Associate Director, and Division Director level. It is written to validate all aspects of the functional specification. After approval, this procedure is placed under document control and any modifications require re-approval.
6. Validation test: The validation test procedure is now executed to validate the final total system product, including all software, hardware components, and hard-wired portions.
7. Operation and maintenance: During the entire life cycle of the ACIS systems, all modifications, including improvements, require approval of the ASD Radiation Safety Policy Committee. Corresponding revisions of the validation test procedure are prepared, approved, and executed to re-validate the system. Any component changed, whether due to a failure or an improvement-based replacement, requires a partial execution of the validation test procedure. Any software or PLC firmware change requires a full execution of the current approved validation test procedure. In addition, according to DOE requirements, each ACIS system requires a re-validation at least once every six months.

Pg. 7, para. 6, Data logging of the....

Data logging of the radiation monitors is planned for the entire APS and is seen to be possible prior to the end of FY95. Data logging of the ACIS interlock system database and checking it against the critical required functionality is possible, and will be tested for feasibility during FY95.

Pg. 7, para. 7, Interlock software should be....

All four ACIS implementations have the same high-level functional requirements and, except for deliberate attempts to have variations between the redundant PLC chains, much of the ladder-logic is by necessity, similar.

ADDITIONAL HARDWARE CONTROLLED ACCESS AREAS:

Pg. 7, para. 8, The following list of additional hardware....

The APS has no provision for beam-on controlled access and so this section does not apply.

INTERLOCK KEY ACCOUNTABILITY:

Pg. 8, para. 1, Written procedures for....

There is an approved (at the division director level) and controlled procedure for the control of all ACIS keys.

Pg. 8, bullet 1, Keys that affect....

All ACIS keys, including operational, reset, and those of key trees, are under the exclusive control of the ACIS System Manager or designee. The ACIS key control procedure will be modified to require an annual inventory of all ACIS keys.

Pg. 8, bullet 2, If a safety system....

The existing ACIS key control procedure requires that all keys lost or damaged must have their keyswitch or keylock retired permanently from service. Alternately, the tumbler core may be removed and permanently retired, saving the mechanism.

Pg. 8, bullet 3, Extra keys must never....

Duplicate keys are not allowed to be employed - see above response.

Pg. 8, bullet 4, Keys and locks will be....

Most ACIS keys are made using an exclusive groove series, making them non-standard. Most ACIS keys are stamped “DUPLICATION PROHIBITED.” The possibility of having the remaining keys appropriately stamped will be investigated.

Pg. 8, bullet 5, The signature of the....

The existing ACIS key control procedure will be modified to require division director or designee approval for all interlock key and/or lock procurements. Procurement will be notified of this requirement.

Pg. 8, bullet 6, Access to keys....

Keys (beamline-related) to be stored in the Main Control Room will be locked and

access to them limited by ASD Operations Group procedures. This process is expected to be in place by April, 1995.

Pg. 8, bullet 7, A key that secures...

The only ACIS keys used to control access to a controlled area are the 70 ratchet door and five "super door" keys. It is impractical to utilize all of these keys in the ACIS control panel. These keys are to be locked in the Main Control Room and access limited by ASD Operations Group procedures. This process is expected to be in place by April, 1995. Consideration will be given in the future, if warranted, to interlocking these 75 keys to release a single operational key.

ENTRY REQUIREMENTS:

Pg. 9, para. 1, Radiation surveys are required....

Current APS procedure conforms to these requirements.

SEARCH AND SECURE:

Pg. 9, para. 2-3, Search and secure procedures....

Search and secure procedures are written, approved, and under document control for two of the four ACIS controlled areas. The remaining two procedures will be in place prior to commissioning activity in December, 1994.

There will be established by the ASD Operations Group such a procedure for testing the adequacy of the search procedures. This procedure will be auditable.

ACCESS TO AREAS WITH POWER ON BUT NO RADIATION PRODUCTION:

Pg. 9, para. 4, Written procedures for access....

According to the interpretation provided by the author of this document, this refers to access to an area for which all systems required for radiation production are powered up, but the beam is held off by some device. No such access is allowed to any APS controlled area.

ACCESS TO AREAS WHERE RADIATION IS BEING PRODUCED:

Pg. 10, para. 3, Written procedures for access....

No such access is allowed to any APS controlled area.

MAINTENANCE, REPAIR AND TESTING:

Pg. 10, para. 8, Any maintenance or repair work....

Current approved and controlled procedures require that all work on ACIS systems be performed by the ACIS System Manager, designee, or their direct-supervised staff. Currently, all maintenance and repair records are kept by the ACIS System Manager with copies to the ASD Division Director. These procedures will be amended to require

an auditable record of such repairs and maintenance.

Pg. 11, para. 1, Testing of the entire....

Current approved and controlled procedures require the DOE-required six-month re-validation cycle. There are no current plans to request a longer cycle.

JUMPERING:

Pg. 11, para. 2-5, Bypassing or jumpering of....

Any and all bypassing of ACIS interlocks require an application specific, approval and document-controlled procedure. All such procedures must be of an equal or improved safety level. If such a procedure will result in a lower level of safety, ESH-HP area office approval will be sought.

All ACIS bypass procedures include a pre-check of the affected functionality.

All ACIS bypass procedures include a post-check of the affected functionality.

All ACIS bypass jumpering actions are recorded in the APS Operations Group logbook, a permanent record. All special jumpering devices are keep within locked and tamper-protected racks, and access is restricted to the ACIS System Manager and designee.