CERN SAFETY ALARM MONITORING

H. Nissen, S. Grau CERN, Geneva, Switzerland

Abstract

The CERN Safety Alarm Monitoring (CSAM) system acquires safety alarms and safety information generated by CERN safety equipment such as fire and gas detectors, evacuation, emergency stops and other safety related systems, which are located in both surface and underground areas of CERN sites and accelerators. Currently there are 22170 alarms from 1025 safety equipment. This information is transmitted in a high priority and diversely redundant way to the CERN Safety Control Room for immediate intervention of the CERN Fire Brigade. The system was designed based on two main standards, the EN 50136 and IEC 61508 and was commissioned in 2003. In 2009 it was decided to launch a consolidation project in order to upgrade both hardware and software. The consolidation project includes deployment of a private CERN wide fibre optic TCP/IP network for the transmission of safety alarms, an upgrade of the SCADA software, a database upgrade and the replacement of all computers. In this paper the system is presented, the ongoing consolidating work is detailed and the middle and long term improvement plans for the system are described.

SYSTEM OVERVIEW

Scope

The CSAM system gathers safety alarms generated by equipment such as fire and gas leak detectors, emergency stops and other safety related systems, which are located in both surface and underground areas. This information has to be transmitted as a high priority message and in a diversely redundant way to the Safety Control Room (SCR) for immediate intervention by the CERN Fire Brigade (FB). Experience shows that the quality and accuracy of the information, provided by the monitoring system, is crucial to ensure a quick and efficient intervention of the Fire Brigade. Therefore, the system must provide users with the necessary information to identify without ambiguity, the nature of the problem and its exact location, 365 day/year and 24h/day.

The information captured by the detectors is also sent to the Technical Infrastructure control room (TI), Experiment Control Rooms (XCR) and to external systems requiring this information. In fact, the TI has a double back-up function with respect to safety alarms: firstly, it could be used by the FB if their SCR was not operational, and secondly, it could complement the FB's safety actions with possible technical actions.

As a result of the hazard and risk analysis a Safety Integrity Level SIL2 was required to guarantee the delivery of safety alarms to the FB and to other control rooms.

Architecture

The system is separated into two different layers: *acquisition layer* and *supervision layer*.

The *acquisition layer* is PLC based and takes care of the acquisition of the alarms in the different safety zones as well as the transmission to a central PLC and to the supervision layer. The CERN site is divided into 33 different safety zones each equipped with two redundant PLC for alarm acquisition. The alarm signals coming from the CERN Safety Equipment (CSE) are cabled to an input module shared by the two PLC. Both PLC are connected to a common text display used to display the active alarms in the PLC's. Each PLC is connected to a separate TCP/IP network for the transmission of alarm to the central PLC and the supervision layer. In addition, an output on each PLC is activated if the PLC has an active alarm. This output is referred to as *General Zone Alarm* (Figure 1) and is connected to an input on the central PLC via a hardwired connection. This gives the central PLC three paths (TCP/IP network 1 and 2 and the hardwired) to detect if there is an alarm in a zone. Once the central PLC has detected an alarm in a zone this information will be transmitted to the supervision layer and to a hardwired *central alarm display* (CAD). This display consists of a simple graphical representation of the CERN site with a LED in each zone to indicate the existence of an alarm in the zone. The central PLC will also activate a klaxon in the SCR when a new alarm arrives in a zone.

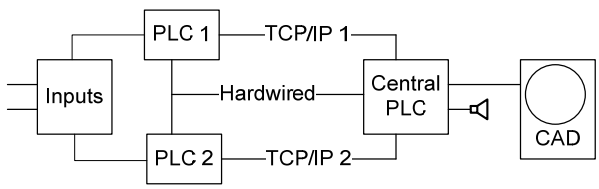

Figure 1: General Zone Alarm

For the transmission of alarms from the PLC to the supervision layer each PLC is connected to two acquisitions servers. The two servers acquire the alarms from all PLCs in parallel but only one will send the alarm up to the supervision layer. The other server acts as a hot standby with automatic switchover in case of problems on the active server. The acquisition server will also acquire the *General Zone Alarm* information from the central PLC for transmission to the supervision layer.

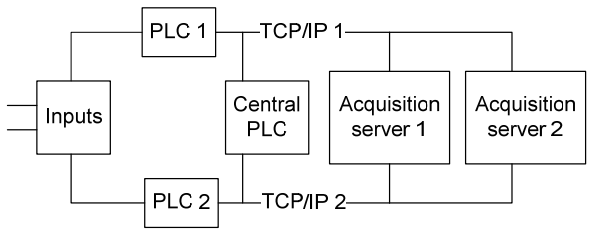

Figure 2: Hardware Alarms

Hardware Alarms (Figure 2) are alarm signals cabled to the PLC combining all alarms of a given type in a building e.g. "Fire building 104" but not the individual detectors. To get information about which detectors are in an active alarm state each CSE is connected to a common acquisition server via the TCP/IP 2 network (CERN TN). There are two ways the system can acquire information about the detailed alarms, referred in this paper as *Software Alarms* (Figure 3). Some safety equipment gives the possibility to connect via OPC (OLE for Process Control) a native protocol for the acquisition server. Other safety equipment only offers a serial port for communication. To transport the serial information over the TCP/IP 2 network the serial information is converted to a TCP/IP packet and sent to the serial acquisition server. As the serial protocol is vendor equipment dependent, specific drivers have been developed for each type of safety equipment.

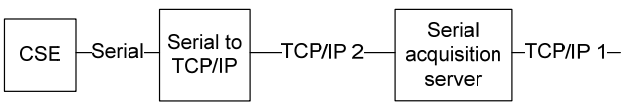

Figure 3: Software Alarms

As this transmission is not redundant (single network single server) it is clear that it does not reach the same safety level as the *Hardware Alarms*.

The *supervision layer* is responsible for presenting the acquired alarms and data to the users of the system. All operators' stations are connected to the two acquisition servers via the two TCP/IP network to ensure redundant transmission paths. The supervision layer main application is responsible for displaying the alarms on the alarm screen as well as on animated synoptic views. Views for displaying analog values and historical data analysis are also part of the application. The supervision application permits commands to be sent to the CSAM PLC to execute safety actions (e.g. remote evacuation alarm commands).

Operation modes

During normal operation alarms are acquired on both PLC and sent to the two acquisition servers and central PLC over both networks. In addition the central PLC supervises the *General Zone Alarm* signals from the 33 zones. If one of the networks is not available the system continues to operate on the second network in a degraded, for the operators transparent, mode. In case of failure of both networks the operators can still be notified that an alarm is present in a zone via the hardwired *central alarm display*. The alarm display will only indicate that there is an alarm in a given zone. In order to get the precise information the operators will have to go to the specific zone and consult the local text display connected directly to the zone control PLC.

Powering

All PLCs in the system are powered by an uninterruptable 48V connection from the electrical breakers power supply. The text display is powered by the same 48V supply. All computers are supplied from 220V UPS with a minimum of 1 hour autonomy. All servers have dual power supplies for optimum redundancy. The switches on the private network are powered by 48V and 220V UPS.

Interfaces

In order for other systems at CERN to have access to system data all relevant information is published on the Data Interchange Protocol (DIP) [1]. This gives other systems the possibility to subscribe to CSAM data for integration in local control systems. The main subscriber is the Technical Infrastructure Monitoring system (TIM) [2] that sends all CSAM data to the LHC alarm service and to the LHC data logging for long term archival of historical data. Other DIP subscribers include the detector control system for the 4 mains LHC experiments. A dedicated interface exists to a specific service (MOBICALL) for transmission of alarms to mobile phones.

DATA INTEGRATION, CONFIGURATION AND MAINTENANCE

The reliability of the information provided by CSAM depends directly on the integrity of the system's configuration data. Erroneous configuration parameters can lead to alarms not transmitted or false alarms. All changes on the operational system are therefore very delicate operations. In order to minimise the risk of errors all configuration data is managed in an off-line database and only applied to the operational system after validation.

To cope with the frequent number of integration, modification, and deletion requests, CSAM uses the Monitoring Data Entry System for Technical Infrastructure (MoDESTI) [3]. The goal of the MoDESTI procedure is to manage the data declaration process. In the first step the alarm responsible declare the alarms to be added, changed or removed using a predefined EXCEL sheet. Before the data is integrated into the reference database it has to pass a series of validations to ensure that the data is consistent. Once loaded on the reference database the data is synchronised to the CSAM database. A dedicated tool (configuration manager) is used to get access to the CSAM data. This tool is written in JAVA and run on JAVA's Rich Client Platform for easy integration with other tools. Once the data have been synchronised the system configuration files can be

generated. The generation is implemented on the database as stored procedures. After the configuration files have been generated the tool will distribute them to all computers. After distribution the configuration manager will transfer the new configuration to all the 66 PLC's and validate that all PLC are correctly configured. The last step in the process is to send a command to the system to integrate the new configuration in the system.

Normally the system is updated every Wednesday afternoon

CSAM IN NUMBERS

The system consist of 36 PLCs, 6 servers, 4 dual screen operator stations and 15 single screen local operator stations. There are currently 22170 alarms defined in the system and 550 analogue measurements. Of the 22170 alarms 1704 are *Hardware Alarms* cabled to a CSAM PLC and the rest are *Software Alarms*. The alarms are generated from 1025 different safety equipment distributed all over the CERN site. In 2011 the average rate of alarms arriving on the alarm screen in the SCR in a 24 hour period where 107 per day. Most of the alarms are generated because of maintenance as all alarms have to be tested every year in order to comply with CERN Safety Instruction IS37.

MAINTENANCE AND USER SUPPORT

An efficient support structure is a key element in the operation of the system. A 24-hour on-call support rota ensures that qualified system experts are available at any time to deal with incidents as soon as they arise. The support hotline is accessible to the TI and the SCR. The hotline is manned by CERN experts during the week and by an external company during weekends and vacations. Problems that do not require immediate intervention are handled by the CERN ITIL Service Management system via a dedicated e-mail address.

CONSOLIDATION

In 2009 it was decided to launch a CSAM consolidation project to ensure smooth operation in the future. The main parameters for the consolidation were the age of the system, a significant increase in the volume of data since the system was commissioned, and the agreement to deploy a new and fully independent redundant network to minimise common modes of failure at the communication level.

During the first consolidation phase all computer hardware (server + PC) was replaced by new machines. The Supervisory Control And Data Acquisition (SCADA) software for the supervision layer was upgraded to the latest version as the communication between SCADA machines had been greatly improved in the new version. The CSAM database was migrated from a local old version of ORACLE to a centrally managed 10g database. A new configuration database was developed so that the configurations files could be generated directly on the database instead of an old external tool used before. The CSAM administrator interface for the database was rewritten in JAVA as the old tool was not fully fulfilling the requirements. Several of the dedicated serial communications drivers were rewritten due to new requirements (e.g. the transmission of analogue values) and to correct several existing problems.

During 2010/2011 the CSAM private network was installed. The network is a fully CERN-wide fibre optic network with no interconnection to the other networks at CERN. The hardware used is different from the technical network to avoid common failure point. It consists of two star points interconnected by a redundant ring topology. From each star point fibres are installed to connect all CSAM equipment. During the installation it was ensured as much as possible, that the routing of the fibres in the building was different from the technical network to reduce common failure points further. The network was commissioned in spring 2011.

Middle and long term consolidation plans

Three main axes of middle term consolidation are foreseen:

Currently all alarms generated during maintenance and tests arrive at the SCR and makes the identification of real FB interventions difficult. A system and procedure to mask alarms caused by maintenance and test is under evaluation. Technically, the masking of alarms is not complex. What it is challenging is to ensure that no alarms are masked or remain masked by error, to guarantee the required SIL2 level.

The CSAM PLCs are currently supplied with one 48V feeder. Experience has shown that this is not an optimal configuration and a solution for having two separate feeders to supply the PLCs will be implemented.

The serial driver are foreseen to be split onto several machines in order to reduced the load on the machines and improve the availability of the data acquired by the drivers.

The long term consolidation plans includes the replacements of all the PLC hardware as this equipment will reach it end of life in the next 10 years.

REFERENCES

[1] W. Salter on behalf of the LDIWG, "DIP description", CERN, Geneva, Switzerland, April 2004

[2] J. Stowisek, A. Suwalska, T. Riesco, "Technical Infrastructure Monitoring at CERN" EPAC'06, Edinburgh, Scotland, UK, June 2006

[3] R. Martini, "MoDESTI System Work Flow", CERN, Geneva, Switzerland, February 2007