SAFETY ALARMS AT CERN

P. Ciriani, L. Henny, P. Ninin
ST Division – Communication and Monitoring Group (ST/MC)
CERN, Geneva, Switzerland

Abstract
In order to operate the CERN accelerators complex safely, the acquisition, transport and management of safety alarms is of crucial importance. The French regulatory authority [Direction de Sûreté des Installations Nucléaires de Base (INB)] defines them as *Level 3 alarms*; they represent as such a danger for the life and require an immediate intervention of the Fire Brigade. Safety alarms are generated by fire and flammable gas detection systems, electrical emergency stops, and other safety related systems. Level 3 alarms are transmitted for reliability reasons to their operation centre: the CERN Safety Control Room (SCR) using two different media: the hard-wired network and a computer based system. The hard-wired networks are connected to local panels summarizing in 34 security areas the overall CERN geography. The computer based system offers data management facilities such as alarm acquisition, distribution, archiving and information correlation. The Level 3 alarms system is in constant evolution in order to achieve better reliability and to integrate new safety turn-key systems provided by industry

1. INTRODUCTION

Level 3 alarms at CERN are alarms raised in situations endangering people and requiring immediate action by the Fire Brigade. (For a fuller definition with the references, see Section 2). They concern the whole of CERN, that is the Meyrin, Prévessin and LEP sites. Their main users are the firemen in the SCR (Safety Control Room).

The Level 3 alarm system comprises *detection equipment* on the spot:

- fire detection equipment,
- flammable gas detection equipment,
- emergency stops,
- miscellaneous (for a detailed classification, see Section 2).

The first three categories cover more than 90% of the Level 3 alarms.

Signals are transmitted via the *communication systems.* The data processing system is the main one which provides the SCR with the details (type of alarm, location, description, etc.). This system is backed up by a hard-wired system permitting lower-grade operation in the event of the failure of the main system.

Data handling systems such as the Central Alarm Server (CAS) and the Technical Data Server (TDS), associated with the existing communication networks, make it possible to manage the alarms.

The alarms are *displayed* on workstations or on wall-mounted panels.

For organizational and geographical grouping, CERN has been divided into 34 areas. A local panel in each area shows the alarms that may occur.

1.1 Development

The development of Level 3 alarms management may historically be summarized in three stages.

1.1.1 Stage 1

During an initial stage, from the establishment of CERN to the start-up of LEP, the data were distributed to the SCR and TCR (Technical Control Room) via a hard-wired system showing the location and nature of the alarm on a wall mounted panel. This system was assisted by a data processing system running a log. The TELEMECANIQUE system used in the '70s was replaced by a BBC system in the '80s.

1.1.2 Stage 2

In a second stage, the start-up of LEP brought about a considerable increase in the number of alarms and the merging of the systems with the replacement of the BBC system. This data processing system assisted by a hard-wired system suffers several drawbacks: alarm triggering times are not accurately represented and alarm bursts disrupt the system; only the geographical indication of the area generating the alarm but not its nature is represented on the local panel.

1.1.3 Stage 3

Developments in the third stage are towards a more uniform system which should result in more reliable and easier operation in the SCR. The modifications involve the bulk integration of industrial systems, improvements in the data processing system (CAS and the introduction of the TDS, see Section 5) and the improvement/renewal of the hard-wired system and local panels. This program is now in hand and should be completed in 2000.

1.2 The future

If this third stage proves reliable, the system thus installed may be regarded as the starting point for the LHC.

2. DEFINITIONS AND REGULATIONS

A Level 3 alarm is generated by an accident or abnormal situation. The type of alarm concerns (Fig.1):

- smoke detector,
- gas detector,
- emergency telephone,
- general emergency stop,
- oxygen concentration detector,
- flood detector,
- actuating an evacuation signal,
- lift blockage,
- “dead man” handle type alarm.

The above definitions are found in the Safety Instruction 37 (TIS IS37). The legal documents relevant for safety at CERN are the following:

- Staff Rules and Regulations, 10th edition, 1st January 1996,
- CERN Safety Policy, SAPOCO 42, Rev. September 1994,
- "Ionizing radiation" agreement between France and CERN, 28.4.1972,
- The French decree "Quality arrangements" dated 10.8.1984,
- The "Safety of installations" agreement between France and CERN dated 31.10.1984,

- TIS Safety Instruction N° 37,
- The final LEP safety report, 1994 edition.

This report was written under the terms of the agreement signed by the French State and the Organization on 31.10.1984. It was drawn up for the Directorate for the Safety of Nuclear Installations. Here are the alarm transmission provisions in Article V.8.3.1: "*Les **alarmes** de **niveau 3** sont disponibles sur le réseau informatisé des services généraux. De plus un réseau câblé fil-à-fil assure la **redondance** nécessaire pour la transmission des alarmes de niveau 3*".

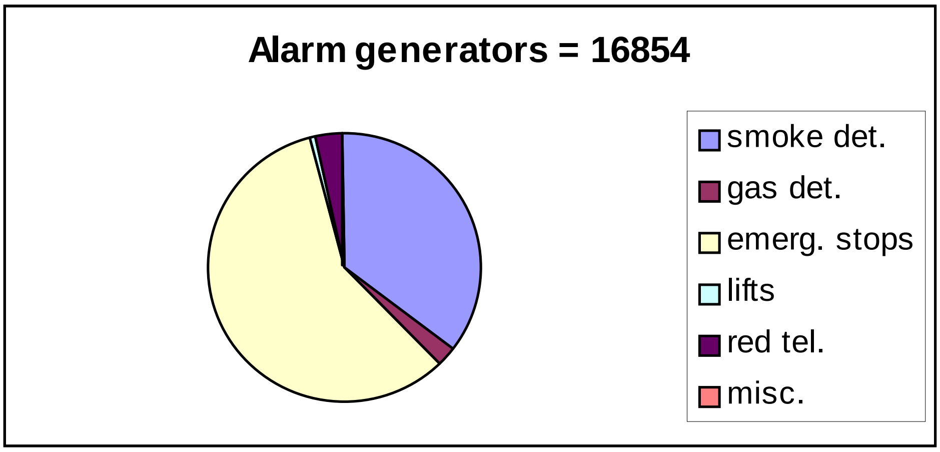

Figure 1 - Level 3 alarms distribution.

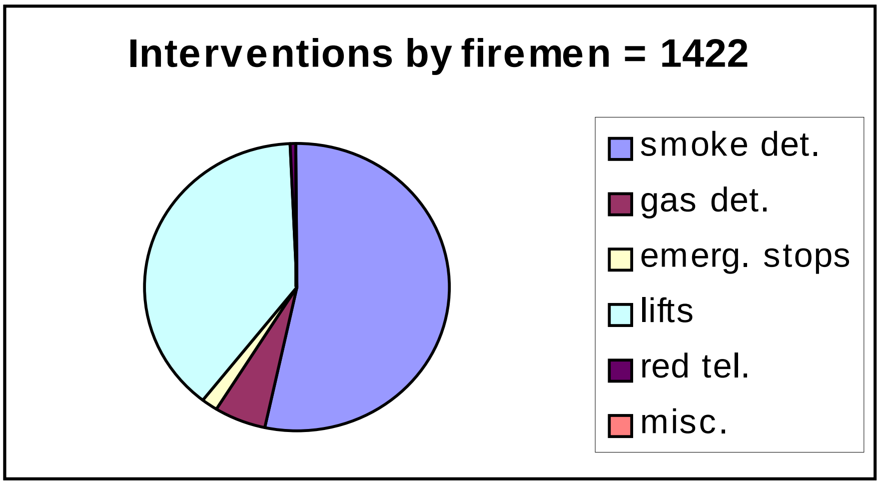

Figure 2 - Firemen interventions.

3. GENERAL DESCRIPTION

3.1 Present situation

In LEP and progressively on the Meyrin site, all Level 3 alarms are transmitted to the SCR (Fig. 2) and to the TCR via a computer network and displayed as a text message on a terminal (Fig. 3). At present, the Central Alarm Server handles only 3640 alarms over the 16854, the remaining alarms being not yet computerized.

The redundancy required by the “Installations Nucléaires de Base” rules is achieved by means of a hard-wired network [1]. All devices generating an alarm of level 3 are connected to the Safety Control Room. In LEP and progressively on the Meyrin site, these hard-wired signals are transmitted via a local panel (one *for each defined area*) which displays the location of the alarm source. The hard-wired signal causes a LED to blink on the local synoptic panel indicating the building from which the alarm comes and the type of alarm.

Apart from Red Telephones, an incoming subsequent alarm would make a LED blink faster. When the detector that caused the alarm is reset to zero, the corresponding LED remains bright; should the alarm(s) vanish, then the LEDs will go off. Transient alarms are also handled but will only be cleared after the reset of the detector and the disappearance of the alarm. A "General Alarm" summuray signal from the local synoptic panel is always transmitted to the SCR; this signal indicates the area concerned.

Only a reset of the local panel will turn off this "General Alarm" in the SCR.

3.2 Adaptations under way

After the double safety alarm transmission system was put into service for LEP, the same approach was adopted for the modernization of the other CERN areas. The SPS areas have been almost completely renovated and the 14 remaining areas of the Meyrin site will be following as the oldest fire and flammable gas detection systems are replaced by modern ones.

4. HARD-WIRED NETWORKS

4.1 History

The Level 3 alarms were originally only transmitted in hard wired form, and the location and nature of the alarm were displayed on a large mimic diagram in the TCR and SCR. Owing to the long distances involved with LEP, local panels were set up covering all the Level 3 alarms in a geographical area. Each local panel is connected by two wires to a summary panel in the SCR. (See Figure 4.)

Subsequently, this principle was extended to all CERN's sites for the sake of uniformity and to cut down the number of LEDs to connect. From this time on, the nature of the alarm was lost and only the location remained. There are at present 34 local panels.

4.2 Visual aspect

The local panels are of the standard 19" size and silk-screen printed on anodized aluminium panels. The background is green, the buildings concerned pale grey, the buildings not involved and the access roads are of the natural colour of the panel. The LEDs displaying the alarms are red.

4.3 Operating principle

The local panels are represented on the summary panel by a LED which lights up when a Level 3 alarm is actuated on the corresponding panel. With each local panel is associated a computerized "general area alarm".

Each area consists of:

- patch panels centralising the alarm generator contacts,
- an interface (relay boards and sequencer),
- a local panel.

On the local panel, there are one or more LEDs per building. They are identified according to the alarm type (F for fire detection, AU for emergency stop, etc.).

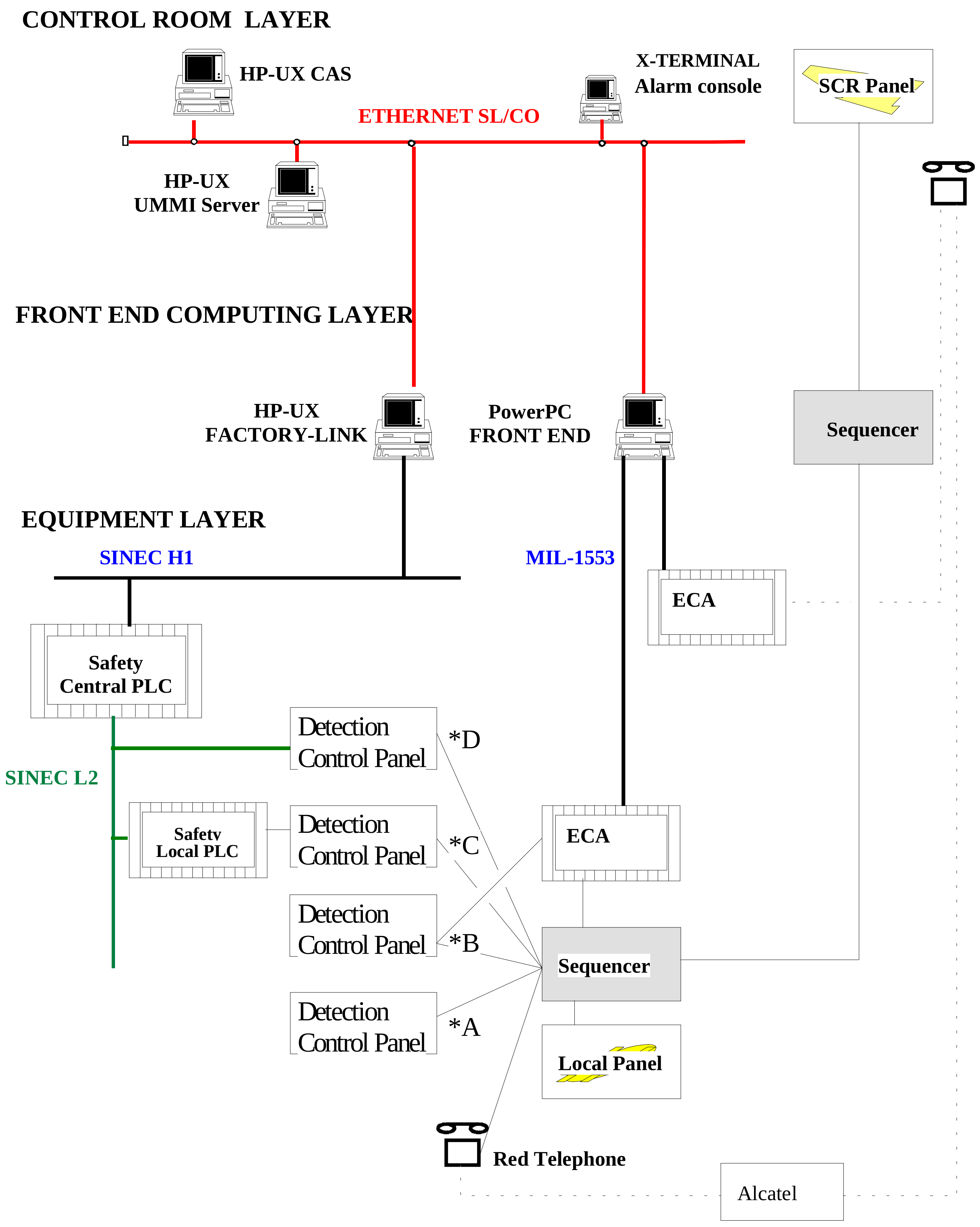

Figure 3 – “*Level 3 alarms*” present acquisition chains.

4.4 Limitations of the existing system

The limitations of the existing system are mentioned below:

- The redundancy is not always ensured, as some computerized and hard-wired alarm transmission cables share the same path.
- The technology used in the current system dates back to the '60s. Dry contacts run from the alarm generators to relay interfaces, which redistribute them via wires to the local and master panels. This technology has acquired certain limitations with time: poor contacts, "stuck" relays, sensitivity to vibration, etc.
- It is not an industrial but a "CERN" system. Monitoring and corrective maintenance have become difficult with time.
- Lines monitoring requires the use of current loops to detect any breaks and short circuits. This was acceptable at the time of the PS and SPS, but has become difficult with LEP owing to the long distances between the acquired points and the main interface, as the line resistance becomes very considerable due to the end of line load resistance.
- Induction and parasitic phenomena occur on the transmission cables.
- It is difficult and expensive to update the "hardware" panels.
- A paper based cable documentation system has been in existence since the beginning of CERN. This system is still in use despite several attempts at computerization. These have failed mainly owing to a lack of human resources and the complexity of the proposed systems. It is difficult to update the documentation and it is therefore not fully up to date. A new computerization project, jointly with the CERN telephone service, is on hand.

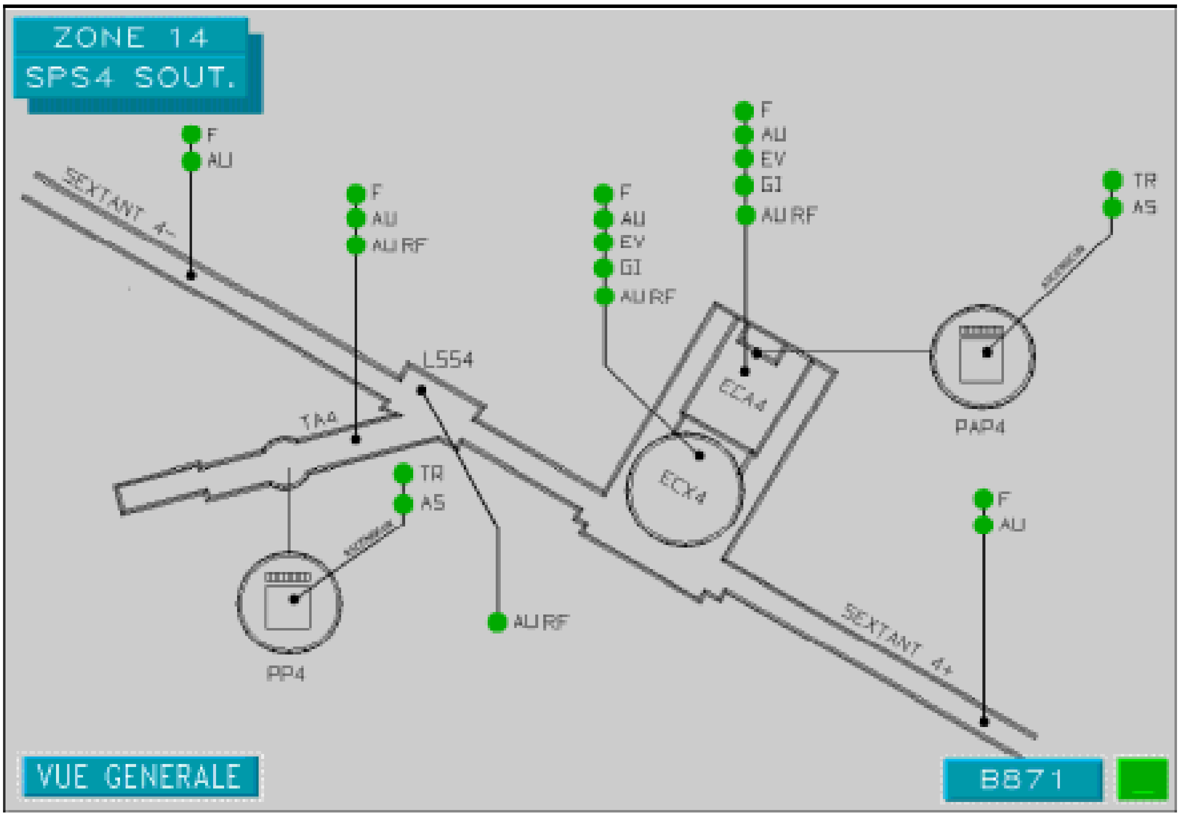

Figure 4 - Example of local panel and computerized mimic diagram.

5. EXISTING COMPUTER SYSTEMS

The SCR is an alarm-driven control room in the sense that the arrival of an alarm alerts the operator so that he may take appropriate actions. The operator acts upon the alarms primarily by consulting and interacting with mimic diagrams. These human-computer interfaces [2], alarms and mimic diagrams, have been structured systematically and standardized to a large extent, in spite of the large diversity of installations being supervised. Any new installation must be integrated seamlessly into this environment. (See Figure 3.)

5.1 The Central Alarm Server

The Central Alarm Server (CAS) [3] is the common alarm server for all alarms handled by the SCR. It gathers alarms from the equipment for logging and presentation to the users. The Central Alarm Server is not only used for the safety alarms, but mainly for the SL accelerator complex and technical services. This demonstrates its robustness and adaptability. A hot spare system is implemented to provide maximum availability to the users.

The Fault States (FS) are detected at the equipment level by User Surveillance Programs (USP) and are sent using a defined protocol to a local alarm server. The captured alarm is sent to a process which performs alarm treatment such as data reduction, and handles the communication with the CAS. The CAS stores and logs centrally all the alarms. The CAS dispatches alarms on an event-driven basis to the alarm consoles. Within the CAS, every alarm is completed with related static information (responsible, location, etc.). The CAS offers many other functionalities such as alarm archiving, retrieval and alarm inhibition. A related system: the “Help Alarm” provides detailed location, cause, consequence and actions information for every alarm.

5.2 Equipment Integration

The oldest integration of fire and gas detection information is performed by connecting a detection system to a local sequencer which animates local synoptics. The sequencer is itself wired to the digital input ports of an Equipment Control Assembly (ECA), allowing the safety event to enter the alarm level 3 software transmission chain (Fig. 3 *A).

An ECA is a G64 based system which monitors analog, digital inputs and outputs. The ECAs are connected to a long distance MIL-1553 fieldbus deployed around the SPS and the Meyrin site.

The captured alarms are sent by the ECA to the CAS via the Front End devices using the alarm processes described before. The Front End devices are standard VME racks powered by PowerPC processors running LynxOS. They act as gateway between the field buses and the Ethernet control network.

Even with the more modern integration methods, the detection system is always connected in parallel to a sequencer for hard-wired data transmission to the SCR.

In the early nineties the fire and gas detection systems were connected directly to the ECAs (Fig. 3 *B).

Since 1993, Siemens PLCs have been increasingly used in conjunction with the industrial supervisor FactoryLink. In this context, the detection system is connected directly to the PLC (Fig. 3 *C). Such local PLCs communicate via Profibus to a data concentrator which forwards the data via the Siemens Sinec H1 protocol to FactoryLink.

FactoryLink has been integrated in the technical infrastructure control system. A special CAS interface module was developed and added to the FactoryLink application in order to transmit alarms in a standard way.

The latest technology which will be described in the next chapter integrates directly the detection system at the Profibus (Sinec L2) level (Fig. 3 *D) (Defined as phase 3 in the Introduction).

6. ALARM LEVEL 3 SUPERVISION BY THE TECHNICAL DATA SERVER

6.1 The TDS context

At CERN, the TCR monitors data coming from the electrical distribution, cooling water, air conditioning, vacuum, cryogenics, safety and other systems.

A TDS has been implemented to manage this data. The TDS was firstly introduced to improve alarm management (acquisition reliability, alarm burst handling, time stamping).

It provides data collected from equipment using a standard TCP/IP interface to the high-level control software such as Human Computer Interfaces (HCI), a Data Logging System (DLS) and a Central Alarm Server (CAS). It performs real time data storage and distribution, alarm filtering, data archiving and playback, and command management in a distributed, multi-platform environment. Technical infrastructure data are used by other CERN control rooms and by those responsible for equipment. The TDS is now operational and several thousand tags are under integration.

The aim of the TDS is to focus on reliability and performance, its concept has been rapidly applied to the field of the Level 3 alarms.

6.2 TDS principles

Equipment data are sent by their control devices using drivers (e.g. SINEC H1, CERN SL Equip, Landis Visonik) to an Equipment Controller (EC) which converts them to the TDS tag format and forwards them to the TDS using the Generic TDS Equipment Access Protocol (GTEAP).

The tags are then stored in the TDS's local real-time databases (RTdaq) and are published to subscribing applications by a central server. The client applications receive the data by subscribing to particular data sets called data groups. All data arriving in the TDS are archived for 72 hours (allowing post-mortem analysis of incidents). Archive data can be played back in client applications just like the real-time data. The alarms are sent to the expert system (RTie) using the RTworks Guaranteed Message Delivery (GMD) mechanism which ensures that no data is lost even in the case of network or server unavailability. The expert system performs alarm deduction, filtering, alarm burst detection, and data correlation.

The TDS processes communicate via a dedicated message server. Applications can run on a single workstation or can be distributed across multiple processors in a heterogeneous network.

A special mechanism informs in real time the relevant client applications of any non-availability of an element (RTdaq, EC..) in the data transmission chain.

All commands sent using the TDS are identified, logged, and their execution status is checked. The TDS application programming interface (GTAAL) allows any client application to exchange data with the TDS. It is based on the reception of pre-defined messages handled as application call-backs.

Tag definition and system configuration data are held in a reference database providing a totally data driven system.

The TDS supervision module monitors the overall system and centralizes error treatment. An anti-flooding mechanism has been implemented whereby only tags, different from their default values, are transmitted at initialization thus optimizing system performance.

The application of the TDS to alarm level 3 management is demonstrated by the new fire-detection and ventilation-supervision system of the SPS.

The detection systems are integrated at the Profibus level by a PLC data concentrator, located in every SPS surface building. This device communicates via TCP/IP to an Equipment Controller interfacing the TDS. The TDS interfaces with the Landis Visonik control system using another Equipment Controller and sends command sequence to the SPS ventilation processes according to decision matrices.

The SPS fire detection-control system [4] was provided by an external contractor and easily integrated into the TDS using the GTEAP specification. The TDS captures the data as close as possible to the hardware and distributes it safely to any customer such as the Central Alarm server. The data may be filtered or correlated by the TDS expert system according to the specification of the appropriate specialists [5] - [9].

7. FUTURE DEVELOPMENT

The method of the Level 3 alarm transmission as described above and illustrated in Fig. 5 is to be applied to the whole of CERN. A wide-ranging program is on hand and will be completed towards the end of the year 2000. It includes:

- installing standard local mimic diagrams for the 34 areas (so far, 18 are operational; 11 on the Meyrin site are partially connected);
- integrating all the Level 3 alarms under the ST Division's responsibility (elimination of the old ECATCR) in the TDS;
- the replacement of the sequencers and distribution frames (especially on the Meyrin site);
- drawing up a complete database for cables (already started);
- the analysis of all the cable systems in order to detect the "shared modes".

At the end of its renewal program, CERN should have a reliable Level 3 alarm distribution and management system meeting the requirements of the INB. Likewise, this design would be uniform on all the sites and machines.

8. RECOMMENDATION FOR LHC

The principles now established and the experience obtained with the existing system may be used as a starting point for the LHC era. It is strongly recommended that the LHC should be regarded as a machine forming an integral part of CERN and that uniformity of principles should be ensured for the Laboratory. We must avoid repeating the experience of the LEP project, where the use of different principles in alarm management resulted in the need for subsequent standardization.

The complementary nature of the hard wired and computerized systems should be retained. It is unrealistic to consider the hard-wired system solely in relation to the number of existing alarm systems. Greater attention will have to be paid to the computerized system to ensure the maximum reliability expected of a safety system.

Finally, the principles now established, with the necessary technological evolution, can be used as a basis for the LHC monitoring. There must be one single principle for the whole of the laboratory, covering both old and new installations.

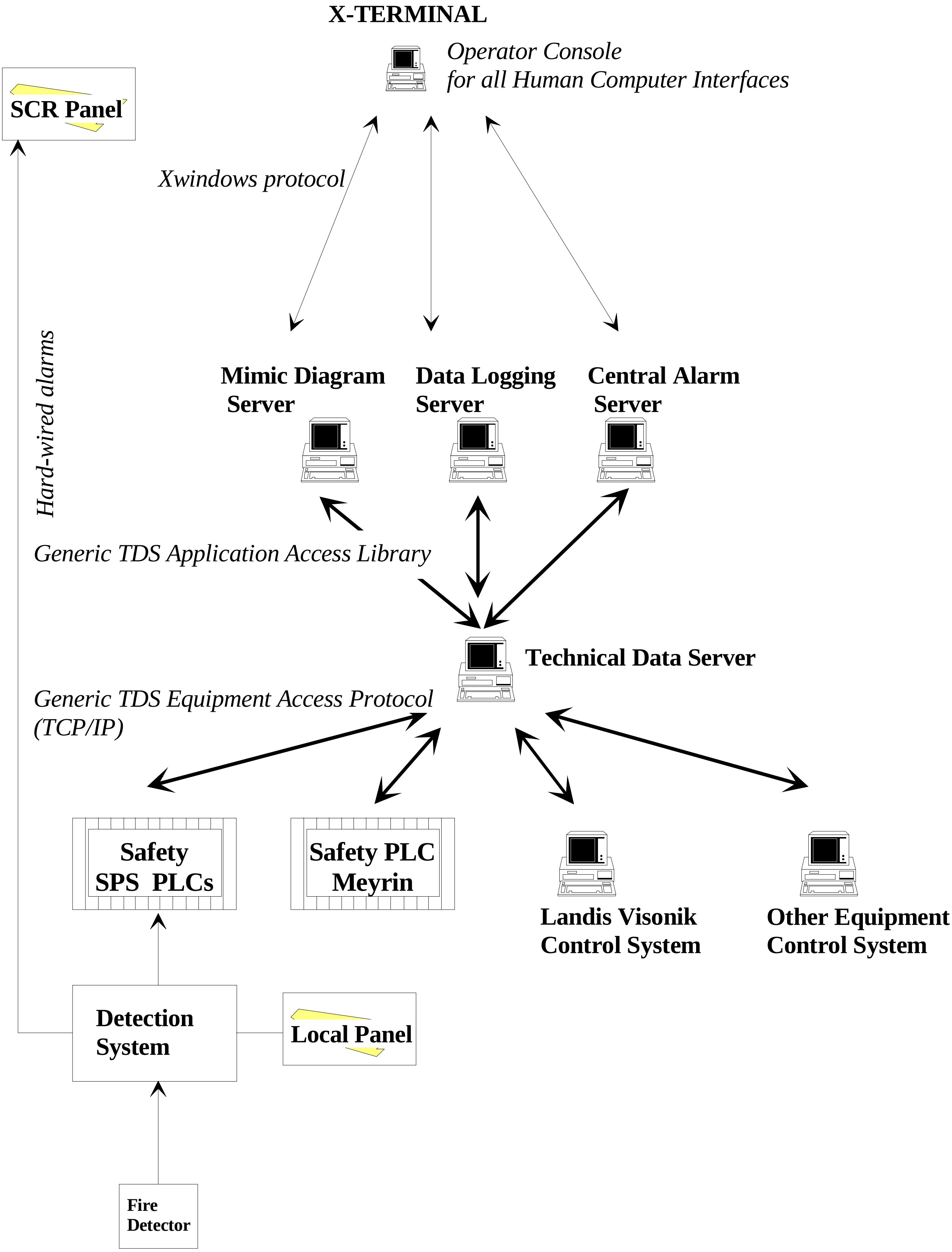

Figure 5 - New level 3 alarms acquisition chain

REFERENCES

[1] Descriptif technique du système filaire du LEP - Alarmes de niveau 3, ST/MC/5/NB/mg du 28.1.1994.

[2] Nicole Gonthier, CERN Alarm System User Interface, SUM, SL note 95/117 (CO) (1995).

[3] Utilisation d'un logiciel commercial graphique pour le contrôle des installations techniques du CERN, CERN-ST-MC-TCR/92, (October 92).

[4] SPS Access Control Renewal: Functional Specifications, TECNOST (April 1997).

[5] P. Ninin et al., Technical Data Server V1.0 ICD, ST/MC/96-12PN (December 1996).

[6] P. Ninin, Technical Data Server: a Modern Vision of Large Scale Supervision, ICALEPCS'97, this Conference, Beijing, 3-7 November 1997.

[7] P. Ninin, E. Cennini, P. Sollander, D. Blanc and F. Bonthond, Industrial Control System for the Technical Infrastructure at CERN (November 1997)

[8] P. Ciriani, Trends in industrial control systems in ST Division (January 1998).

[9] J. Fivet, L. Henny, H. Schönbacher et L. Stampfli, Rapport sur les détections d'incendie, 23 janvier 1995.