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.