C-AD Access Controls Safety Instrumented Systems Group Retreat Presentation

Past
Present FY 09 run
and Future

Jonathan Reich
Group Leader

07/10/2009

Jonathan M. Reich

22 years at BNL C-AD

•BNL C-AD Access Controls/Safety Instrumented Systems Group leader and Cognizant engineer for all C-AD safety systems. 5 years

•C-AD Access Controls/Safety Instrumented Systems Group Project Engineer II. 5 years

•C-AD MCR Operations Coordinator – 6 years

•C-AD MCR Operator – 5 years

My BNL/C-AD Job responsibilities and authorities includes the following:

Maintain, develop, and operate C-A Dept. Personnel Safety Systems in support of the C-A scientific/technical program.

Direct the work of the Collider Accelerator Personnel Safety Systems Group comprised of Electrical/Electronic Engineers and Technical Specialists.

Plan, design, develop and use new or improved engineering techniques for the Personnel Safety Systems or equipment for the solution and completion of technical and research projects for the Accelerator Complex at the Collider Accelerator Dept.

Responsibilities:

……..

Identify potential hazards, environmental concerns, and unsafe conditions or practices in work or at work site, **and implement or suggest controls to minimize risk.**

Cease work activity, and/or issue a Stop Work Order upon observing imminent danger, and report the danger immediately to supervisor or ESH Coordinator.

……

Authorities:

Accelerator PSS Certification signature authority

C-AD Radiation Safety Pre-Beam Checklist signature authority for all C-AD enclosures

Act *to ensure safe and effective operations……..*

BNL/C-AD Safety Systems

BNL/C-AD safety systems share the following characteristics:

- They mitigate risks to the general worker within a controlled area. (Prompt Radiation hazard/ODH/Laser etc) We make it SAFE for you to enter beam enclosures. Without a Safety Instrumented System Severe Injury or Death is very likely.
- They are based on Electrical/Electronic/Programmable Electronic technology.
- They act to sense a dangerous condition.
- They automatically take action to alert personnel to the presence of a hazard, and in most cases act to mitigate the hazard.

Successes

- Gate issues have been diminished throughout the PASS
  (2 problems, strike switch adjustment required). All newly upgraded gates 4GE1,4GE2,6GE1, and 6GE2 have had zero failures where in the past they had chronic problems(alignment, dropping sweeps etc)

- IRIS Recognition/Smart Key Tree Training verification and access Systems worked extremely well with this run with little or no experimenter inconveniences. Very innovative and flexible system.

- Aside from 10+ hours from the 30-40 year old Relay system failures(reach backs/dirty contacts, bad relays) ACS/PASS failures have diminished significantly. Safety Systems Barley mentioned at time meetings for failure rates this run. Not in Top three or Top Ten failure hours by group this run. Safety Systems have been always been in top ten/three in previous runs.

- ERL PASS completed, very well documented, and working very well for Laser/ODH/and 50Kw Power Amplifier operation

Reasons for Successes

- Replaced some mechanical switches with magnetic type switches
- Replaced some Electric strikes with Electro-Magnetic locks
- Addressed and repaired grounding problems throughout PASS
- Initiative to repair hundreds of connections which were poorly terminated or making poor connections.
- + hundreds of other small repair jobs throughout the Safety Instrumented Systems Relays/PASS
- A very dedicated, hard working, willing, and enthusiastic Safety Systems Group working many long and off hours to provide SAFE and reliable Safety Instrumented Systems.

Access Key Panel
AC POWER

CAUTION
NO SMOKING
CAUTION

Failures

- One significant failure was a bad key tree micro switch. Took some time to find. Incorporated better recovery plan to keep Ops going.
- Relay problems are chronic due to end of life problems. Open coils, dirt contacts, bent contacts etc. Need to replace with more modern system ASAP.
- Poor equipment choices for environmental conditions still persist(E. Strikes, limit switches)
- Final element failures such as contactor failures(fail to read back as off due to age/mechanical wear and tear of 20-40year old components

20-Oct-08	Key tree at NSRL gate BGE1 would not acknowledge the capture of keys and would not release keys after a confirmed iris scan. This held up operations because the beam stops could not be opened.	Turned over to Iris Scanner Engineer.He reloaded software.	10h 49m
30-Oct-08	NSRL PASS system division A UPS tripped. Sweep was lost in all NSRL zones.	Removed and replaced UPS, operation was restored back to normal.	1h 0m
20-Jan-09	LTB beam stops closed. Though initially indicated as a Switchyard crash, it was found to be caused by the J15 beam shutter, which had closed and could not be opened.	While previously thought the B-line had been bypassed from the AGS security system, it was found upon the B-line losing power that this was not entirely correct. The B-line reached all the way back to the J15 beam shutter. After diagnosing how the B-line affected the AGS security system, some time was spent getting permission to modify the security logic. Permission was received, the work was performed, and the system was tested to be functioning correctly.	5h 31m
28-Feb-09	LINAC falls into a security interlock. cannot open beam stops...	W.Lamar replaced relay contact for LINAC beamstop readback, relay GK8 contact 5 & 6 in LINAC security panel.	2h 54m
28-Feb-09	LTB beam stops would not open on command	cleaned dirty contacts in logic strings for the Booster BeamStops.	1h 38m
4-Mar-09	480V contactor for UD1-2 hung. The supply is a critical device for the AtR line. The PASS PanelView reported the problem as an AGS Injection Problem rather than an AGS Extraction Problem. Time was wasted as personnel went off in the wrong direction to troubleshoot the problem	Upon extencive troubleshooting ,found 440ac contactor to be at fault.At the time we turned over job to Cas Group for further troubleshooting. The possible Display problem was notified to our Personnel Protection System Engineer.	1h 0m
11-Mar-09	TTB beam stops would not open on command.	Cleaned a dirty contact in TTB logic string	1h 0m
12-Mar-09	All Linac input is off on a reachback. Holding off BLIP and RHIC programs. beamstop_09 could not be opened even when commanded	W. Lamar reports that Access Controls removed and replaced a bad relay, relay GK6. Some time was also necessary to reset supplies and re-secure the Linac. Sweep was lost as a consequence of the repair.	3h 47m
12-Mar-09	B-Div is missing the "key-tree complete signal" in bldg 958. This signal is required by both A and B divisions in order to change modes. ACG replaced a bad micro-switch (switch #3) to the key-tree at NSRL. The R-line has been changed from Mode_9 to Mode_17 and then to Mode_18 where it resides	replaced a bad micro-switch (switch #3) to the key-tree at NSRL	3h 3m
25-Mar-09	LTB rchbk relay timing was found to be wrong. Dirty contacts may have caused or contributed to the TTB Issues.	The LTB and TTB Relay system were producing reach backs and beam stop failures repeatedly as time progressed through this Run. The problem became chronic. Maintenance time to remedy was requested over two Maintenance days and permission was not granted to do the work. Failure was declared and PPSG was allowed to perform maintenance on the various relay logic strings in BLDG 914 ACS enclosure and adjust the reachback time delay relay to its required value of 3 sec.	1h 32m
29-Mar-09	RHIC zones 9z1 and 10z1 had to be swept before resuming machine setup.[hence the one hour impact on the program]	Discovered "A" Div Gate switch out of tolerance. Removed and replaced switch at 10GE1.Took a look at 9Z1 zone found no problems there.	0h 21m
10-May-09	sweep lost in zone 9z1 at store (9EL1 in alcove C lost its reset)		1h 5m
10-May-09	Lost store due to permit being pulled by switch on escape ladder 9EL1. Upon investigation by W. Lamar, latch on the associated door was not fully engaged, so wind blowing the door was causing intermittent actuation of its failsafe switch. Door was firmly closed and switch sensitivity adjusted to prevent recurrence of this problem.		1h 51m
25-Jun-09	Jumpered chipmunk NM-224 was causing an A not equal to B failsafe interlock which prevented injection into RHIC.	The jumper was replaced by access controls personnel.	1h 25m
25-Jun-09	6b_ps1 pass division caused a permit link failure which adjourned RHIC injection.	A permit module card was replaced	1h 10m
8-Jul-09	U downstream had A=B Div error which could not be cleared from MCR. AC contactor failed to readback as off	Support cleaned and adjusted contactors for UD1 and UD2.	1h 41m
			39h 47 min
			Minus 4 h 37 min for non-Security System problem
			35 h 10m
			10h 51 m for dirty/faulty relays
			~ 25 hours significant time off for FY 09' run!

Inconveniences

- During one Maintenance Day Most all Card readers at C-AD had lost ability to accept valid cards. Suspect Lightning/electrical disturbance may have contributed to this failure. Need to add spike surge protection to Card Reader Network.

- During an attempt to load B Division Code to RHIC PASS, the Processor faulted due to compiler incompatibilities.(4 hours of ODH alarms sounding) (Need to check compiler compatibility before attempting to download and need to add EEPROMS for fast recovery in cases of processer faults etc.

Suggested Improvements and upcoming projects

- Replace and upgrade all Problematic gates ~ 15 more
- Replace LINAC, BOOSTER, AGS relay based safety systems with more modern safety PLC's which will provide better safety and reliability and a faster MTTR and much more efficient Re-Certification(Less time required) due to significantly better diagnostics.
- Replace all sensors and final elements with much more reliable and safety rated components(switches, contactors, etc)
- Devote dedicated resources(2 Techs, 1 Eng) to check and perform ECN on all required QA-A1 drawings(Hundreds) for errors, omissions. Big job. Known for many years, we must address this deficiency now.
- MCR Gate Video system upgrade to digital systems and large flat panel displays.
- NSRL OPLESS Access
- VTF, SBH
- Re-Certification streamlining
- Upgrade entire RHIC/U line PASS with Safety rated plc's and components(discreet/no monitored current loop circuits/no more human servos) ~ 2013???

Proactive Not Reactive Safety

Chris Soranno, Omron STI machine and process safety engineer, adds that machine safety is evolving from being historically reactive to being increasingly proactive. “Proactive safety looks at machines and processes before accidents happen, which is far less costly and makes it easier to identify causes,” he states. “In the past, proactive safety was viewed as something that slowed productivity. This isn’t true if you do proactive safety correctly. If you know how a machine or system should perform and you can compare this to how it’s performing in reality, then this directs you how to fix it, and you can reduce risk based on those performance requirements.”

Serious Concerns

C-AD is Currently using non-safety rated components chosen by Non Safety Group Personnel Engineers and Technicians over the years. Why not use better rated safer components (Sensors, logic solvers, and actuators? Current PSS's may not be able to achieve require risk reduction currently required due to design and component issues.

It is Suggested to utilize a Third Party Functional Risk and Safety Assessment to evaluate our current Risk Reduction requirements and Safety Systems and future requirements/corrections

Currently used components

LEBT Beam Stop switch - Honeywell BZ-2RW80-A2

From US NRC Equip. Failure Rate estimates

~ 3x10E-04 PFD demand

GE CR120A Relay used for disabling F6,DH2-3,LTB DH1 Power Supplies

Failure to energize 1x10E-04 PFD

Short across NO 1x10E-08 /hr

Failure NO contact to close 1x10E-07 /hr

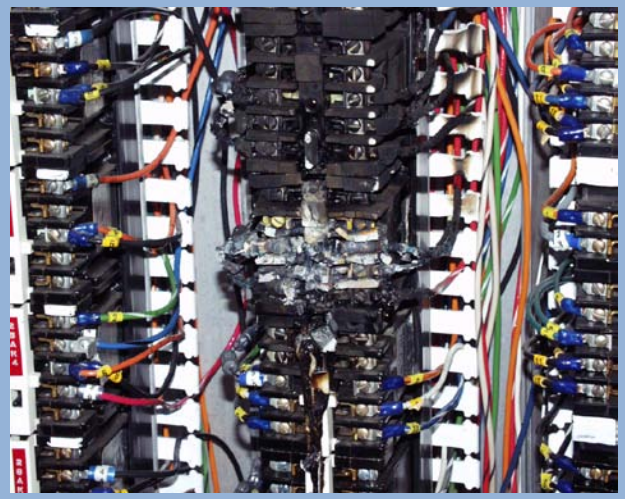
Suggested Components

Safety Ratings for AB Switches	
Standards	IEC 60947-5-3, IEC 61508, EN 954
Safety Classification	Cat. 4/SIL3
Functional Safety Data ¬	PFH_D: > 1.12 x 10^9 MTTFd: > 385 years

Safety Ratings for AB safety relays	
Standards	IEC/EN 60204-1, ISOTR 12100, EN 61508, ISO 13849-1
Safety Classification	Cat. 4 per EN 954-1 (ISO 13849-1), SIL CL3 per EN IEC 62061, PLe per ISO 13849-1
Functional Safety Data	PFH = 1.63E-09

Old and under-rated components have lead to unsafe, potentially unsafe, and spurious failures

Relay generated fires.



Component choices not adequate for environment.

Limit switches failed in closed position with ice preventing open condition sensing at 4GE1. Potentially very dangerous

BNL C-AD has had the good fortune of sound engineering practices and a little luck to avoid dangerous failures using existing Safety Systems.

There have been some unexpected behavior throughout the years though and old/under rated components have also contributed to problems. Some are systematic failures, others are environmental induced failures, and others are general spurious failures(loops etc)

The following failures or potential contributors to failure(only a small fraction of actual failures) have occurred over the years and are part of the public record in OC logs etc.

- Output module channel ON continuously without command-fan control, not detected remotely.
- Relays near end of reliable life 20-40years old.
- Most contactors used for critical device power control, >20years old.
- UD1-2 PS contactor failed to read back safe-40 year old contactor in use and re-built
- Many relay contacts failed to close or make contact.
- Relay coil failures
- Fire generated from Relay. Dangerous Failure.
- 4GE1 Gate Limit switches frozen with ice in closed position Door open not detected. Dangerous failure
- Slow response from GE relays for B15 IXFMR logic prevented LTB Beam stops from being disabled when transformer interlock tripped and 20degree PS off.
- Numerous spurious trips from all systems relay and PLC. Many due to sub-standard components. E. Strike switches, flimsy gates, inadequate waterproofing and specification requirements for out door Safety equipment, deteriorated and under-rated cables indoor and out.
- AGS North Gate: Local Gate locked status and access mode not clear to worker.
- Numerous Beam Stop Reach backs due to slow response times.
- Unclear/incomplete/inaccurate Electrical Drawings for Safety Systems
- Bare stranded wire discovered, used for connections resulted in A Division 24VDC PS supplying voltage to B Division Hardware-PLC DC inputs for chipmunk NMO224 Rad and FS interlock

We can do much better.

Performance-based standards and Functional Safety
A worldwide acceptable good practice

- **These standards address how to properly implement prescriptive-based interlocks and are widely accepted by hundreds of Governments/organizations/Labs/Manufacturers/ Businesses.**
  - ANSI / ISA 84.00.01-2004 – Application of Safety Instrumented Systems for the Process Industries
  - IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems
  - IEC 61511 - Functional safety: Safety Instrumented Systems for the process industry sector
- IEC 62061 is a machinery sector standard based on IEC 61508 (Functional safety of electrical/electronics/programmable electronic safety-systems)

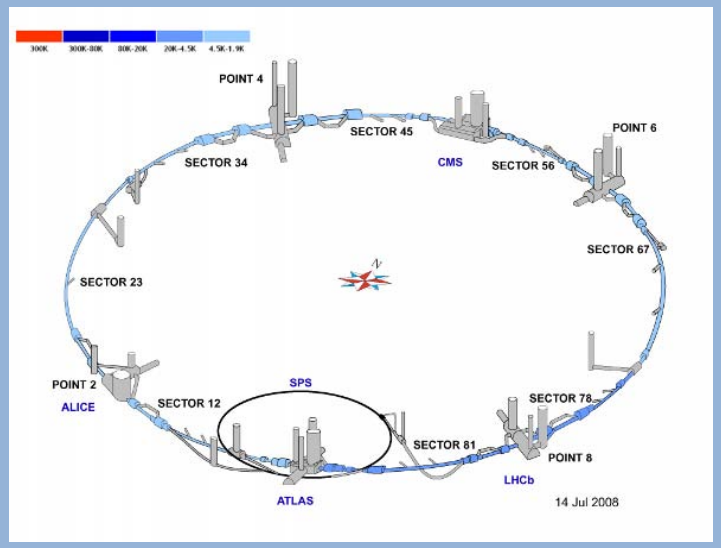
Changing Horizon and Outlook

- US Congress has mandated that U.S. Department of Labor (OSHA) and Nuclear Regulatory Commission (NRC) develop plans to assume responsibility for safety regulation of non-reactor DOE facilities.
- OSHA and NRC have strict regulations requiring use of “accepted good practice” methods.

These standards help to Quantify the Risk and Safety System Requirements to mitigate the calculated risk and consider the entire system through the Safety Lifecycle and provide very sound guidelines.

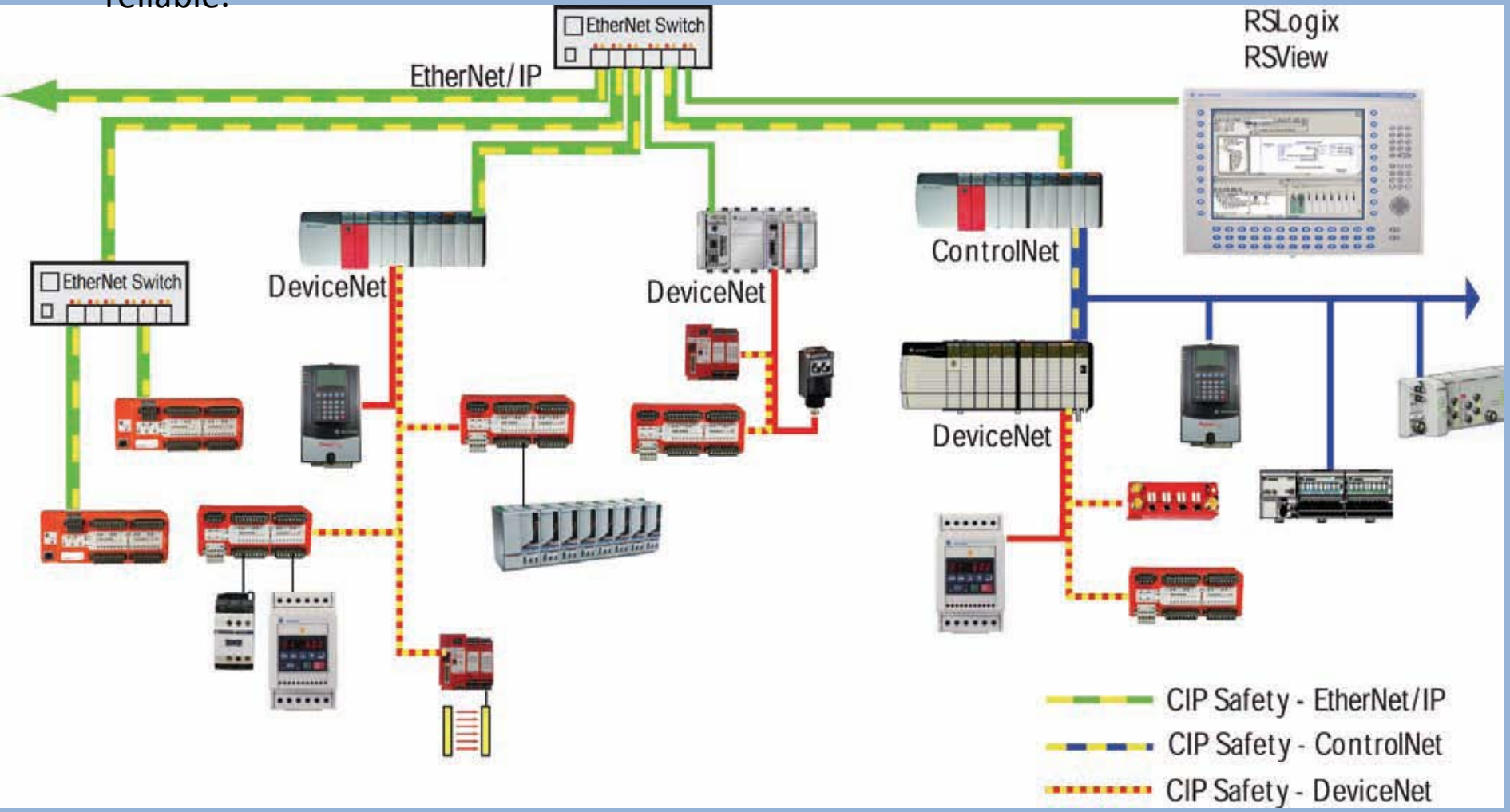
Other Accelerators using IEC and ISA Standards

Use ANSI 84.01, IEC61508, IEC61511 and other IEC standards for both personnel and equipment protection design basis.



- LHC
- Diamond
- JLAB

Future Systems will be modular and consistent in construction and certified **Quantitatively** and Qualitatively to be able to meet required risk reduction. Communications between subsystems will be much more efficient, faster, and more reliable.



Benefits of suggested improvements

- **System continuously tests itself for faults(I/O, Processor, Com., etc.)Re-certification testing becomes much more efficient and much less intensive and time/resource consuming.**
- **We can reduce re-certification time period significantly**
- Single Programming Platform, RSLOGIX5000 - $ cost savings
- Less hardware needed to achieve better results - $ cost savings
- Higher level of Availability and reliability - $ downtime savings
- Higher level of safety achieved than with industrial PLC's (SIL1>>SIL2/3) Peace of mind
- Modular architecture - $ cost savings
- Conducive to third party audits, inter-departmental, outside firm, DOE
- Standard Safety Function Blocks for consistent and certified Code -Peace of mind
- Only Single Programmer may be Required= more support with less people $ cost savings and improved efficiency
- Cost effective for spares $ cost savings