THE CERN DETECTOR SAFETY SYSTEM FOR THE LHC EXPERIMENTS

S. Lüders*, R.B. Flockhart, G. Morpurgo, S.M. Schmeling, CERN, Geneva, Switzerland

Abstract

The Detector Safety System (DSS), developed at CERN in common for the four LHC experiments under the auspices of the Joint Controls Project (JCOP), will be responsible for assuring the equipment protection for these experiments. Therefore, the DSS requires a high degree of both availability and reliability. It is composed of a Front-end and a Back-end part. The Front-end is based on a redundant Siemens PLC, to which the safety-critical part of the DSS task is delegated. The PLC Front-end is capable of running autonomously and of automatically taking predefined protective actions whenever required. It is supervised and configured by the CERN-chosen PVSS SCADA system via a Siemens OPC server. The supervisory layer provides the operator with a status display and with limited online reconfiguration capabilities. Configuration of the code running in the PLCs is completely data driven via the contents of a "Configuration Database". Thus, the DSS can easily adapt to the different and constantly evolving requirements of the LHC experiments during their construction, commissioning and exploitation phases. Currently, the DSS is being installed and commissioned for the construction of the CMS and LHCb experiments.

INTRODUCTION

The Detector Safety System (DSS) project covers one of the grey areas that still existed in the development process of the experiments at the Large Hadron Collider (LHC) at CERN: equipment protection.

According to CERN rules there are three alarm levels. The responsibility for the highest level of safety, which is defined as "accident or serious abnormal situation, especially where people's lives are, or may be, in danger" [1], is delegated to the CERN Safety System (CSS). Normal operation of the detectors is performed by the corresponding detector control systems (DCS). This left an area of uncertainty, especially as the availability and reliability of a PC-based DCS does not seem to be sufficient to ensure proper equipment protection.

In 2001, the four LHC experiments produced a document [2] defining requirements for a system assuring equipment protection for the valuable, and sometimes irreplaceable, detectors. The outcome of this is the DSS.

SCOPE AND REQUIREMENTS

The main goal of the DSS is to detect abnormal and potentially harmful situations, and to minimize the consequent damage to the experiment's equipment by taking "protective actions". By implementing this strategy, a reduction of the occurrence of higher level alarms with more serious consequences can be expected, and therefore an increase of the experiment's running time and efficiency. The DSS should complement but not duplicate existing systems, such as the DCS and CSS. By working together, these three systems will ensure that situations that may lead to equipment damage, or place people in danger, are well covered.

As a consequence of the above mentioned goals, the following main requirements were defined for the DSS. It has to be:

- highly reliable and available, as well as simple and robust,
- a cost-effective solution for experiment safety,
- operated permanently and independently of the state of DCS and CSS,
- able to take immediate action to protect the equipment,
- scalable, so that it may evolve with the experiments during their assembly, commissioning, operation and dismantling (a time-span of approximately 20 years),
- maintainable over the lifetime of the experiments,
- configurable, so that changes in the setup can be accounted for,
- connectable to other sub-(detector-)systems, and
- integrated into the DCS, so that existing tools can be reused, and that the look & feel, monitoring, and logging are standardized.

A complete overview of the DSS inside the experiment's control system architecture is shown in Figure 1. It is composed of the following entities:

- the equipment that is acted upon, i.e. primary services, and the equipment under control of the experiment,
- the DCS, which is a coherent multi-level control system running together with its own front-end and which might take corrective action to maintain normal operation,
- the CSS together with its own sensors, taking all required safety actions (e.g. calling the fire service) in case of an alarm and which is required by law,

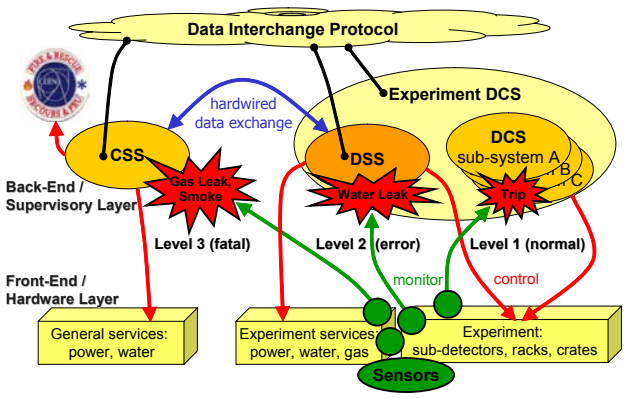

Figure 1: The experiment's control infrastructure.

*Stefan.Lueders@cern.ch

- the DSS, which is embedded in the experiment's DCS, and
- the Data Interchange Protocol, that provides information exchange between the experiments, the LHC, the technical services, and the CSS.

IMPLEMENTATION

The DSS implementation distinguishes between a Front-end, to which the safety-critical part of the DSS task is delegated, and a Back-end, which supervises the Front-end though a SCADA system (Figure 2). Their inter-communication is performed through a dedicated OPC server / gateway PC.

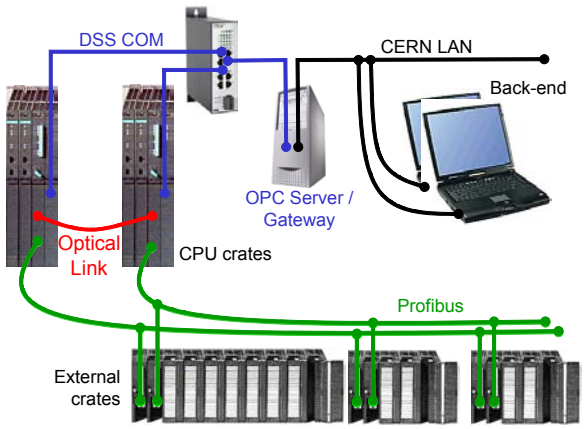

Figure 2: General DSS Hardware Architecture.

Front-end Architecture

The implementation of the Front-end follows the industrial standard used for such applications, using a redundant PLC system. All parts of the Front-end are compliant to the relevant safety norms.

The PLC continually monitors the experiment's equipment using hardwired information from dedicated digital and analogue sensors (e.g. PT100, humidity sensors, status signals of sub-detectors, information from external systems). Only hardwired sensors are considered to be safe, since networked information can not be guaranteed to be reliable. According to a set of rules defined by the user — the "Alarm-Action-Matrix" — the Front-end will automatically and immediately take predefined actions using dedicated actuators (e.g. cutting electrical power).

The PLC: The core of the DSS Front-end is the redundant PLC system S7-400 H from Siemens [3], which is certified for SIL 2 applications. In such systems, the two CPUs constantly compare their states and automatically detect abnormalities. In the event of a problem, only the "good" branch continues to operate.

Both 414-4H CPUs of the redundancy pair run the same "Process Code". The code and the corresponding data blocks can be modified without disturbing the DSS operation itself. Therefore, the DSS software can smoothly evolve to cover future needs.

Both CPUs scan the input signals of the DSS sensors. All values are filtered and checked. According to the Alarm-Action-Matrix, the state of the actuators is determined and set. This sequence is repeated periodically. The process time for a typical experiment is of the order of 500 ms, depending on the complexity of the matrix and the number of channels. Thus, the reaction time of the DSS to an abnormal situation is below one second.

Each of the two redundant CPUs is mounted in a crate together with redundant power supplies and the Ethernet communication processor CP443-1. To achieve synchronization, four (non-redundant) optical fibers interconnect the two CPUs. Common time synchronization is achieved by connecting them to a network time server at CERN.

Several external crates of type ET200M provide the interface to the DSS sensors and actuators through I/O modules. Each external crate can hold up to eight modules, where each digital (analogue) I/O module can handle up to 32 (8) channels. External crates and/or their modules can be (dis-)connected during DSS operation.

Up to 32 external crates can be connected to the CPUs via a redundant cable pair using the PROFIbus protocol. Thus, redundancy is achieved down to the level of PROFIbus communication. The I/O modules themselves are not redundant, but redundancy at this level can easily be obtained by doubling the number of sensors.

Detector Safety Units (DSUs): The Front-end functionality is split into several identical DSUs. The lower half of the standard 52U high DSU rack is dedicated to the infrastructure to connect sensors and actuators via patch panels. The upper half hosts the CPU crate and two external crates, an Uninterruptible Power Supply (UPS), and the OPC server/gateway PC (Figure 3). Only two DSUs contain a CPU crate, and only one the OPC server. Each DSU monitors its own state by the use of internal sensors and one dedicated I/O module.

Since the sensors and actuators are widely spread over underground caverns and the surface of the experiment's site, the DSUs act as cable concentrators to minimize the overall cable length. Each DSU is responsible for a distinct geographical area. The DSUs hosting the CPU crates are located at different places to minimize the danger of accidental damage by a single cause.

Each DSU is backed-up by the 1000VA online UPS SUOL1000XLI from APC [4]. Battery-packs allow each DSU to be independent of the general power network for at least one hour. This is sufficient to bridge the latency until the start of a diesel backed-up power network.

Patch Panels: In the optimal configuration, 224 digital sensors or actuators and 64 analogue sensors can be connected to one DSU. Thus, adequate space for cabling is essential.

The patch panel terminals from WAGO [5] allow for an easy connection of different types of digital and analogue sensors. All digital channels are galvanically isolated from each other and from the I/O modules by the use of opto-couplers. Modifications (i.e. adding or removing extra sensors or actuators) can be made during the running of the DSS and do not interrupt the process itself.

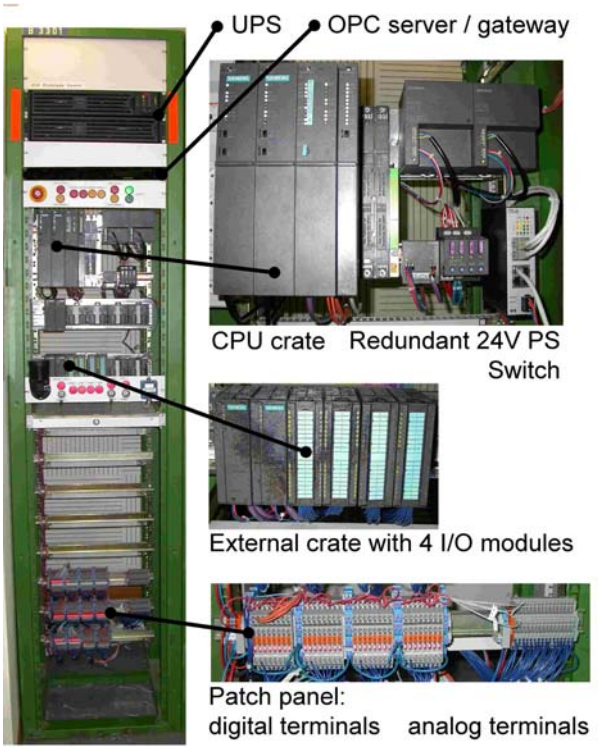

Figure 3: Hardware Layout of a Detector Safety Unit.

All digital sensors and actuators follow the "Positive Safety" rule. The normal condition is signalled by a "high" level (16-30V), while alarm conditions give "low" levels (0-5V). In the case of a broken wire, the PLC automatically assumes an alarm condition. Actuators are powered through normally / closed contact relays, which open in the case of an alarm. Short-circuits or broken wires of the analogue sensors are detected by abnormal readings.

The OPC Server and Communication

The communication between PLC and Back-end is routed through a dedicated 1U high rack-mounted PC (SuperServer 5013G-I [6]) acting also as a gateway. The data exchange is handled by an OPC server running on this PC [7].

The PLC communication is performed through a dedicated DSS network using common Ethernet switches and the special Siemens Ethernet adapter CP1613 installed in the gateway PC. This adapter handles transparently the redundancy of the CPUs and communicates with both using the ISO protocol.

The communication with the Back-end uses the standard CERN network connected to the PC's NIC.

Back-end Architecture

The Back-end, based on the PVSS [8] SCADA system and the JCOP Framework tools, constitutes the User Interface for the operators in the experiment control rooms. It is used for configuration, monitoring, logging, display, and as a gateway to external information.

Although the runtime safety-critical aspects are concentrated in the Front-end part, the Back-end configuration functionality also plays a role for safety, by limiting the possibilities for operator input errors. This is achieved by providing detailed assistance to the user, and by analysing his input. Any detected inconsistency is rejected before being downloaded to the Front-end.

The Back-end stores the current configuration of the system in the PVSS database, while it is planned to record the history of modification into an Oracle database. This database will also be used to log all changes of the sensor values defined in the system, as well as all the alarms detected and the protective actions consequently taken. All user actions will also be logged.

The user will be alerted whenever a new alarm is detected and will acknowledge the alarm, and reset it once the abnormal situation has gone. Subsequently, the user will be able to take the required actions (probably via the DCS) to bring the detector back into operation.

To ease the work and the understanding of the user, help pages are foreseen for every alarm, as well as a hierarchical synoptic display system, showing the origin of the alarms and the sensors in the experiment's layout.

Finally, the Back-end will also be capable of issuing warnings, so that the user can react in advance to developing situations that could eventually evolve into alarms.

CONCLUSIONS

The initial requirements for the DSS for the LHC experiments can be fulfilled with a relatively simple and robust system. This system has undergone a review in the summer of 2003, which allowed for the final series production. In total about 15 DSUs will be built and deployed to four experiment areas in the coming two years.

The costs for one complete DSS depend largely on the experiment's needs, but are in the order of 60000 Euros (sensors, actuators and their cabling are excluded).

ACKNOWLEDGEMENTS

We especially want to thank the DSS Advisory Board for the excellent collaboration. Furthermore, we would like to thank all the people helping with the finalization of the prototype and the actual construction of the series.

REFERENCES

[1] CERN, "Alarms and Alarm Systems," CERN TIS/GS, Geneva, IS37 Rev. 2, May 1998.
[2] DSS Working Group, "A Detector Safety System for the LHC Experiments - Final Report," CERN, Geneva, CERN-JCOP-2002-013, April 2002.
[3] Siemens AG, Automation and Drives, Germany
[4] American Power Conversion Corp. (APC), U.S.A.
[5] WAGO Kontakttechnik GmbH, Germany
[6] Supermicro Computer Inc., U.S.A.
[7] OPC Task Force, "OLE for Process Control," The OPC Foundation, Austin, TX, U.S.A.
[8] ETM AG, Austria