EUROPEAN LABORATORY FOR PARTICLE PHYSICS
LABORATOIRE EUROPEEN POUR LA PHYSIQUE DES PARTICULES

CERN-ST-99-034
February, 1999

RECOMMENDATIONS FOR THE LHC SAFETY ALARM SYSTEM

H. Laeger

Abstract

A working group was set up to define the LHC safety alarm system, also known as *Alarm-of-Level-3-System (AL3S)*. The mandate asked for recommendations to be elaborated on four items: the overall concept of the *AL3S* for machine and experiments, the transmission and display of safety alarms, the *AL3S* during civil engineering construction, and the transition from the present LEP to the final LHC safety alarm system. The members of the working group represented a wide range of interest and experience including the CERN Fire Brigade, safety officers from experiments and machines, and specialists for safety and control systems. The recommendations highlight the need for a clear definition of responsibilities and procedures, well-engineered homogeneous systems across CERN, and they point to several important issues outside the mandate of the working group. These recommendations were presented, discussed and accepted by several CERN and LHC committees.

Presented at the 2nd ST Workshop
Chamonix, France, February 2 - 5, 1999

1 INTRODUCTION

Obliged to build and to operate the LHC as an *Installation Nucléaire de Base (INB)*, a working group *LHC Alarms-of-Level-3-System (WG-AL3S)* was initiated by the *INB* liaison officer and the LHC project leader in January 1998. This working group had as its mandate four chapters relating to Safety Alarms, a more general term of *Alarms-of-Level-3*, as defined in the TIS Safety Instruction *SI 37*:

- the overall concept of the *Alarm-of-Level-3-System* for the LHC machine and experiments
- the redundant transmission and the visual display of *Alarms-of-Level-3*
- the alarm system during the civil engineering construction phase
- the transition from the present LEP to the final LHC safety alarm system.

The membership in the *WG-AL3S* was discussed with the Technical Coordinators and the Division and Group Leaders of all the experiments and divisions concerned by these safety issues. Thus, very competent and committed members with a large variety of experience formed this working group, including representatives from TIS and CERN's Fire Brigade, experimental and divisional Safety officers *(GLIMOS, DSO)*, control system specialists, as well as legal advisors.

The *WG-AL3S* took into account the experience gained with safety systems, both inside and outside CERN. In particular, LEP experience was thoroughly analyzed, and visits were made to the Geneva and Paris airports and to Eurotunnel. Many international and national Standards were also carefully considered.

Three distinct recommendations for the safety alarm systems for LHC have been formulated by the working group: those concerning the civil engineering work sites, the transition from LEP to LHC and finally, the main document treating the overall concept and redundant transmission. All items of these recommendations will be briefly presented here; and a few selected ones will be discussed in some detail.

2 THE SAFETY ALARM SYSTEM FOR THE CIVIL ENGINEERING WORK SITES

When elaborating the recommendations for the safety alarm system for the civil engineering work sites, the *WG-AL3S* had to consider that the responsibility for safety on these work sites lies with the contractors, but that CERN's Fire Brigade is to be called for emergency and rescue interventions. The standard *Red Telephone* is installed all over CERN's premises and offers an adequate means for emergency calls. Every *Red Telephon*e establishes two diversely redundant transmission paths to the *Safety Control Room (SCR)* of the Fire Brigade. One uses the normal telephone exchange system and connects directly to dedicated telephone sets in the *SCR*. The location of the *Red Telephone* emitting the emergency call is indicated on these sets, permitting the Fire Brigade to localize the caller, even if the latter is not able to do so himself. Every emergency call is recorded in the *SCR* for further analysis, if required. For the second transmission path, the existing *Alarm-of-Level-3* system is used. This system transmits an *Alarm-of-Level-3* to the *SCR*, indication on a synoptic display panel the safety zone where the call is originating, and showing its detailed location on a video screen display. All instances of *Alarms-of-Level-3* are recorded in a database and are available for later retrieval and analysis.

The *WG-AL3S* recommended the installation of *Red Telephones* on every civil engineering work site. CERN management has accepted this and put ST/CE in charge of implementing the recommendations. The details of number, location, connection points, period of availability, testing etc are to be agreed by the contractor, CERN's Fire Brigade, ST/CE, and ST/MC. These recommendations are valid during the civil engineering construction periods, probably through the years 1998 to 2003.

3 TRANSITION FROM THE LEP TO THE LHC SAFETY ALARM SYSTEM

The dismantling of LEP and the installation of LHC in the surface buildings and the underground caverns and tunnels represents a complex combination of parallel and successive works spread over time and in space. We will see a very dynamic evolution of safety zones, with changing risks and consequently with changing requirements for safety alarm systems. It would be pretentious to want to define several years in advance detailed recommendations for safety systems during this transition phase, for risk situations, which can not be evaluated with sufficient accuracy at present.

The *WG-AL3S* therefore, recommends that the people in charge of LEP transformation and of LHC installation be designated responsible for all related safety issues. These people, the Project and Group Leaders for the machine and the Technical Coordinators for the Experiments, shall be assisted by the Safety Officers of the divisions and the experiments concerned, and TIS shall advice.

Together, they shall ensure that risks are properly evaluated for every area and that minimum requirements for safety systems and alarm transmission are defined. The implementation of these requirements is then the task of ST/MC, which has to make all the provisions and to take all the necessary actions throughout the transition period. The need may occur for the installation of provisional safety alarm systems and alarm transmission for specific areas and for limited periods. It is expected that the transition period will start in 2000 and end in 2001.

4 THE LHC SAFETY ALARM SYSTEM

4.1 Experiences with Safety Alarm Systems

The *WG-AL3S* examined the present installations of safety alarm systems, related emergency procedures and experiences of the users. The experience over the past decade with the LEP machine and experiment provided essential input for specific user requirements. Very valid insight was also gained through the visits made to the Geneva and Paris airports and to Eurotunnel. Furthermore, a thorough search for relevant standards revealed a large amount of codified experience, which had not been sufficiently exploited at CERN for past installations of safety alarm systems and associated procedures. The essential elements of the recommendations of the AL3S working group are derived from the analysis of the user experiences with present installations and from relevant standards.

4.2 Responsibilities

Experience with LEP has clearly revealed shortcomings due to fragmentation of responsibilities. In the extreme case, there have been up to five different divisions involved in the design, installation and maintenance of safety alarm systems in one single experimental

cavern. All kind of shortcomings resulted from this: from waste of resources due to duplication in work, over non-homogeneous technical solutions, reduced performance to multiple technical and human interfacing. One of the major recommendations of the *WG-AL3S* addresses this point, stipulating that the responsibility for the entire LHC safety alarm system for machine and experiments should be with one unique service, and that adequate resources should be made available to this service for the required high quality of work. CERN management has very rapidly implemented this recommendation by giving the responsibility for implementation to the ST/MC group, to be done in close collaboration with TIS and the safety officers and group leaders in the divisions and experiments concerned.

4.3 Homogeneity and Global Approach

CERN's Fire Brigade, the main actor in case of emergencies, needs to be informed of safety alarms in exactly the same manner, from wherever these alarms originate and by whatever techniques they are detected and transmitted. It is, therefore, recommended that a unique and homogeneous concept of safety alarm systems, transmissions and displays be introduced for all CERN premises, accelerators and experiments. This means that the safety alarm systems, which will be introduced for the LHC machines and experiments, shall also be applied progressively to all other installations at CERN.

The *WG-AL3S* also recommends that during the process of design and implementation the safety-case shall be considered globally. This means in particular that the operational and maintenance interdependencies of the safety alarm system with other important systems, such as the controlled access, the radiation safety, or accelerator and experiment controls shall be thoroughly evaluated.

4.4 Engineering Methods and Technology

Two points of the recommendations address engineering methods and new technology. Rigorous modern and methodical engineering practices should be applied throughout the life cycle of the project. In particular, for domains such as project management, acceptance testing, documentation and training, improvements with respect to past practices are most desirable. Concerning the choice of technologies, the *WG-AL3S* recommends the use of state-of-the-art digital technology for the transmission of safety alarms. This implies for example that a computer system, conceived for the safety case, or multiplex telephone technology are acceptable, and implicitly, that hard-wired transmission is not. It is also important that if new technology is chosen, the installation of pilot systems and very thorough field-testing are required. It is conceivable to use one of the Meyrin site safety zones, which needs adaptation, as a pilot installation before large-scale implementation for the LHC machine is started. The present trend to integrate proven industrial equipment, rather than developing CERN specific equipment, should be enhanced.

4.5 Standards

There exist a large number of international and national standards related to safety alarm systems and to safety alarm transmission systems. Recently also several standards dealing with the use of computers for safety related systems have been emerging. It is surprising to what extend CERN has in the past neglected to make good use of such

standards, which in fact represent a codified rich experience in the field. The *WG-AL3S* has conducted a wide search on relevant standards and listed a dozen of them for careful consideration.

5 TECHNICAL RECOMMENDATIONS

5.1 Safety Zones

Presently, the CERN premises, accelerators and experiments are divided into *Safety-Zones*. There are a total of 36 of these zones and all of them have a *Local-Alarm-Display*, indicating the type and the location of safety alarms. This concept shall continue and every *Local-Alarm-Display* shall be situated within the *Safety-Zone* concerned.

5.2 Redundancy

One of the most important elements of the technical recommendations is the request for two completely independent and diversely redundant, dedicated alarm transmission systems. The meaning of "diversely redundant" is that different technologies shall be used for the two systems. Both systems shall be designed and installed such that the risks of common mode failures are reduced to the minimum. In addition, both systems shall be permanently and automatically supervised for correct functioning. The Interface diagram of figure 1 shows the overall context of the two systems, their relation to each other and to other systems and the peripherals.

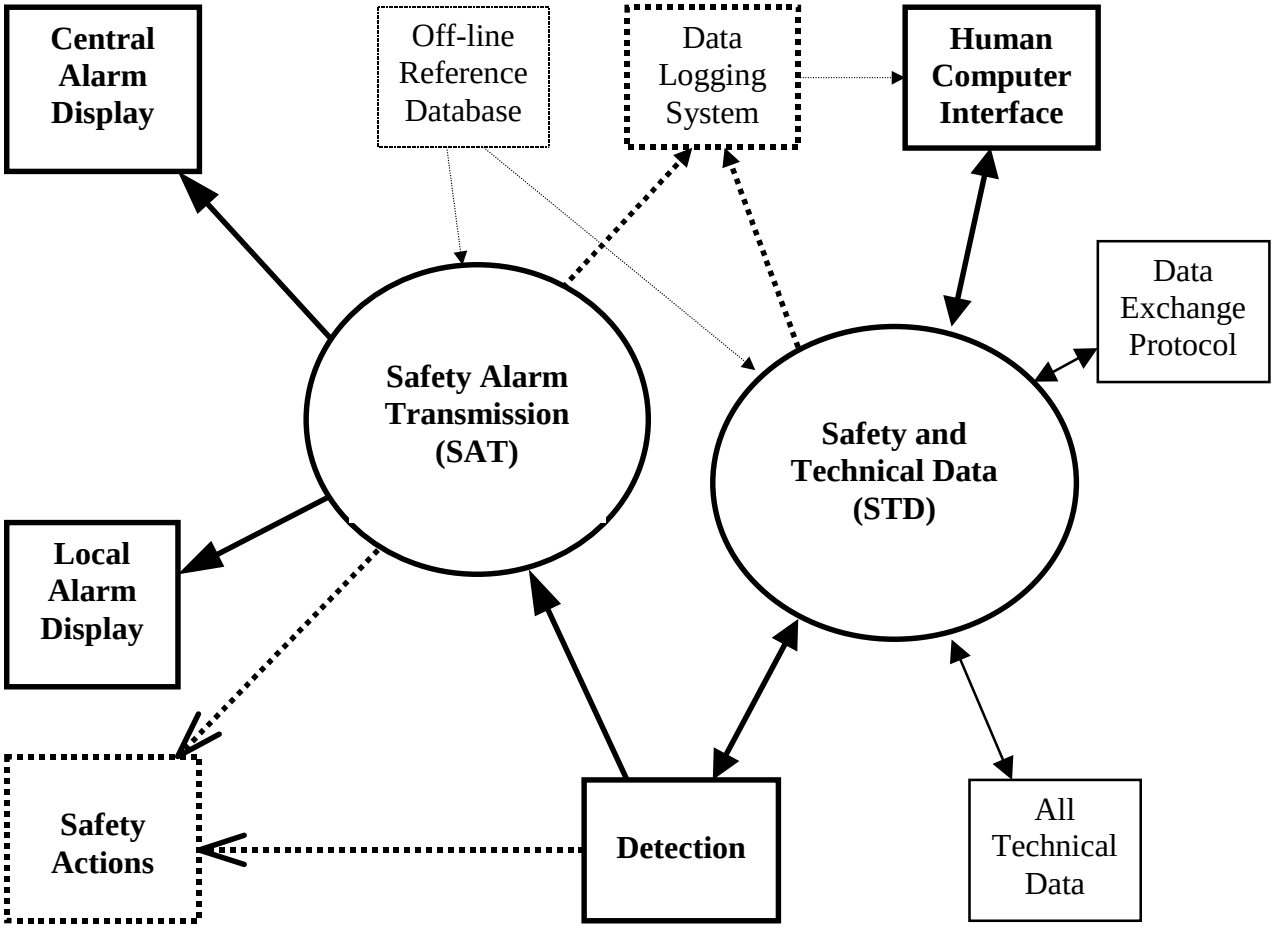

Figure 1: Interface Diagram of the LHC Safety Alarm System

Both systems, the *Safety-Alarm-Transmission system (SAT)* and the *Safety-and-Technical-Data system (STD),* carry sufficiently detailed information on the type and location of the safety alarms that the Fire Brigade can decide on the action to be taken even if one of them is not available.

5.3 Safety-Alarm-Transmission (SAT)

The *SAT* only transmits safety alarms and technical alarms related to the detection and transmission of these alarms, with the exclusion of any other alarm or information not related to safety. The information is primarily intended for the Fire Brigade *(FB),* i.e. CERN's alarm-receiving center responsible for emergency and rescue actions. The Technical Control Room *(TCR)* has a double back-up function with respect to safety alarms: firstly to be usable by the *FB* in case their Safety Control Center *(SCR)* should not be available, and secondly to accompany the *FB*'s safety actions with possible technical actions. Therefore, all *SAT* information shall be displayed identically and redundantly in the *SCR* and in the *TCR*.

For the alarm detection, transmission and display, industrial products approved for the safety-case shall be used. The request for detailed information on the type and location of every safety alarm to be displayed, excludes for the LHC the use of the present CERN technology, i.e. electro-mechanical relay systems and hardwired cabling. Instead, an industrial fieldbus as implemented at the two visited airports, or a multiplex system as used for telephone communications can be considered. A detailed evaluation of these and other possible technical solutions is required, including thorough field-testing and pilot installations.

In many situations, safety alarms need to trigger safety actions automatically, like for example a gas leak needs to have the gas supply cut very rapidly in order to prevent the risk of explosion. For these kinds of automatic actions, the equipment most suitable and closest to the detector shall communicate directly with the appropriate actuator. Here, the distances being short, the communication may be via local fieldbus, or via hardwired contacts. A specific request from the experimental physicists is that the alarm detection equipment in experimental zones shall be capable of providing hardwired signals for use by the experiments.

5.4 Safety and Technical Data System (STD)

The *STD* transmits all detailed information on safety alarms as well as all detailed technical alarms, equipment states and data for the entire technical infrastructure of CERN. This technical infrastructure may include systems such as electric distribution, cooling, ventilation, air conditioning, cryogenics, vacuum, and naturally all safety systems. This system is primarily intended for the *TCR,* but also for the *SCR* and other users, such as accelerator control rooms or the equipment specialists. At LEP, the control system for the technical infrastructure is common with that of the accelerator. This causes many operational shortcomings and problems. The basic requirements for the control of classical technical systems are also different from those for accelerators. Technical systems require a very high degree of reliability, transmission time is not a major concern, whereas accelerators need to transfer large amounts of data with high speed. Therefore, the working group has

recommended that for LHC the *STD* shall be independent from the control systems used for the accelerator and the experiments.

5.5 Data Exchange with Other Control Systems

In LEP a major operational shortcoming is that data exchange between different control systems was not designed from the outset and could never be satisfactorily implemented afterwards. There are many technical, accelerator and experimental slow control systems or subsystems whose correct or optimal operation depends on other systems. It is, for example, important for an experiment to have information on cooling conditions as supplied by the cooling water or the air conditioning system. Following one of the recommendations of the working group, the CERN Control Board has set up a working group to define a common data exchange mechanism between all LHC control systems. The STD shall be designed so that it is capable of implementing the forthcoming data exchange protocols. It appears that the Technical Data Server (*TDS*) implemented by the TCR in recent years has already the basic essential features for data distribution to subscribers. This *TDS* concept and probably even its present implementation are considered a good elements for the *STD* and data exchanges with other systems.

5.6 Reference Database and Data Logging

For the present technical installations at CERN, there are control systems that have no systematic description of their process, equipment or control parameters in a database. Operation and in particular maintenance of such systems is difficult, inefficient and full of errors. Well-designed, systematic, consistent and complete reference databases are a must for efficient control systems. It is recommended to have one common reference data base for both alarm transmission systems, the *SAT* and the *STD*.

An essential requirement from control room operators, but even more from equipment specialists is to be able to make historical analysis of system behavior and of special events. Data logging is common practice for computerized control systems nowadays and a common data logging system shall be implemented for *SAT* and *STD*. This data logging system shall allow efficient logging, retrieval, treatment and display or export of all data transmitted via *SAT* and *STD*.

These two recommendations are a challenge for the design engineers, as this requires additional interfaces between SAT and STD that are to be independent and redundant systems.

5.7 False Alarms

False alarms represent major problems for the *SCR* (Fire Brigade) and *TCR* operators. The *WG-AL3S* recommends serious efforts to be made during all stages of specification, design, implementation, testing and maintenance to avoid false alarms of any level. This request clearly concerns sensors, detectors and alarm systems, but also all process systems and equipment, as false alarms will hide real alarms and will lead to inappropriate actions by the operators. The matter of false alarms being very badly handled in present technical installations at CERN and needing to be substantially improved, the contribution by M. Batz is dedicated specifically to this subject [1].

6 ADDITIONAL WORKING GROUPS

During it's half year of animated discussions, the *WG-AL3S* came across subjects which have close relations with the LHC Safety Alarm System, but are somewhat outside its mandate. The working group, therefore, formulates several recommendations for the attention of the CERN management, which all require, in one form or another, additional working groups to be set up.

6.1 Risk Analyses and Alarm Systems

Technical working groups should be set up to analyze risks, and to define sensors, detectors, installations and actions best suited to the expected risks. All LHC experiments and the LHC tunnel itself contain various installations representing specific risks. About five such working groups, each with the Safety Officers and other competent people, possibly also with outside experts, will be needed. The ST Division, in particular its Alarm and Access Group will have to participate in all of them, and it will have to play a leading role on those matters where it has expert competence.

6.2 Procedures, Documentation and Training for Emergency Situations

At present, we find situations at LEP whereby the respective responsibility and actions in case of emergency interventions are not defined, not clear or not properly implemented. Another major shortcoming concerning emergency situations are the poor state of required documentation, which is either not existing, of poor quality, or not up-to-date. CERN management should ensure that the procedures for safety and rescue interventions are consistent, correctly documented, properly implemented and that regular targeted training is provided for all people involved.

6.3 Data Exchange

The importance of data exchange between all control systems of the LHC machine and its experiments has been stressed above and a working group, setup by the CERN Controls Board, is already active.

6.4 TIS Safety Instruction SI 37 *Alarms and Alarm Systems*

This Safety Instruction SI 37, *Alarms and Alarm Systems*, needs to be reviewed. In particular, it contains some statements that are not in accordance with international standards. It also gives instructions, for instance, for hard-wired alarm transmission with which the *WG-AL3S*, after very careful considerations, does not agree for the LHC machine. SI 37 is furthermore very unbalanced, concentrating mainly on procedures for temporary unavailability of alarm systems. It is also clear that these procedures, relying on paper forms, can not work and that an electronic system is needed, in particular to get the required signatures in time and to provide the correct information on the maintenance state of safety alarm systems in real time to everybody involved.

6.5 Implementation of the *WG-AL3S* Recommendations

The last recommendation of the *WG-AL3S* expresses the need for a kind of supervisory body that should ensure that the recommendations are properly and fully implemented. As the recommendations have been formulated intentionally in general terms, leaving much freedom to those responsible for the definition, design and implementation of the alarm systems, it is probable that interpretations will need arbitration. The supervisory body should have a major role to play in this respect. CERN management has meanwhile decided that the TIS Division Leader should be chairman of this supervisory body, and that two other competent and high-ranked technical people should assist him.

7 CONCLUSIONS

Following a suggestion made by the *INB* liaison officer and a mandate given by the LHC Project Leader, the working group *WG-AL3S* elaborated and formulated recommendations for safety alarm systems for the LHC, to be implemented progressively for all CERN premises and installations. These recommendations have been presented and widely discussed by several safety, machine and experimental coordination and technical committees. They have been endorsed by these committees and by the CERN management and are a good basis for homogeneous alarm systems for the LHC machine and its experiments. CERN management has entrusted the ST Division, in particular the two groups AA (Alarms & Access) and MO (Monitoring & Operation), a heritage of the late group ST/MC (Monitoring & Communication), with the technical implementation of these recommendations.

Through the attribution of this challenging task to one single service unit, CERN management clearly expresses its wish to obtain in the most effective way a homogeneous and reliable safety alarm system. It is now up to us, the AA and MO groups of our ST Division, to establish or to enhance existing collaborations throughout CERN, a vital prerequisite for the demanding tasks ahead, and set very rapidly to work. It is likely that we will require some additional highly qualified manpower in order to be able to cope with the multitude of tasks requiring innovative management, systematic quality approaches and high technical competence.

REFERENCES

[1] M. Bätz, An invitation to Design LHC Systems for TCR Supervision, this Workshop