SAFETY SYSTEM CRITICAL DEVICE
DO NOT TAMPER
CALL SAFETY PERSONNEL

SAFETY SYSTEM EQUIPMENT
FOR SAFETY PERSONNEL ONLY
PLEASE DO NOT TAMPER

SSG Contact Information: ssg_list@jlab.org or extensions 7024 or 7285
Attention: This component is under PSS configuration control. Contact the safety systems group before removal.
call:

PSS Configuration Control and You

PSS is Everywhere

PSS systems monitor the status of sensors like door switches, radiation monitors (CARMS), beam stoppers…etc. and make the decision as to whether it is safe to allow operation of accelerator equipment. If all signals are OK the PSS will "Permit" these devices run.

There are actually two parallel separate PSS systems, labeled System A and System B. Both monitor sensors and permits are required from both systems for accelerator operation. In order to perform this monitor/permit function thousands of PSS wires and fiber optic cables run throughout the accelerators and test facilities.

Do Not Tamper

ANY unauthorized access to PSS components or wiring, even with the best intentions, is considered tampering. In order to reduce the probability of an accident to below one in 1000 years [that's one in eight and a half million hours] the Safety Systems Group (SSG) must manage all sources of errors that could lead to a compromise in the ability of the PSS to perform the safety function. In practice it means managing configuration control over thousands of components, wires, software, and documentation.

Make no mistake; the major function of the PSS is to prevent people from being killed from hazards that arise as part of the accelerator operations. By circumventing the PSS configuration control, a person might directly contribute to the death or serious injury of a coworker.

What we don't know we can't fix

If a part of the PSS is damaged or even accessed in any way, a problem can inadvertently be introduced that could lead to harm of an individual or accelerator down time. For example, opening a PSS panel to look inside might lead to a critical wire short circuiting. ***The most important thing to us is that we know when PSS components or wiring has been accessed so that we can check to make sure everything is OK.***

In the design of the PSS we acknowledge that we cannot continuously monitor every piece of the PSS for failure. The system is designed so that most failures result in the system dropping to a safe state; this is termed "fail-safe". However, it is recognized that there are several classes of failure modes that are not detectable until you go looking for them. For example, the contacts on a door sensor might weld shut so that they never read the 'door open' position. This is an unsafe failure mode since the PSS believes that the door is always shut and it is therefore OK to run, even though it is not. A major part of the semi-annual certification process is dedicated to ensuring that all undetected failures are found and repaired. Note that the chance of one switch failing within the 6 month certification period is rare, but not improbable. It is the chance of two switches failing unsafe in the same place during the same 6 month interval that gets the chance of failure

of the system well below one in 1000 years – ***Assuming that the system has not been tampered with.***

Potential PSS Failure Sources

Several potential failure sources are given below. In order to maintain the integrity of the PSS all of these sources must be evaluated and controlled. Notice that component failure is only a small part of the overall picture. The Safety Systems Group must consider and manage all of the following potential error sources:

Operation and Maintenance Errors

- Specification Errors
- Implementation Errors
- Transcription/Documentation Errors
- Maintenance Errors
- Information Interpretation Errors (misread screen, incorrect icons, incorrect assumptions…)
- Operator Errors

External Energy Sources

- Impulse Energy Sources (lightning, high current arcs...)
- Electro-Magnetic Interference (lightning, welders, RF…)
- Mechanical Impact (Forklift, Crane…)
- Contamination (Water, chemical, radiation…)

Inadequate Configuration Control

- Change Errors
- Unauthorized Modifications
- Unauthorized Access to PSS Components (Conduit, Box Duct, Permit Signals,…)
- Configuration Errors (Jumpers, Pull-ups, …etc.)
- De-commissioning Errors

Component Failure

- Stress related failure
- Component wear out

But I own this!

Sometimes PSS components are mounted in other people's equipment. It is tempting, even considered sacred, that the equipment owner has the right to move, alter, or otherwise change PSS equipment within their domain. ***THIS IS NOT THE CASE!*** The Safety System Group owns not only PSS equipment but the entire safety function the PSS equipment is intended to perform. A crash switch is a piece of equipment. The Safety Function is that when the crash switch is pushed it will shut off all hazardous equipment controlled by the PSS.

SAFETY SYSTEM CRITICAL DEVICE DO NOT TAMPER CALL SAFETY PERSONNEL	**SAFETY SYSTEM EQUIPMENT** FOR SAFETY PERSONNEL ONLY PLEASE DO NOT TAMPER	SSG Contact Information: ssg_list@jlab.org or extensions 7024 or 7285 **Attention: This component is under PSS configuration control. Contact the safety systems group before removal.** call:

Places to be especially careful:

- Inside equipment that receives a Permit from the PSS.
- PSS equipment like crash switches and message displays mounted in control room consoles and racks.
- Beamline Elements that perform PSS functions like the CEBAF aperture A2.
- IOCs and CAMAC cards that are interfaced to PSS equipment like beam stopper controls and ODH monitor analog-to-digital converters.
- PSS Table Tray and Conduits
- PSS inter-building conduits (There are dedicated underground cableways for PSS signals.)

In 1995 and 2003 the United Kingdom Health and Safety Executive published a report that analyzes how some critical safety systems failed. Figure 1 gives a breakdown of the major causes. Note that Inadequate Change Control accounted for 17% of the incidents.

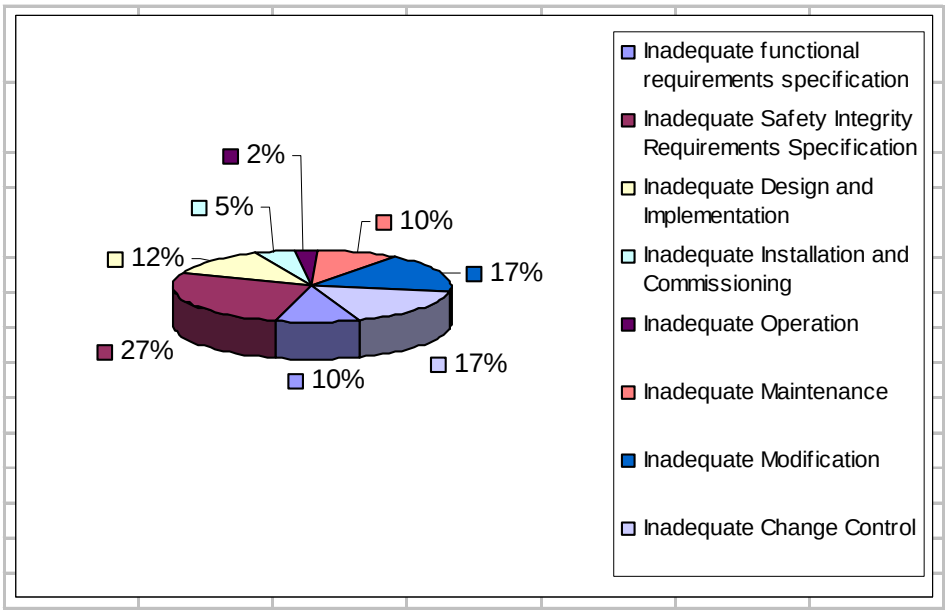

Figure 0 HSE Investigation of Safety System Accident Causes

What do the labels mean?

Safety System Critical Device – Do Not Tamper

These labels describe devices that are so critical to safety that if they are compromised, the loss of the device could lead directly to personnel exposure to lethal doses of radiation. Critical devices are so important that they are implemented in threes. For example, in each of the endstation beam lines there are two beam stoppers and PSS control of the arc magnets. Any one of the three devices can prevent beam from the BSY being transported to the endstations.

Safety System Equipment – Do Not Tamper

These are the default labels that identify all safety system components, wiring, and racks. Again, even opening a rack or cable way without permission is considered tampering.

Attention:…PSS Configuration Control

These labels identify equipment controlled by the PSS but not owned by the Safety System Group. They are there to ensure that the components are not inadvertently altered or removed. Again, the most important aspect of this is that the Safety Systems Group is aware that a component may be changed or removed. This is so that the safety function can be reevaluated and evaluated tested as necessary.

The Safety System Group does not "own" every safety device from end to end. For example, the PSS needs to control when the Gun can turn on but the safety systems group does not, and should not, design electron guns. The "attention" label identifies the critical components within a system that the PSS uses to shut down and monitor the status of the device. For example, within the RF High Power Amplifiers, there are special control relays dedicated to the PSS function. These relays are labeled with the "Attention" configuration control sticker.

The "Un-label"

Every square inch of PSS equipment cannot be covered with labels. Sometimes labels fall off or are affected by the weather. This in no way absolves responsibility for recognizing PSS equipment and ensuring that SSG personnel know If something has been affected by your work or people working around you. PSS interlocks are generally found in the following areas:

- CEBAF Accelerator – all areas including tunnels, service buildings, Counting House, and endstations.
- Free Electron Laser – all areas, including user labs
- Test Lab (Building 58)
    - Cryomodule Test Facility (CMTF) control room, test cave, mezzanine, 1 MW test stand, coupler test stand)
    - Vertical Test Area –test area, both control rooms, under floor
    - Injector Test Cave – control room, laser clean room, both sections of test cave

The list on the following page gives an idea of the types of devices interfaced to the PSS. The list is neither all inclusive nor exclusively uniquely all PSS devices. The intent is to familiarize you with the types of devices that are part of the PSS so that if you are not sure about a specific device you know enough to contact the Safety Systems Group before altering the equipment.

SAFETY SYSTEM CRITICAL DEVICE DO NOT TAMPER CALL SAFETY PERSONNEL	**SAFETY SYSTEM EQUIPMENT** FOR SAFETY PERSONNEL ONLY PLEASE DO NOT TAMPER	SSG Contact Information: ssg_list@jlab.org or extensions 7024 or 7285 **Attention: This component is under PSS configuration control. Contact the safety systems group before removal.** call:

Types of Equipment that are part of the PSS or interfaced to the PSS

- All entrances/Exits to and from a beam enclosure
- All software that runs on or communicates with a PSS device
- Any AC Power Circuit that powers a PSS component
- Beam Stoppers and Diffusers
- Blue (ODH) beacons
- CEBAF Injector Aperture A2
- CEBAF and FEL Public Address Systems
- Conduit, cable tray, and box duct containing PSS wiring
- Controlled Access Exchange Keys
- Controlled Area Radiation Monitor (CARM) Interfaces
- Crash Switches
- Door interlock Switches
- Electron Gun Laser Shutters (FEL and CEBAF)
- Gun, RF, and Magnet Box Power Supply interfaces
- IOCs named "IOCPSS…"
- Magenta (Radiation) beacons
- Magnetic Door Locks
- Movable Shielding (VTA)
- Permanently Installed ODH Monitors
- PSS Beam Current Monitors
- PSS Beam Kickers
- PSS computers including PCs and IOCs running PSS applications
- PSS controlled AC Power Outlets
- PSS equipment racks all equipment in them
- PSS fiber optic network systems including Modbus Plus, Remote I/O, and access room video.
- PSS Message Displays
- PSS warning horns and alarms (klaxons)
- Run/Safe Boxes
- Switches that are intended to shut off a radiation producing device
- Tunnel Equipment hatches
- Tunnel Gates and Doors, including detector hut doors and truck ramp roll-up doors
- Tunnel Lighting Contactors
- VTA RF Switchboxes

Bottom Line…Let us know

If you see that your work may affect PSS devices let us know. If you have accessed, damaged, or otherwise come in significant contact with a safety system device, do the same. If no one in the Safety Systems Group is available, let the on-duty Crew Chief know (x7050). We will check it out.