SUMMARY OF SESSION 5
HOW SHOULD WE HANDLE SAFETY?

Markus Albert and Ghislain Roy
CERN, Geneva, Switzerland

1. INTRODUCTION

This session was originally titled ‘Safety! Who cares?’ in a fairly provocative way. A clear conclusion of this session and discussions that were held at the workshop is that there is a wide concern for safety among the people in charge of control room operations. This was shown as well by the quality of the seven talks presented in this session on subjects ranging from safety standards to a practical case of a safety incident:

• Application of Functional Safety Standards in a Particle Accelerator Environment.	L. Scibile (CERN)
• Operations at CERN under INB Regulations.	A. Faugier (CERN)
• Operations and Regulations at Fermi National Accelerator Laboratory.	P. Carolan (DoE/FNAL) D. Johnson (FNAL)
• How does the Control Room handle Safety at ESRF?	P. Duru (ESRF)
• Operations experience with the RHIC Particle Accelerator Safety System.	N. Williams (BNL)
• Safety Issues in Accelerator Operations: Groundwater Contamination.	P. Ingrassia (BNL)

The first three presentations concentrated on design standards and regulations, in other words the methods and context of Safety in our environment. The next two presentations showed examples of Safety in Practice: from a Control Room point of view and from an Access system point of view. Finally the last presentation is a real case study and analysis of a safety incident with the lessons learned and some useful advice to everybody.

2. STANDARDS AND REGULATIONS

L. Scibile introduced the notion of Functional Safety, in the words of J-C Laprie: The notion of functional safety, or dependability, is defined as the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers.’ Functional safety has a two-fold objective: Guaranteeing that systems work and that they work safely.

L. Scibile then went into more details of Functional Safety Standards, a set of methods, based on international standards IEC 61508 –> 61511, aiming at providing a system which is reliable, available, maintainable and safe all along the life-cycle of the system, from specification to decommissioning. Besides the avoidance, elimination and prevention of faults functional safety standards can facilitate the application of rules and the compliance to national regulations. Extensive applications of the methods at CERN are foreseen in the fields of control systems, control room operations, and operational processes.

Some messages picked up during the presentation:

Safety is first about people…
Safety objectives help answer the question: ‘How much quality is enough?’
‘How much safety is enough?’ is the wrong question; ‘how much money is enough to make it safe according to my objectives?’ is the right question!

A. Faugier reviewed the rules and regulations enforced in some of CERN's installations. In France a large spectrum of facilities such as nuclear reactors, waste conditioning plants, factories for the fabrication or transformation of radioactive materials, plants for storage of radioactive materials or waste, and finally particle accelerators with a beam power larger than 0.5 kW are all classified as Basic Nuclear Installations (INB or Installation Nucléaire de Base). By convention (international agreement) between CERN and France, the Super Proton Synchrotron (SPS), Large Hadron Collider and Cern Neutrino to Gran-Sasso (CNGS) facilities are now under INB rules and regulations. The implications are numerous and very similar to those stemming from the rules presented by P. Carolan of the Fermilab DoE office in his talk.

A major difference however is that the US Department of Energy has not classified its Accelerator Facilities in the category of Nuclear Facilities but is providing specific rules and regulations for the operation of accelerators. DoE establishes a contract with the organization that operates the facilities and can enforce rules and regulations through the contract and sometimes even outside the contract.

As an example P. Carolan reviewed DoE Order 232.1A, applying to all DoE facilities and titled 'Occurrence Reporting and Processing of Operations Information'. It aims at keeping DoE and others informed of occurrences at facilities that could adversely affect security, health and safety of the public, the environment, etc. All reported occurrences are logged in a database that will soon be available to the public via the Web. P. Carolan also noted that a small percentage of occurrences involve accelerators and only a small percentage of these involve operations personnel directly; a tribute to the quality of the work performed by operations personnel in accelerator laboratories.

Most of the reported occurrences concerning accelerator operations fall under one of the following categories:

- access control procedure violations
- improper Lock-Out / Tag-Out practices
- improper response to radiation alarm
- excessive prompt radiation / shielding problems
- exceeding operational limits
- experiment safety (breakdown in hazard mitigation, and hazard communication between accelerator/support/users)

It should be noted that one occurrence in the last category lead to one experiment being cancelled.

As an application of the above, D. Johnson explained how the Operations Group of the Beams Division at FNAL have implemented a 'Conduct of Operations' in response to another DoE Order. The idea of having Conduct of Operations was taken originally from the Institute of Nuclear Power Operations and translated to Accelerator Operations in late 1989, although DoE owned accelerators are not classified as nuclear facilities. The Conduct of Operations is structured in 18 chapters covering all aspects of accelerator operations.

The 18 chapters of the Conduct of Operations	
Organization and Administration	Independent Verification
Shift Routines and Operating Practices	Logkeeping
Control Room Practices	Shift Turnover
Communications	Operations Aspects of Facility; Chemistry and Unique Processes
Controls of On-Shift Training	Required Reading
Investigation of Abnormal Events	Shift Orders
Notifications	Operations Procedures
Control of Equipment and System Status	Operator Aid Posting
Lockouts and Tagouts	Equipment Labeling

D. Johnson explained how they have turned this required document into a working document to help them in their mission. In particular the following advantages were listed and are shared with other DoE laboratories represented at the workshop.

- Common operational attributes
- Do not rely solely on 'Word of Mouth'
- Forces people to write it down
- Used to train Department/Group
- Generates understanding and new ideas
- Aids in audits and reviews

3. SAFETY IN PRACTICE

In this part of the session the first talk exposed the handling of safety aspects in the Control Room of the Electron Synchrotron Radiation Facility in Grenoble (France). P. Duru explained that their goal for the operation of the facility is 'a good availability, a satisfactory Mean Time Between Failure (MTBF), all together in SAFE CONDITIONS'. A more appropriate formulation would put the safety aspects first and turn the goal into 'Providing, under SAFE CONDITIONS, a good availability and satisfactory MTBF of the facility'.

The Safety Console in the control room, facing the main console, is in the back of the operators. It regroups a wide range of alarm panels: Fire detection, Flooding detection, and Red Phone. The operators are trained in First Aid and can be called on an accident. Procedures to answer any of these alarms are provided in the form of easy to read and follow flow charts. Alarms are automatically printed and Red Phone conversations are taped and broadcast in the control room.

Besides this first line responsibility during shift work, the operations group handles the scheduling and co-ordination of all work in the tunnel during technical stops; they deliver fire permits and work permits. This allows them to be aware of all activities in the machine and to give proper advice and instructions to the personnel who are to enter the ring. The Personal Safety System for access into the machine is also centralized on the Safety Console and the operators can be called to do a radiation survey of the zone where people will enter.

The range and depth of the safety responsibilities of the ESRF operations group is impressive and certainly stressful. It is however not uncommon for smaller facilities to organize themselves like this while larger laboratories tend to decouple some of the general safety aspects (Fire, Red Phone…) from beam operations for obvious reasons of size and logistics.

N. Williams, head of the Access Controls Group at Brookhaven National Laboratory, presented another side of the coin in a large accelerator facility. The Personnel Access Safety System (PASS) allows access control into the Relativistic Heavy Ion Collider (RHIC) and its experimental areas. The PASS combines the monitoring of Oxygen Deficiency Hazards (ODH), Electrical Hazards and Radiation Hazards integrated into a single system. Fire alarms and Flammable Gas alarms are also taken into account since the ventilation and air extraction from the tunnel is triggered by this system.

The Personnel Safety System employs small Programmable Logic Controllers (PLC) interconnected as two sets of peers, separated into channels 'A' and 'B'. This is done to achieve a redundancy level, for the most complex part of the system, greater than that provided by the dual level achieved by other designs. The high redundancy objective also implies having separate power supply lines and UPS for the two different crates at each access point and goes as far as providing a separate development for each of the two systems: different environment and programming team to also avoid common mode failures. The more critical devices are surveyed through this double PLC system and through a relay-based system. More arcane safety aspects of the system have been taken into account by providing panelviewer consoles in place of PC based units for the access console in order to eliminate the risk of a hacker getting into and tampering with the system.

N. Williams also presented the hardware (gates and keys) used for controlling entries into the machine. Besides the classical cards and keys found in most laboratories, two specific experiments at BNL have requested the installation of biometrics devices for access control into their experimental zones: Iris Scans for one and Palm Tracks Recognition for the other. Much interest was generated by these aspects and some of the advantages of e.g. the Iris Scan techniques are worth mentioning:

- The system is totally hands free. No possibility of contamination and the handling of materials and safety clothing or masks are not a problem; eyeglasses or contact lenses do not affect the system.
- The system is fast (identification in 2 seconds), tremendously accurate and relies on a comparison of pictures of the iris being taken by an autofocus CCD camera. No laser as required by retinal scan.
- No card to carry, no password or PIN to remember, but it is a PERSONAL Identification Nevertheless!

In the summary session the question was asked whether BNL would consider a wider use of biometrics systems if they had a choice and the answer was positive; N. Williams explained that they are now considering using biometrics identification for site access as well.

4. CASE STUDY

P. Ingrassia presented a case study starting from an incident of water contamination that happened at BNL in 1997. Following a storage pool leak of 5 Ci of Tritium the water table on site was found to be contaminated beyond the allowed Drinking Water Standard although it was by no means a large contamination. The laboratory drilled a large number of wells to check this contamination and found some other locations on site with water contamination albeit from other causes. First lesson: if one starts looking for occurrences of a given problem chances are they will look hard enough and eventually find them.

Looking at the contributing causes of the second source of contamination, beam loss at a quadrupole in a beam line to a target, the main cause is found to be inattention to details all along the chain of responsibility. Beam losses in this particular case were higher than expected from design and almost all the monitoring of the beam was at the target, raising again the question of how we define beam quality. The beam loss monitors that were installed in the beam line were unreliable which is worse than not having them because they tend to be ignored even if the signal is correct. Tuning

procedures focusing on ALARA principles, although properly implemented and followed, did not help since the instrumentation was either missing or not reliable and ignored.

P. Ingrassia expanded on some of the lessons learned from this case study:

- For any beamline or accelerator it must be assumed that there will be some beam loss, and that any soil used as shielding must be covered to prevent rain leaching out contaminants. An activation study should be routinely performed following the first run of a new beam-line to confirm the beam loss assumptions that were made the during design phase. The situation should be reviewed whenever operational conditions change (increased intensity or different beam parameters such as spot size…).
- Ensuring that the beam is fixed on target does not necessarily ensure that the beam is not lost on upstream components and operators must also monitor beam loss on a routine basis, with proper procedures in place, in order to limit the level of soil or material activation. Remote sensing devices (loss monitors or equivalent) must always be operational all along the beam path and procedures to respond to loss alarms must be in place. In fact the question of interlocking the beam if the beam loss monitoring system is not available was raised.
- Operator mindset needs to change to become proactive in minimizing losses and ‘Clean Records’ should be favored. An intensity record on a target is only acceptable if the losses are also well controlled; in other words beam quality needs a very careful definition. In some cases the intensity on target will clearly be limited by loss limits, not by intensity limits from the accelerator.
- Wherever the actions of the operators on the beam could have an impact on the environment the operators must be made aware and trained in Environmental Protection Issues. It was added at the summary session that this should also apply to Public Relation Issues both towards the local community and the Press.

5. CONCLUSION

This session was interesting in many respects. The subject of Safety can sometimes be perceived as rather unimportant or less important than the mere performance of the accelerator, until an incident occurs. The operators who know the machine and control the machine operation on a daily basis are best placed to play a significant role in advocating and ensuring safe operations from design to beam tuning. The level of interest for Safety matters shown at the workshop is certainly a sign that Safety is taken very seriously by Operations teams across all accelerator installations independent of the size and type of beams.

APPLICATION OF FUNCTIONAL SAFETY STANDARDS IN A PARTICLE ACCELERATOR ENVIRONMENT

L. Scibile, S. Grau, P. Ninin
European Organisation for Nuclear Research – CERN
1211 - Geneva - 23, Switzerland

Abstract
Many systems used by the CERN accelerators and the technical infrastructure have to respect stringent requirements in terms of reliability, availability, maintainability and safety either for operation, security, or legal aspects such as the one required by French Regulatory Authority (Installations Nucléaires de Base - INB). The functional safety approach provides a structured method for achieving these requirements. In particular, the new IEC 61508 standards give guidance for system design and an effective and safe system exploitation. When designing new systems, it also sets out a generic approach for all the safety lifecycle activities: requirements, design, realisation, installation, operation, maintenance and even the decommissioning. The standards consider the functional safety from three different, but related, perspectives: technology, procedures and human interventions on the systems. This paper gives the results of the first attempts made at the CERN Technical Service division to use these standards and gives some suggestions on how to improve functional safety in a particle accelerator environment.

1. INTRODUCTION

As computer control becomes usual for many CERN accelerators and technical infrastructure applications, it becomes apparent that the failure of these systems is likely to have an impact on the operation and/or on the safety of the people and the equipment. The risk of a failure with its consequences has given rise to stringent requirements in terms of Reliability, Availability, Maintainability and Safety (RAMS). Moreover, CERN must also comply with the safety requirements set out by the French Regulatory Authority: the INB (*Installations Nucléaires de Base*).

To increase the RAMS performance of a particle accelerator environment is a big challenge because it involves the management of the opposite requirements of safety and flexibility. The other challenging aspect is to organise the work processes to cope with the reduction of resources, the dynamics of the new computer control technologies and the CERN outsourcing policy.

The functional safety standard for Electrical/Electronic/Programmable Electronics (E/E/PE) systems IEC 61508 [1] has been used as a management guideline to structure the work on safety-related control systems. An overview of this approach and the IEC 61508 is given in Section 2.

The benefits and the pitfalls of the practical application of this approach in the Technical Sector (ST) division are presented in Section 3.

2. FUNCTIONAL SAFETY

2.1 Description of functional safety

The definition of functional safety, or dependability, has been expressed by the J-C Laprie [2] as:

'The notion of functional safety (dependability) is defined as the trustworthiness of a computing system which allows reliance to be justifiably placed on the service it delivers.'

Consistent with this definition, functional safety has a two-fold objective: guaranteeing that systems work and that they work safely. Therefore, functional safety can be seen as a method for developing a system that attains the proprieties of reliability, availability, maintainability and safety. In addition, the application of an overall safety lifecycle guarantees that these proprieties are maintained from conception to decommissioning. Functional safety is based on three major axes: people, procedures and methods. And the results of a recent study by the UK Health and Safety Executive on the causes of accidents, shown in Fig. 1, support this strategy that people, procedures and methods are capital for the reduction of faults and accidents.

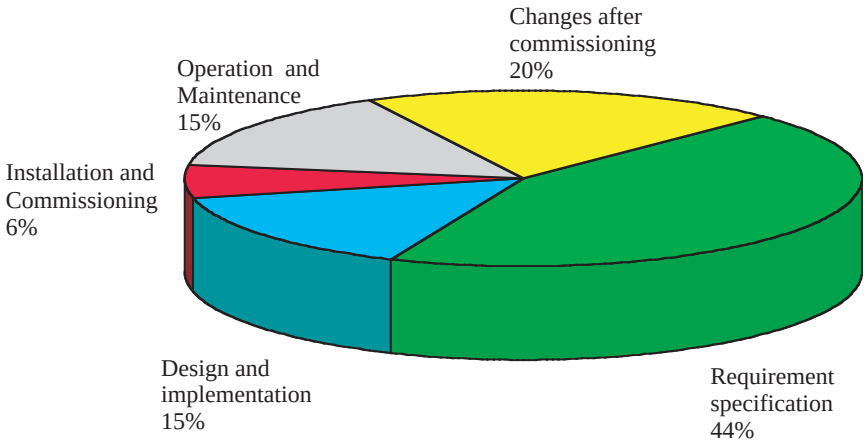


Fig. 1: HSE statistics on causes of accidents

In the field of computer controlled systems, the functional safety standard IEC 61508 defines a generic approach and a technical framework for dealing systematically with safety related activities. This methodology enables us to minimise system failures and optimise performance. It is particularly interesting because it defines the skills needed to deal with safety, the required procedures to be defined and carried out, as well as the kind of development methodologies to be used. The standard also provides an overall safety lifecycle that focuses the attention on the safety aspects of each phase of the development process.

2.2 Functional safety, quality and the standards

The functional safety approach addresses the issues of awareness, responsibility and commitment in the organisation (or a project). In this mindset, special attention is given to the understanding and the evaluation of the real needs/expectations in terms of functional and safety requirements.

The IEC 61508 provides all the processes to build the understanding of the real needs/ expectations in order to meet them. In addition, the standard explicitly addresses the issue of continuous process improvement (as found in the Capability Maturity Model developed by the Software Engineering Institute [3]). This mindset, with the processes for achieving it, is the basis for a total quality in safety-related control systems. And quality is of fundamental importance to safety because it relates to the ability of a system to meet its requirements.

On the other hand, in addition to providing the answer to the question 'how much safety is enough?' in terms of Safety Integrity Levels (SIL), the IEC 61508 also provides a way to answering to the question 'how much quality is enough?' Therefore, there is a multiple result by adopting a functional safety approach: the achievement of the required RAMS and the assignment of the sufficient effort in terms of design, realisation, installation, operation and maintenance, management and quality.

3. FUNCTIONAL SAFETY IN THE ST DIVISION

3.1 Why?

In order to face the issues of quality, project management, operation & maintenance, safety and cost optimisation for the concept phase of the CERN Safety Alarm Monitoring (CSAM) [5], the ST/MO group formed a team for functional safety. After a positive experience, functional safety is being extended to other safety-related or critical control systems.

Quality: As largely explained in this paper, the issue of quality is solved by adopting the overall safety lifecycle of the IEC 61508 with the adherence to the requirements for the management of the functional safety.

Project Management: Safety-related projects must cover additional management tasks. These also include the management of the safety requirements and their allocation, functional safety assessment and functional safety audits.

Operation and Maintenance: The standards provide an organisational framework for identifying and managing the operation and maintenance of safety-related systems. These include specific procedures for reducing the risk of accidents. The application of a systematic analysis of the operational constraints during maintenance and the definition of the preventive maintenance based on the required RAMS imply a maintenance plan with an overall cost estimation.

Safety and cost optimisation: The functional safety approach brings to an overall estimation and optimisation of the total life costs of a safety-related system because it implies the justification of the proposed solutions against measurable required safety performance and the optimisation of the operation and maintenance procedures.

3.2 How?

People are an essential element in the organisation of functional safety. Therefore, special training was organised in order to increase the knowledge of the team, to raise the awareness of the risks associated to safety-related control systems, to create a common base of knowledge and to have a feedback from industrial experts.

The training objectives have been attained and the results have been applied during the preparation of the functional and safety requirements for the CSAM technical specifications [6].

The process of knowledge acquisition/sharing has continued by actively participating to specialist conferences and seminars and by making presentations at CERN working groups and workshops.

3.3 Where?

The functional safety approach is being applied in different areas and problems as described in the following paragraphs:

Overall projects: For the CSAM project [5], functional safety has been set-up from the very beginning. The IEC 61508 has been used as a canvas for the concept phase and for structuring the system lifecycle. The standards have eased the preparation of the technical specifications and the performance requirements for the CSAM invitation to tender. In particular, it has helped in the drawn up of clear and concise performance requirements for a result oriented contract; it has also been useful for the cost estimation of the system itself and of the long-term operation and maintenance services.

Re-engineering: The execution of a systematic analysis for the SPS smoke removal control system is providing an essential overall understanding of the main safety functions executed by the system. The analysis has indicated functional priority and critical elements. The first phase has provided technical recommendations to guarantee that sufficient effort is invested in these functions.

Dependability analysis: As a quality commitment to continuous improvement, a functional safety approach was used for the dependability analysis of the Technical Data Server [7]. Even in this case, the execution of a systematic analysis has uncovered potential for improvement and has also identified and quantified the weak points of the current system.

Functional safety support: To add value to a project, a functional safety engineer must be fully involved in the design team. Functional safety support was provided for the Water 2000 monitoring project. The main contributions have been an insight to the control system risks and a set of recommendations to mitigate or eliminate them.

4. CONCLUSION

This paper gives the results of the first attempts made at the CERN Technical Service division (ST) to use the IEC 61508 functional safety standards. It is shown that functional safety can be applied in different fields and under different perspectives. After an initial investment in training and coaching, the functional safety approach is producing the expected confidence in the concerned projects and systems. In particular, the collaborative effort for the CSAM project has produced robust specifications and precise cost estimations. The use of systematic and methodical analysis has also helped to identify other systems' deficiencies and inefficiencies and has provided means to avoid or eliminate them.

5. ACKNOWLEDGEMENTS

It is a pleasure to acknowledge the support and the invaluable contributions given by all the member of the CSAM Team.

References

[1] IEC 61508, *Functional Safety of Electrical/Electronic/Programmable Electronics (E/E/PE) systems, Part 1, General Requirements,* Geneva: International Electrotechnical Commission.

[2] J.-C Laprie, *Dependability: Basic Concepts and Terminology,* International Federation for Information Processing WG 10.4, (Ed.) Springer-Verlag, 1992.

[3] M. C. Paulk, *Comparing ISO 9001 and the Capability Maturity Model for Software,* Software Quality Journal, Vol. 2, No. 4, December 1993, pp. 245-256.

[4] IEC 60601-1-4, *Medical electrical equipment - Part 1-4: General requirements for safety - Collateral Standard: Programmable electrical medical systems,* Geneva: International Electrotechnical Commission.

[5] S. Grau, P. Ninin, R. Nunes, L. Scibile, C. Soler, *CERN Safety Alarm monitoring Project*, 3rd ST workshop Chamonix, February 2000.

[6] S. Grau, L. Scibile, F. Balda, A. Chouvelon, *Application of risk management for control and monitoring systems*, 4th ST workshop Chamonix, January 2001.

[7] R. Bartolome, F. Havart, L. Scibile, S. Grau, *Achieving a 'SIL 1' TCR monitoring system*, 4th ST workshop Chamonix, January 2001.

HOW DOES THE CONTROL ROOM HANDLE SAFETY AT THE ESRF?

Ph. Duru, L. Hardy, P. Berkvens, P. Colomp
European Synchrotron Radiation Facility, Grenoble, France

Abstract

The operation of an accelerator presents a very particular risk; exposure to radiation either directly from prompt radiation during operation or from induced radiation during tunnel access. The access to the machine tunnels is therefore fully controlled.

Moreover, all the buildings also present various risks, depending on the laboratories and other installations that they may contain and by the presence of people 24h a day. The premises are then under supervision.

In order to provide full control of all these risks, different systems of interlocks, locking, monitoring and detection have been installed at the ESRF which send all the information to the Control Room.

In collaboration with the Safety Group, specific procedures have been elaborated which help the Operators to handle any event in the best way possible.

1. INTRODUCTION

The European Synchrotron Radiation Facility (ESRF) is an X-ray source of the third generation. The accelerator complex is composed of a Linear accelerator (e- 200 MeV), a synchrotron (300 metres – 6 GeV) and a Storage Ring (844 metres).

The ESRF accelerators have been in full routine operation for more than six years. The source delivers 5600 hours of X-ray beam to nearly 40 beam lines simultaneously. Our first goal is to ensure good availability of the Machine as well as a satisfactory Mean Time Between Failures (MTBF) all together in safe conditions.

2. THE DIFFERENT ASPECTS OF SAFETY AT ESRF

2.1 Fire

Almost every room throughout the buildings is equipped with one or several detection heads. Depending on the nature of the risk, the sensor may be of anionic, thermostatic or UV type. There are about eight hundred detection heads operating at ESRF, all of which are computer controlled.

2.2 Flooding

Many pieces of equipment installed on the site are water-cooled. They are of course protected by over temperature and/or flowmeter interlocks in case of a water cooling system failure, but the bursting of a pipe or a hose may lead to major damages if the fluid is spread over equipment. It may also bring the water distribution system to a stop because of a low level in the network. A flooding detection system is installed in all the tunnels, the beam lines and in the rooms containing the main Machine dedicated equipment.

The geographic situation of the Facility, where two rivers join, and its construction altitude require also a constant watch over the ground water level.

2.3 Personal Safety

The size and the configuration of the ESRF site have made the installation of a Red Phone network mandatory ever since the construction of the Facility. The objective is simple: to be able to contact the Control Room very easily in case of any emergency need (fire, faintness, accident etc…). There are about 230 red phones located in all the buildings of the ESRF site.

2.4 Temperature overheating

All central computer resources are concentrated in one room. The equipment in this room is indispensable for the running of the ESRF; a shutdown of the network equipment or any of the server computers immediately disturbs the work of a Group, a Division or even the entire Facility. A failure of the air conditioning unit would create an increase of the ambient room temperature and may lead to a severe control system crash. Any temperature increase triggers an alarm in the Control Room.

2.5 Interventions scheduling and co-ordination

The numerous types of equipment are subject to upgrade, modification, repair or preventative maintenance. Most of these duties are undertaken during the Machine Shutdowns, planned one year in advance but may take place at anytime in case of failure or breakdown. In order to optimise the interventions in terms of safety, resources and quality during the Machine Shutdown, the Operation Group takes over the co-ordination of the tasks.

2.6 Safety related with X-ray source

The general Radiation Protection policy at the ESRF stipulates that everybody working at the ESRF is considered as a non-exposed worker. Therefore, under all conditions one must guarantee that nobody exceeds the corresponding radiation limits (1 mSv per year). This is obtained via appropriate shielding of all accelerator tunnels and of the X-ray beam lines, and via all the corresponding Personnel Safety Systems. One particular aspect is the radiation hazard created by induced activity, limited exclusively to the accelerator tunnels. For this purpose, the Operations Group co-ordinates a system of work permits. Before entering any accelerator tunnel, a radiation survey must be made of the induced activity in the area concerned. This survey is made by the Safety Group (start of main shutdown, important intervention) or by the Operators (routine intervention during Controlled Access). As a result of these surveys specific safety procedures are elaborated.

3. THE ROLE AND THE TOOLS OF THE OPERATION GROUP TO HANDLE SAFETY

3.1 Fire Detection System

Every alarm trigger, following either a real detection of smoke or a failure of the detection system, is reported to the Control Room. The message written on the screen gives the identity of the head triggered or the faulty device, the name of the building and the number of the room. An application made on a SuperCard by the Operators and installed on a computer in the Control Room enables the fast localisation of the triggered detector, by going through windows from the number of the detector to the plan of the building and the room concerned.

Different procedures, depending on the time of the day and the status of the Machine (run or shutdown), are available in the control room in a form of a flowchart. They describe the steps to follow, and give all the relevant information to the Operator on shift; from the verification of the alarm on the spot to the initiation of the proceedings for the evacuation of the building, the call to the Fire Brigade and to the on-call Safety Engineer.

A fire permit is mandatory to perform any work that may produce smoke and trigger a sensor (welding, grounding, etc…). A copy of any delivered fire permit is posted in the control room; in case of a fire alarm, the Operator can verify if it comes from the concerned works or not.

3.2 Flooding Detection System

It consists of a sensitive cable laid on the accelerator tunnel floor and linked to a controller, which permanently measures its conductivity. In the case of fluid detection on the cable, the controller triggers an alarm and, via a computer, gives an approximate distance that facilitates the localisation of the leak. In the other critical rooms, such as beam lines and main power supply cubicles for instance, the detection system is made of optical detectors.

In the case of an alarm, the Operator will enter the zone to investigate the problem. A procedure gives the Operator the steps to follow to ensure his own safety from a radiation protection and an electrical point of view and to protect the equipment. Depending on the seriousness of the failure, the Operator will carry out the repair himself or call the on-call Maintenance Technician.

3.3 Red phone System

As soon as somebody picks up any red phone anywhere on the site, or dials 10 from any other telephone set to report any kind of incident, he is automatically connected to the red phone receiver located in the control room. An on-line printer keeps track of all the emergency calls and gives precious information as to the location of the phone call. An application based on the same principle as for the fire detection system will be developed in the forthcoming months.

A checklist guides the Operator during the call to get all the relevant information from the caller. The corresponding procedure is then applied, depending on the nature of the call.

All the Operators are trained to above all to help any injured person, in the frame of his working environment; depending on the situation. The Operator on shift may decide on the spot to go and give the victim assistance, whilst waiting for the Emergency Aid Brigade.

3.4 Interventions scheduling and co-ordination

A few weeks before the shutdown, the list of the interventions foreseen by every Equipment Group Leader is sent to the Operation Group Co-ordinator. He will then elaborate a detailed schedule, listing the tasks to be undertaken, taking into account the different constraints raised by the nature of the work such as handling, bake out, alignment, electrical and fluids cut-offs etc… The proposed schedule is accessible via the internet and submitted to all concerned people. It is regularly updated before and during the shutdown.

At the start of the Machine Shutdown, the Safety Group performs a Radiation Protection survey inside all the tunnels. From the measurements taken during this inspection, a Radiation Map showing the zones containing activated equipment is drawn up by the Operation Group and posted in all the access chicanes of the Machine. Depending on the type of intervention to be performed on the equipment, their electrical power supplies may be subject to a partial or complete ‘consignation et mise à la terre’.

For any intervention planned inside the tunnels, a Work Permit Form must be filled in by the Intervention Responsible and submitted to the Operation Group and the Safety Group for approval. The permit contains the description of the intervention, the place and the names of the people in charge of the works. It provides information about safety-related actions or requirements such as shielding dismounting radiation exposure limitation or electrical insulation. A copy of the Radiation Map is attached to every work permit.

The Co-ordinator assumes the follow-up of the activities carried out during the Shutdown and reshapes the schedule in accordance with any modification. The Operator on shift or on a normal day assists the Co-ordinator during the day and carries out a safety round during the night and the weekend. He will pay particular attention to the zones where bake out is being performed.

At the end of the shutdown, once all the work permits are recovered by the Operators, a safety round is performed by the Safety Group and the Operation Group Co-ordinator in order to verify that

all the shielding parts and protective covers have been put back in position. A protocol is then filled in, signed by both parties and recorded in the Machine Operation Logbook.

3.5 PSS and Radiation Protection

The PSS (Personnel Safety System) is a hardwired, redundant system. The PSS provides the permits for the different accelerator systems, allowing different operation modes. These modes are selected on a safety key panel located in the Control Room. The tunnels are locked after the search has been made by at least two operators. Entering any zone is always possible in Controlled Access, using a system of safety keys, supervised by the Control Room.

As explained before, the main role of the Operation Group in terms of Radiation Protection, is linked to the problem of induced activity inside the accelerator tunnels. During interventions under Controlled Access, the Operators carry out the radiation measurements. For this purpose the Safety Group provides the Control Room with radiation monitors (Eberline FH-40GL survey meters) and operational dosimeters (Rados DIS-1 badges). Written safety procedures are available in the Control Room.

4. CONTROL ROOM PARTICIPATION IN A NUT SHELL

Table 1: Statistics of the last four years

Year	Fire Alarm	Red phone	Water Leak	Lift failure	Others
1997	30 (1 fire)	3 (2 serious)	0	1	1
1998	14	5 (5 serious)	1	1	0
1999	22 (1 fire)	5 (4 serious)	1	1	0
2000	41 (2 fires)	8 (4 serious)	3	1	1

5. CONCLUSION

Since all the main safety equipment is linked to the Control Room, the Operation Group is called to react and participate in all safety related events. As well as being trained to be Machine Operators, in the event of an emergency their skills and common sense will be invaluable to insure the safety of all present on the ESRF site.

FIRST YEAR EXPERIENCE WITH THE RHIC PERSONAL ACCESS SAFETY SYSTEM (PASS)

N. W. Williams
Brookhaven National Lab, Upton, NY, USA

Abstract
Review Operations first year experience with the RHIC Particle Accelerator Safety System (PASS). This includes the accelerator access controls, radiation monitoring and the oxygen deficiency hazard(ODH) monitoring systems.

1. INTRODUCTION

A single RHIC Personnel Safety System was installed to protect the Collider personnel from Radiation Hazards, Oxygen Deficiency Hazards (ODH), and Electrical Hazards and assure full compliance with regulatory requirements. In the past, ensuring personnel safety at accelerators meant an Access Control System designed to protect personnel from radiation hazards only. Integrating all personnel safety systems in RHIC is expected to result in a superior level of personnel safety and equipment protection, while providing greater operational efficiency. It is also intended that the Personnel Safety System have a closer interface with the fire protection elements installed as part of the conventional construction than has been the case in other accelerator construction.

2. DESCRIPTION

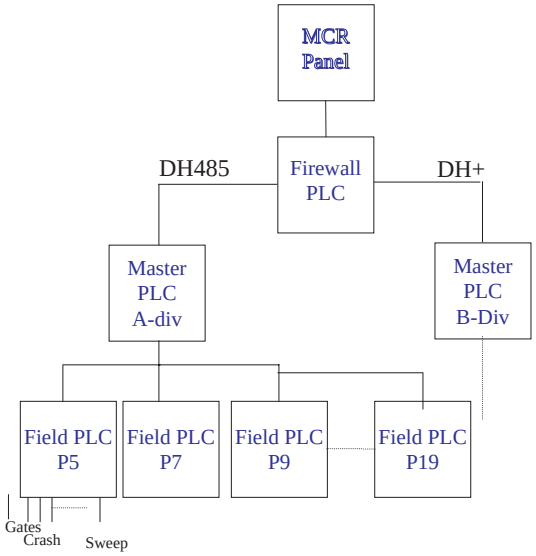
Required safety systems for Oxygen Deficiency Hazards (ODH), Electrical Hazards and Radiation Hazards are integrated into a single system. The Personnel Safety System will employ fourteen small Programmable Logic Controllers (PLC) interconnected as two sets of seven peers, channels ‘A’ and ‘B’ in Fig. 12-1, rather than a few larger units hierarchically connected to multiple remote I/O chassis. This is done to achieve a higher level of redundancy for the most complex part of the system, than that provided by the dual level designs.

2.1 Control Devices

Commercially available Programmable Controllers are configured to attain the level of redundancy necessary to achieve compliance with DOE 5480.25. A network of PLC units compensates for the complex set of failure mechanisms exhibited by individual processors compared to designs based upon relays, much as an OP-Amp compensates for component variability with gain and feedback or a bridge is supported by its interconnecting I-beams.

In order to reduce the potential for Common Cause failure events, the core PLC system will be comprised of two different brands or models of PLCs (Allen Bradley PLC 5 and SLC 5/03,4 processors) such that basic hardware and software elements will be of different origin; each PLC has its own independent UPS and line power feed. Complications introduced by physical bus limitations result in a rather complex interconnection pattern, however, a minimum of two independent channels labeled ‘A’ and ‘B’ is always maintained. The ‘A’ and ‘B’ channels are in turn connected to one of two Command and Control processors which provide supervisory control and monitoring functions. These processors are in turn redundantly connected to a Personnel Safety System-generated display located in C-AD Main Control System (MCR).

PASS System Block Diagram



2.2 Crash, Gates and Sweep sub-system

An emergency shutdown system labeled CRASH, which uses 'pull cord' type switches, is installed throughout the collider enclosure. With minor exceptions, these are essentially continuous coverage on both sides of the enclosure tunnel. Because of magnet locations, coverage in supported injection areas are installed on one side only. Each unit protects 65 m (200 ft) of tunnel. The CRASH switches are not hard wired into a lockout system, but are connected in a redundant manner to a PLC in the 'A' channel and to another PLC in the 'B' channel. When a CRASH is called for, the Personnel Safety System removes power from selected critical power supplies or closes selected critical vacuum valves. In addition, the Beam Dump System will be activated. This dual approach is necessary because the Beam Dump system, while engineered and constructed to high standards, is not considered part of the Personnel Safety System.

The Gate system is comprised of thirty five (35) Gate packages and nineteen (19) Emergency Entrance and/or Exit Doors packages. Redundant interlock switches are mounted on each of these doors. Each entry and isolation gate has standardized electronics system for information, display and access purposes. This package includes TV monitoring capability in the Main Control Room (MCR). In addition, there is a card reader based entry logging system and information display at each gate. The Radiation Monitoring system uses the 'Chipmunk' design used at the AGS and at FERMILAB. Interlock outputs will be connected to system PLC units.

Each crash, gate and sweep switch is monitored using a constant (32 mA @ +/-10 Vdc) current source that determines their status. This scheme reduces the complex cable network that would have been required for a completely hardwired system.

2.3 Remote Hardware Interface

The PLCs use remote scanners, plug-in I/O modules and Remote I/O blocks to communicate with the field hardware. All critical devices utilize a combination of relay and R I/O hardware interface.

2.4 Radiation Monitoring

The Radiation Monitoring system employs the 'Chipmunk' design used at the AGS and at FERMI. Interlock outputs are connected to the PLC units. Of the approximately eighteen (18) units installed,

twelve (12) units for experimental area monitoring and six (6) units for RHIC injection. Dose rate data are read by VME based optically coupled SIS3803 scalars into the central control system.

2.5 Oxygen Deficiency Hazards (ODH)

The ODH system is comprised of sensing and processing electronic hardware. The sensing electronics are built around a commercially available oxygen fuel cell. The detected ODH level is sent to the PLC controller which decides if the fans and vents need to be activated. The fans and vents are not automatically activated during stores.

2.6 Flammable Gas Detection Systems

Both the STAR and PHENIX experiments have Flammable Gas Detection System (P10 gas). This system uses industrial grade fixed-point infrared detectors with visual and audible alarms. Fans and vents are used to exhaust the halls. The fans and vents are not automatically activated during stores.

2.7 Fire Alarm Interface to PASS

The RHIC tunnel fire alarm system is connected to the PASS. This allows the use of ODH fans and vents to exhaust the tunnel during a fire. As in the case of the ODH and Flammable Gas systems, fire alarms will not automatically exhaust the enclosure during stores.

2.8 PASS MCR Interface

The MCR interface to the access system consists of the Closed Circuit Television (CCTV) system and Panelviewer computer terminals. The CCTV is used to perform remote access into RHIC entry gates. This uses video multiplexers and fiber optics cables to route the signals to MCR. The video switching is done using a SLC based system.

Panelviewer terminals are used to send commands and get status information from the field peers.

3. UPGRADE TO THE AGS RELAY BASED SYSTEM

Due to the unique requirements of two experiments running at the AGS, various upgrades were done to the beam areas of the AGS access system.

3.1 NASA E951 Iris Identification

NASA experimenters required a method of identification that would require minimal use of hands since they typically carry specimens. Iris identification does not require the use of PIN numbers but allows individuals to stand at the CCD camera and be recognized by unique characteristics of the iris. Iris Identification in conjunction with Trapped Key Technology controls who can enter primary gate. Simultaneous release and video ensured MCR still had entry control. No beam is delivered by MCR until all keys are returned and trapped.

The local reader uses a secure network to log entries in MCR. An enrollment station located in MCR allows users to be checked for proper training. Once scanned the individual’s iris code is downloaded via Ethernet to a processor at primary gate.

3.2 Proton Radiography E933

This experiment uses the Hand Reader technology for access at LANL and requested this setup due to prior familiarity. This was also a cost effective means to address experiment requirements. The enrollment station located in MCR allowed users to be checked for proper training. Once scanned the hand code is downloaded via Ethernet to the access hand reader at PTR house.

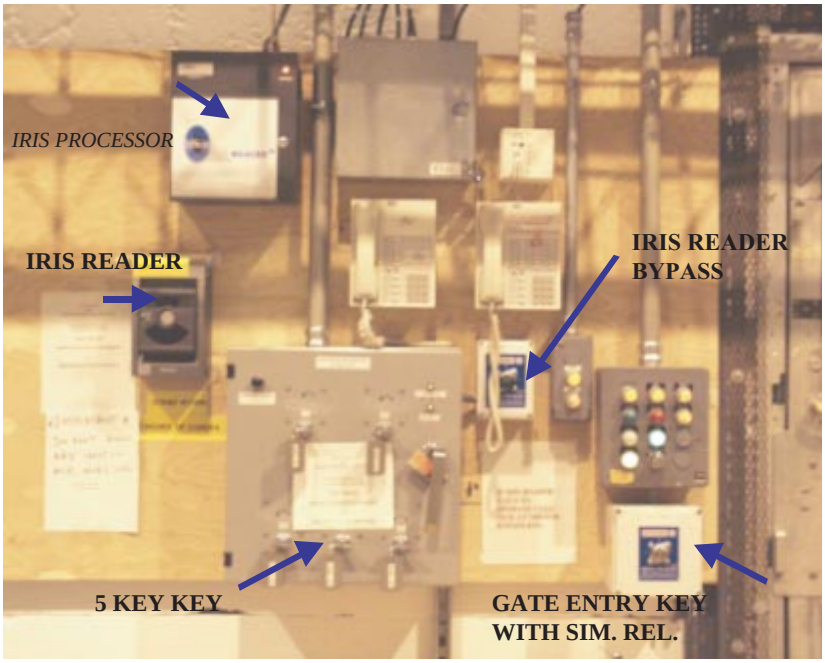
3.3 Advantages of Biometric System:

- Totally hands free. No contamination.
- Tremendously accurate.
- Not affected by eyeglasses or contacts.
- No laser as required by retinal scan.
- Identification happens in 2 seconds.
- CCD Camera is auto focus.
- No password or PIN to remember.

4. LESSONS LEARNED

- Micro-switches in the electric strikes were upgraded to improve the stability of the gate current loops. Gold-plated contacts provided better performance and reliability. In general, these switches are more compatible for the low current loops used in PASS.
- The MCR Panelviewer interface was re-designed to be user-friendlier. The operations staff contributed to the design.

NASA ACCESS CONTROL SYSTEM



PROTON RADIOGRAPHY

5. UPGRADES FOR FY2001 RUN

- During shutdown each of the 14 RF stations at 1004 A will have independent reachback system to PASS. This will give more flexibility and diagnostics to monitor the RF stations.
- A network will be installed at all the RHIC entry and GI gates card readers to a central server. This will enhance our ability to keep the personnel access status up to date. The card readers will query the server for training information of a requester to enter the ring.
- Local key trees will be installed at the experiments to enhance the access into IR regions.
- Hand recognition will be used to verify training and to log entries.

6. CONCLUSION

During the first year of RHIC running, the PASS system performed well. Some changes were required to improve the User Interface. The MCR operation staff contributed greatly to the changes that were implemented to improve the system user interface.

7. ACKNOWLEDGEMENTS

I wish to thank Roy Heyder, Jonathan Reich and Tom Tallerico whom contributed to the content of the paper.

References

[1] Robert Frankel, SAFETY SYSTEMS (WBS 1.12), RHIC Design Manual, January 1994.

SAFETY ISSUES IN ACCELERATOR OPERATION: GROUNDWATER CONTAMINATION

Peter F. Ingrassia
Collider Accelerator Department, Brookhaven National Laboratory, Upton, NY 11973 USA

Abstract
The Environment, Safety, Health, and Quality (ESHQ) is an integral part of how we do business at the Collider-Accelerator Department at the Brookhaven National Laboratory. Although the department has had a good track record with regard to safety, ground water contamination was observed in 1999 due to high intensity proton operations at the AGS. This paper will examine root causes and lessons learned from our experiences.

1. INTRODUCTION

Following the discovery, in 1997, of five Curies (Ci) of tritiated water contained in a plume emanating from the spent fuel rod storage pool at the High Flux Beam Reactor (HFBR), the Laboratory began an aggressive program to locate and characterise other sources of groundwater contamination. Four sources were found in the Collider Accelerator Complex. Three sources were associated with high intensity proton operation at the Alternating Gradient Synchrotron (AGS). One source was identified with the AGS internal beam dump known as the 'E20 Catcher'. Another other source was identified with chronic beam losses on one of the final quadrupoles (VQ12) in the beam transport used to bring protons from the AGS to the production target for the muon g-2 experiment. A third source was associated with the beam dump in the decommissioned neutrino beam line and will not be discussed here. The highest concentrations of tritium (^{3}H) and Sodium 22 (^{22}Na) in the vicinity of the E20 catcher were found to be 2 times and 1.75 times the drinking water standard respectively. The highest concentrations of ^{3}H and ^{22}Na in the vicinity of VQ12 were found to be 90 times and 0.15 times the drinking water standard respectively. The drinking water standard is 20,000 pCi/L for tritium and 400 pCi/L for ^{22}Na. The drinking water standard limits the internal dose to 4 mRem for an individual who annually ingests water (200 gallons ~ 800 litres) contaminated at a concentration corresponding to the standard. With regard to the problems at the HFBR, it is interesting to note that self-illuminated EXIT signs that generate light by taking advantage of ^{3}H decay, contain approximately 20 Curies of the isotope. A Curie is a measure of the activity or concentration of a radionuclide. It is defined as 3.7×10^{10} disintegration per second.

2. MECHANISMS

Iron, concrete, and soil are the primary shielding materials for radiological protection. Most secondary particles created by the interaction of primary protons with accelerator components will be stopped in the shielding. When a high-energy secondary interacts, a variety of radioactive nuclei are produced. The mass numbers of the atoms produced range from the mass of the target-plus-one down to a mass number of three (^{3}H). Most of the nuclei produced are short lived. The two longest-lived isotopes produced are ^{3}H and ^{22}Na with half lives of 12.3 and 2.6 years respectively.

Radioactive nuclei created in concrete and iron are, in general, not dispersible. On the other hand, radioactive nuclei created in soil may be dispersed by water. Sodium and hydrogen tend to form water-soluble compounds that tend to be dispersed. Figure 1 shows a section of the AGS tunnel, which represents a typical shielding design. The bold inner rectangle depicts the concrete tunnel. The inner trapezoidal shape shows a 'soil cement' shield that was added in 1989 in preparation for the

commissioning of the booster and higher intensity operation. The outer trapezoidal shape corresponds to the soil overburden. Rainwater seeping through the soil transports the radioactive materials in the soil downward to the water table. At the water table, the water flow again becomes horizontal, tending to transport the radionuclides in the direction of the laboratory boundary.

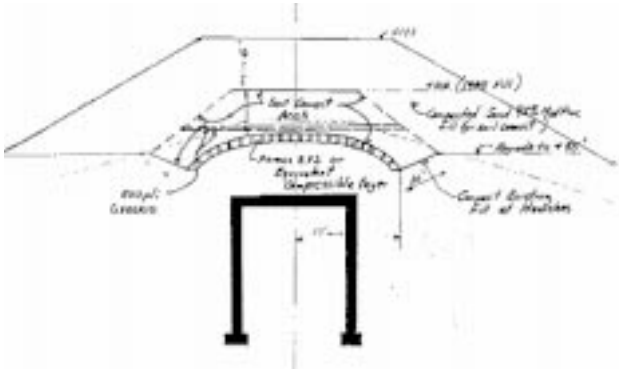


Fig. 1: AGS tunnel section view

The rate of migration of the nuclides is 0.75 feet per day. Given the migration rate, the location of the source two miles from the lab boundary, and the direction of groundwater flow, it would take in the order of two years for the radionuclides to reach the site boundary. Given the time scale, the concentration of radionuclides would be reduced when they reach the laboratory boundary owing to the radioactive decay of the nuclides and the continued influx of rainwater. Wells were drilled to map the extent of the contamination. The contamination was found to be confined to narrow plumes 20-30 feet across, approximately 40 feet underground, and in the case of the VQ12 plume, 250 to 300 feet long.

3. PAST OPERATIONS INVOLVING THE SOURCES OF CONTAMINATION

The catcher, at the E20 position in the AGS ring, was used as a beam dump from 1984 through 1999 when a new device was installed. E20 is a three-meter long block of tin-lead alloy (solder) with a beam tube at its centre. The device can be translated and skewed in the horizontal plane to minimise losses at injection. It was designed to accept any and all losses through the acceleration cycle including automatic or manual aborts of the circulating beam. It was not intended as, nor was it used as, a place to continuously dump particles. Operators were instructed to reduce the intensity of the circulating beam or to cease proton injection into the AGS rather than activate the catcher unnecessarily.

The quadrupole known as VQ12, part of the final focus for the muon g-2 experiment production target, was the source of the largest groundwater contamination problem that the Collider- Accelerator department has faced. The beamline optics were such that a beam position displacement at AGS extraction, was magnified by a factor of six at the downstream position of VQ12. The fact that ‘beam quality’ was only routinely monitored at the production target resulted in chronic beam loss at VQ12. One reason for the lack of beam quality monitoring was that new instrumentation was under development for RHIC and although intended for use during proton operation, its installation was delayed.

4. PRESENT OPERATIONS INVOLVING THE SOURCES OF CONTAMINATION

The E20 catcher has remained in the AGS ring. It has been positioned so that it intercepts none of the circulating beam. A new ‘beam scraper’ has been installed at the J10 position. An engineered solution has been employed to protect the groundwater. A gunite cap was placed over the soil at E20 and J10 to prevent rainwater from leaching ^{3}H and ^{22}Na out of the soil. During high intensity proton operations,

operators review the loss pattern at E20 to verify that they are minimal. Operators prevent the deliberate dumping of more than three pulses of high intensity beam anywhere in the AGS.

VQ12 is still an integral part of the beam transport to the production target. The beam optics were re-worked in 1999 so that changes in beam position upstream do not cause losses downstream. New loss monitors were installed and four were placed in the vicinity of VQ12. Operators regularly monitor the losses in the beam transport. A gunite cap was placed over the soil around VQ12.

5. CONCLUSION - LESSONS LEARNED

Given that losses are unavoidable, and the fact that soil is routinely used for shielding, it is no surprise that the soil shield became activated. What was a surprise was the fact that the activation had spread. The root cause for the problem was inattention to detail throughout the organisation. The lack of attention to detail made the situation at E20 unavoidable in that activation was present but we were not expecting it to spread. The VQ12 situation, in my judgement, could have been averted but again the lack of attention to detail played a significant role. The initial optics in the beam transport were off the mark. The lack of working instrumentation was a mistake. The inability of the operators to identify the loss was a disappointment but not a surprise. Given the lack of instrumentation the discovery of the loss would have been difficult. Operations management was at fault too. The procedures provided for the operators had them focusing on processes rather than on positions along the beam path – hence their focus was diverted from the problem area.

A number of lessons were learned from our experiences and the lessons have had an impact on accelerator operations. Foremost in our education was the fact that operators must posess a greater awareness of the environmental impact of accelerator operation. Knowing that some beam losses are unavoidable, we learned to cover soil used as shielding wherever loses are expected in the chain of accelerators. We have learned to confirm assumptions made during the design phase regarding soil activation adjacent to new beam lines by conducting soil activation measurements.

Operators in the MCR have learned to do business differently. The Operators routine includes monitoring of beam losses at critical locations during high intensity proton operations. The routine monitoring is prescribed by formal procedures. We have learned not to rely on one instrument to determine beam quality; beam loses must be considered as part of the ‘quality equation’. ‘Watchdog’ software is used to generate alarms when high losses are experienced at critical locations, or during prescribed segments of the acceleration cycles in the Booster, the AGS, and the external beam transport. Critical to many of our lessons is the changed behaviour of the Operators. They have learned to react as required and to be proactive to prevent losses where possible.

6. ACKNOWLEDGEMENTS

The author wishes to acknowledge and thank Edward T. Lessard the Associate Chairman for ESHQ in the C-A Department and Gary Schroeder of the Environmental Services Division and Bet Zimmerman the Environmental Services Division Manager at BNL for their valuable assistance in the preparation of this work.

OPERATIONS AT CERN UNDER INB REGULATIONS

André Faugier
CERN, Geneva, Switzerland

Abstract
The CERN high energy accelerators are classified as INB ('Basic Nuclear Installations') under the French legislation. The rules and regulations governing such installations will first be exposed in general terms. The consequences and constraints for accelerator operations will then be reviewed, particularly the needs for documentation in and around the control room (logbooks…), the requirements for written procedures, the operation of the access system and the possible conflicts of interest.

1. INTRODUCTION

Founded in 1954, the CERN laboratory is located accross the French-Swiss border, near Geneva. About 70% of the two largest accelerators of CERN (LEP/LHC and SPS) are located on french territory.

In 1984, a convention has been signed between CERN and the French government, where by the organization agreed to take the necessary steps to guarantee the safety of the installations of the LEP machine, according to modalities submitted to the approbation and the control of the French authorities.

In July 2000, a new convention has been signed, concerning the LEP dismantling, the new LHC collider under construction in the LEP tunnel, the SPS machine and its transfer/injection lines including the future CNGS (neutrino to Gran Sasso), and their associated infrastructures, both underground and on the surface, within a perimeter precisely defined by a set of plans.

2. THE INB CONTEXT

The signature of these conventions assimilates the installations to an INB like French nuclear reactors or installations for storage of radioactive materials.

The others CERN accelerators which are located on Swiss territory are not presently concerned.

2.1 Control of the installations

The nuclear safety authority (DSIN) controls these installations. The nuclear safety authority (DSIN) itself comes under the authority of the French government environment and industry departments.

On the Swiss part of CERN installations, the control is exerted by the Federal Office of public health (OFSP).

2.2 Organization of the INB structure at CERN

A lot of important and varied studies are requested by the authorities; this in turn implies an important documentation effort. The present structure which deals with these activities includes:

- one INB coordination unit which ensures the permanent link with French authorities and coordinates all the related work (report writing and associated studies) – 1 FTE
- one 'AQ-INB' unit which ensures that all INB activities are in accordance with quality assurance criteria – 0.5 FTE
- a group of about 20 correspondents in the divisions, mainly from the Technical Inspection and Safety division (TIS) and the accelerator sector – ~ 8 FTE.

3. CONSEQUENCES AND CONSTRAINTS

3.1 Specific systems or activities of the INB

In the accelerator domain, INB regulations emphasize on specific systems or activities called important elements for safety (EIS). The accent is put on the radioprotection, on the access system, on the alarms, on the waste treatment and disposal channels, on the traceability; these activities must follow quality assurance rules and are submitted to a careful control.

3.2 Zoning

A justified a priori ‘zoning’ of the installation must be established; the entire perimeter of the INB must be decomposed in conventional and nuclear zones.

In a nuclear zone, the materials waste produced is radioactive or susceptible to be so.

In a conventional zone, the waste produced is conventional.

3.3 Traceability

Every equipment leaving or entering the INB perimeter must be traced as long as it exists, which implies that a somewhat heavy infrastructure has to be to set up.

4. CONSEQUENCES FOR OPERATIONS

4.1 EIS

As previously mentioned, both design, construction and operation of these systems must follow quality assurance rules. Every incident, abnormal event, modification or anomalies treatment must be clearly documented and recorded. Some of these, according to the nature or the impact (personal safety or environment) must be reported to the authorities.

4.2 Operations

Concerning machine and access operations, clear written procedures must be established. The definition of a precise zoning of the installation is generally not done by the Operations. Nevertheless, Operations is strongly involved for the following considerations:

- the nuclear zone must be precise and rather minimized because it is not presently possible to declassify a nuclear zone in a conventional one; the opposite is possible once duly justified;
- the nuclear waste disposal channels are very expensive and necessitate a very heavy work: complete inventory of the radionucleides in the radioactive waste, conditioning to minimize the cost;
- moreover, safety is prevailing on efficiency and doses to the persons involved in nuclear materials handling must be minimized (ALARA).

For these reasons, Operations has rather to think in terms of minimum beam losses, minimum induced radioactivy, localised and well explained beam losses, clean operating conditions and clean ‘intensity records’. Enough resources must be put in an efficient and reliable beam diagnostic system which includes a complete recording of detailed transmission efficiencies/losses, coast data, recording of beam loss data, loss patterns. The logbook has an important role to play here: precision of the information (time stamp), clear documentation of the events or operation mode changes.

The potential advantages of such an approach are numerous, among them can be mentioned:

- easier anomalies treatment and reporting
- easier justification of the zoning redefinition
- cheaper radioactive waste disposal

5. CONCLUSION

CERN has signed conventions with the French Government in which we agree that certain of our facilities become classified as INB.

In the convention, we have agreed to abide by the regulations and statutes concerning INB, this is to guarantee the safety of the operations of the installations through modalities submitted to the approval and the control of the French authorities.

Finally, INB rules compel us to work within a quality assurance frame and therefore ask us to do all efforts to even better master the accelerator Operations.

ASPECTS OF OPERATIONS AND DOE REGULATION OF ACCELERATORS AT FERMI NATIONAL ACCELERATOR LABORATORY

Daniel A. Johnson
Operations Department, Fermi National Accelerator Laboratory, Batavia, IL USA
Pepin T. Carolan
U.S. DOE Fermi Area Office, Chicago Operations, Batavia, IL USA

Abstract

Fermilab is a U.S. Department of Energy (DOE) high energy physics research facility, which operates under the requirements and regulations of DOE facilities. The Beams Division Operations Department is responsible for safely and efficiently operating the accelerators. As a Federal Agency with oversight responsibility, DOE issues a range of guidance, directives and regulations for its contractors to consider or follow in their operations. Operations organizations generally see such DOE regulation in the form of limits, procedures, etc., while others take responsibility for the broader interpretation and labwide implementation of DOE requirements. Over ten years ago, DOE issued Order 5480.19 titled the 'Conduct of Operations Requirements for DOE Facilities.' This order directly impacted the Operations Department. Its implementation led to the creation of an 'Operations Department Conduct of Operations' (no longer required), which is kept updated and still in use today.

We will give an overview of DOE regulation at the laboratory, as related to accelerator operations. We will also talk about the initial worries of the Conduct of Operations and describe how it was made to work at Fermilab. This will hopefully encourage other discussions and encourage the concept of taking credit for things we do 'right.'

1. INTRODUCTION

Fermi National Accelerator Laboratory is operated under contract by Universities Research Association (URA) for the Department Of Energy (DOE). The contract governs how the facility will operate and provides performance criteria for gauging success. The performance criteria are negotiated annually, while the contract is typically maintained over a five-year time frame. The contract includes performance criteria for things like 'number of lost work days,' 'hours of operation,' 'integrated luminosity,' 'collective radiation dose,' etc. The contract also includes the set of all Environment Safety and Health (ES&H) 'standards' that govern both accelerator operations, and work in general at the laboratory. This set is know as the 'Work Smart Standard' (WSS) set and includes State, Federal and DOE regulations, and directives as well as governmental and professional consensus standards. In addition to what is in the contract, other DOE directives and guidance can be applicable to accelerator operations at the laboratory. Some of these DOE directives are geared more toward, or are analogous to, 'nuclear' operations and 'nuclear' facility requirements. A few of the DOE directives and regulations are discussed here from some accelerator operations aspects. The DOE WSS process is an approved method of selecting applicable standards and regulations via peer-review, analysis and consensus.

2. SOME REGULATIONS AND ORDERS AS SEEN BY OPERATIONS

- **DOE Order 420.2**

Safety of Accelerator Facilities

This order calls for identification and analysis of potential hazards and impacts, ensuring training and qualification of personnel, and adherence to written procedures to maintain safe operations. The objective is to prevent injuries and illnesses associated with accelerator operations. Used in conjunction with other ES&H requirements. [1]

Fermilab implements key elements of the Accelerator Safety order via an internal WSS standard called, 'Planning and Review of Accelerator Facilities and Their Operations.' The implementation of this order and guidance shows up in a number of different ways in the Operations Department. A Safety Assessment Document (SAD) and DOE approved Accelerator Safety Envelope (ASE) are required. These documents link to operations in matters like beam intensity limits/operating parameters, access conditions, radiological, occupational and life safety hazard controls, procedures, shielding requirements, training, safety system tests, and other areas. A section of the order implementation guidance deals directly with control room shift operations in the categories of: Organization and Administration, Shift Routines and Operating Practices, Control Room Activities, Communications, Operations, Conduct of Research and Development, and Status Control of Equipment and Systems. Each of these is covered in the Conduct of Operations to be discussed later. DOE 420.2 can be found at: http://tis.eh.doe.gov/portal/policy.html (select DOE Directives, Current DOE Directives, New Series Directives, 400 Series.) Additional information and guidance for Accelerator Safety can also be found at: www.sc.doe.gov/production/er-80/er-83/accelr8r.html

- **DOE Order 232.1A**

Occurrence Reporting and Processing of Operations Information

Keeps DOE and others informed of occurrences at the facility that could adversely affect security, the health and safety of the public, environment, laboratory purpose, etc. [2]

The implementation of this order puts the Operations Department into two different roles, either the role of responder or data collector. Depending on the type of occurrence the operators may be able to control the device, system, accelerator, or provide support to prevent further loss, damage, or potential hazard, etc. The Operations Department may also be required to provide documentation, graphs, plots, or other information on the events leading to and status of machines/systems at the time of the occurrence. Depending on the occurrence, the analysis of the occurrence may also result in changes in practices or procedures for operations. More information on DOE Occurrence Reporting, including Public access to all final, non-sensitive occurrence reports since 1990, can be found at: http://tis.eh.doe.gov/oeaf/orps.html

- **10 CFR 835**

Occupational Radiation Protection

This is part of the Code of Federal Regulations (CFR) and sets the standards and requirements for occupational radiation protection. This document incorporates guidance from both the National Council on Radiation Protection and Measurements (NCRP) and the International Commission on Radiological Protection (IRCP). [3]

To ensure compliance with this mandatory Federal rule, a DOE-approved 'Radiation Protection Plan' was implemented by the laboratory Environment Safety and Health (ES&H) groups, and its implementation can also be impacted by accelerator operations. For example, the operators control the particle beam. If not properly tuned, beam losses can result in higher than necessary residual radiation in the accelerator enclosures and tunnels. This impacts the area radiological postings, protective clothing, training, and other access requirements. The operators also control access to accelerator

enclosures and require workers to sign the appropriate Radiation Work Permits (RWP's), check verification of worker training, provide some of the required protective or other equipment, and enforce other requirements for access.

Operators must also frequently enter the areas for various reasons including search and secure, and therefore ensure their own adherence to all radiological safety requirements. More information on DOE Occupational Radiation Protection can be found at: http://tis.eh.doe.gov/whs/rhmwp/

- **DOE Order 5480.19**

Conduct of Operations (CONOPS) Requirements for DOE Facilities

This DOE order provides standards to improve the quality and uniformity of operations at DOE facilities. This can include any industrial, research, testing, or production activity. [4]

Sometime around 1985 the Institute of Nuclear Power Operations (INPO) released order '85-017 Guidelines for the Conduct of Operations at Nuclear Power Stations.' It was modified and updated somewhere around 1988. It was an eighteen-chapter document, where each chapter dealt with a specific aspect of operations. Late in 1989, the DOE decided to implement a Conduct of Operations program to improve the quality and uniformity of all its facilities. The INPO document was given as an example and DOE standards were expected to closely follow it. At first pass, the implications to accelerator operations looked extremely onerous. Fermilab was not a nuclear facility and didn't want to be treated as one. After the initial shock, each chapter was examined and mapped into accelerator operations. The first versions of the Conduct of Operations for Fermilab were released in late 1989 and early 1990. As it turned out, many of the guidelines were actually being followed by operations. In some cases things were already being done in practice and only needed supporting documentation. After reviewing each chapter, it made sense to put down in writing how the Operations Department does business. This proved to be useful for new employees and audits alike. A few years ago the laboratory, under 'Necessary and Sufficient' and currently under the 'Work Smart Standards' program, decided that the Conduct of Operations was no longer explicitly contractually required. However, employees found it useful. We recently updated it and asked our department employees to reread it. As you will see some of the guidelines in the Conduct of Operations also fall in line with the 'Safety of Accelerator Facilities' mentioned above. In fact, all of the above orders and regulations are tied into the Conduct of Operations. I will briefly describe each chapter and you should be able to see the importance to operations from within and outside the group. The DOE CONOPS order can be found at: http://tis.eh.doe.gov/portal/policy.html (select DOE Directives, Current DOE Directives, Old Series Directives, 5400 Series.) Additional standards and supporting guidance (largely geared toward 'nuclear' facilities) can be found at: http://tis.eh.doe.gov/techstds/standard/appframe.html (Document Number Range 1001-2000).

I – Organization and Administration

This chapter covers the department makeup. It describes the job description of different members of the department and their responsibilities. This chapter also includes things like policies, how to monitor performance, accountability, management training and planning for safety.

II – Shift Routines and Operating Practices

This chapter covers the way shifts are run and standard practices. Things like: how to get status reports, respond to status indicators, reset protective devices, and keep the control room civilized; making operator rounds/tours with inspection sheets (e.g. readings for a system that does not have a remote readback), who has the authority to control equipment and from where, and what standard safety practices are used.

III – Control Room Activities

This chapter sets the stage for acceptable control room activity, materials, and equipment control. This chapter also suggests limiting operator activities to those related to machine operation, to limit distractions caused by working on other projects while assigned to the control room.

IV – Communications

This chapter deals with good communication practices. The use of acronyms, radio/telephone communications, and transfer of instructions to the crew are covered. The proper use of emergency and public address systems are also discussed.

V – Control of On-Shift Training

One of the most pressing issues is training new operators. This chapter discusses the training program, instructor qualification, control of trainees, and assistance from trainees. Also discussed are the number of trainees per trainer, training documentation, approval, and suspension of training in certain situations.

VI – Investigation of Abnormal Events

This chapter covers the occurrence of an event from recognition through completion and trending. It also ties in the reporting requirements of DOE Order 232.1 mentioned earlier.

VII – Notifications

This chapter sets up standards for timely notification of personnel. We must ensure responsive notification of ES&H concerns. Information must be gathered and transferred in a systematic, controlled method. An example of this would be in our safety procedures. A periodically reviewed call-in list is used to make sure proper people are notified. (This chapter tells how things are set up and is not the actual call-in list.)

VIII – Control of Equipment and System Status

This chapter covers the work on equipment/systems and their return to service. The equipment/system must be verified and sometimes certified by operations in the form of a prescribed test. The importance and need for accurate status indicators is also important.

IX – Lockouts and Tagouts

This chapter covers the aspects of the laboratory lockout and tagout procedure. Lockout/tagout requires a separate training course before use is authorized.

X – Independent Verification

As mentioned earlier, equipment and systems returned to service must be verified as functional. A device may have to be in the correct configuration, value, or position. It is important to have independent verification.

XI – Logkeeping

This chapter covers the requirements of logkeeping. We currently use an electronic logbook. It provides a timestamped, legible, and easily searchable record. It cannot be easily changed, but is accessible remotely. A hardcopy is printed for use during shift change.

XII – Shift Turnover

This chapter covers the guidelines for a thorough and proper shift turnover. It identifies use of checklists, document review, and individual turnover.

XIII – Operations Aspects of Facility Chemistry and Unique Processes

This chapter does not directly apply to our operations. It mainly deals with the monitoring of plant chemistry data and parameters (e.g. failed reactor fuel systems, systems employing or storing hazardous and radio-chemicals and gases, corrosion problems, toxic waste systems). Such systems are generally not a part of accelerator control room operations, or if similar systems do exist, are not generally monitored by main control room personnel. This chapter also generally stresses the importance of monitoring, control, and good communications with the technical support groups.

XIV – Required Reading

This chapter covers the use of required reading. It includes acknowledgement of completion, review, and documentation. Procedures classified as 'required reading' must be read, understood, and signed. Any questions on these procedures can be directed to supervisors. The CONOPS manual would also be another example.

XV – Shift Orders

This chapter describes the way to communicate short-term information and instructions to the operating crew. It protects the crew from external requests and distractions. The format content, review, and removal of old orders are discussed. Shift orders for the weekend crews, are frequently entered into the electronic logbook by the Operations Department Head or designee. Since it is a logbook entry, it is dated, signed, reviewed at briefing, etc.

XVI – Operations Procedures

This chapter discusses the use of procedures mainly for safety-related issues during operation. The topics covered are procedure development, content, changes, review, availability, and use. We have several types of procedures: Administrative, Safety, and Emergency Response. Each may have different levels of review and approval. An example of an Emergency Response procedure would be 'Flammable Gas Emergency Response Procedure.' They are written in flowchart format to make them more portable and easy to read.

XVII – Operator Aid Postings

This chapter provides guidelines for the proper use of operator aids. A piece of paper taped to the console, isn't good enough. Operator aids should be developed, reviewed, approved, and documented. Temporary directions on how to reset a unique device may be documented and displayed in the control room provided the proper format is used and approval given.

XVIII – Equipment Labeling

This chapter covers the use of devices labels. A good labeling program provides consistency and promotes better communications. Some of the important points of this topic are label information, placement, removal, and replacement.

3. CONCLUSION

Our main goal is to safely and efficiently operate our accelerators. We all have to deal with orders, rules and regulations. The degree of impact varies, but can usually be traced to a procedure, response, limit, etc. At first, some regulations/orders may look overwhelming and contradictory to the goals. As mentioned, the Conduct of Operations and its association with nuclear facilities initially caused concern. In most cases, given a chance to break down and implement them on our own terms, such orders and regulations can be turned into something useful and maintainable.

References

[1] Safety of Accelerator Facilities, Department of Energy, DOE Order 420.2. http://tis.eh.doe.gov/portal/policy.html (select DOE Directives, Current DOE Directives, New Series Directives, 400 Series.).

[2] Occurrence Reporting and Processing of Operations Information, Department of Energy, DOE Order 232.1: http://tis.eh.doe.gov/oeaf/orps.html

[3] Occupational Radiation Protection, Code of Federal Regulations, 10 CFR 835. http://tis.eh.doe.gov/whs/rhmwp/

[4] Conduct of Operations Requirements for DOE Facilities, Department of Energy, DOE Order 5480.19. http://tis.eh.doe.gov/portal/policy.html (select DOE Directives, Current DOE Directives, Old Series Directives, 5400 Series).