PUBLISHED BY IOP PUBLISHING FOR SISSA

RECEIVED: *July 21, 2009*
ACCEPTED: *September 17, 2009*
PUBLISHED: *September 29, 2009*

The Detector Safety System of the ATLAS experiment

O. Beltramello,[a] H.J. Burckhart,[a] S. Franz,[a,1] M. Jaekel,[a] M. Jeckel,[a] S. Lüders,[a] G. Morpurgo,[a] F. dos Santos Pedrosa,[a] K. Pommes[a] and H. Sandaker[a,b]

[a] *CERN,*
CH-1211 Geneva, Switzerland
[b] *Department of Physics and Technology, University of Bergen,*
Allégaten 55, 5007 Bergen, Norway

E-mail: Sebastien.Franz@cern.ch

ABSTRACT: The ATLAS detector at the Large Hadron Collider at CERN is one of the most advanced detectors for High Energy Physics experiments ever built. It consists of the order of ten functionally independent sub-detectors, which all have dedicated services like power, cooling, gas supply. A Detector Safety System has been built to detect possible operational problems and abnormal and potentially dangerous situations at an early stage and, if needed, to bring the relevant part of ATLAS automatically into a safe state. The procedures and the configuration specific to ATLAS are described in detail and first operational experience is given.

KEYWORDS: Control and monitor systems online; Large detector systems for particle and astroparticle physics

2009 JINST 4 P09012

[1] Corresponding author.

doi:10.1088/1748-0221/4/09/P09012

Contents

1 Introduction

ATLAS [1] is a general-purpose high energy physics experiment at the Large Hadron Collider (LHC) at CERN, Geneva, Switzerland. The detector is located in a cavern 100 m underground and is not accessible during operation. Because of this inaccessibility and of its very large size (the biggest high energy detector ever built, 46 m long and 25 m in diameter) and complexity, advanced control and safety systems are needed.

The normal operation of the experiment is supervised by the Detector Control System (DCS) [2], which is implemented as a distributed system of about 200 PCs. The task to detect severe safety hazards like fire, smoke, flammable gas, etc., which may even put human lives in danger, is fulfilled by the CERN Safety Alarm Monitoring (CSAM) [3]. Between these two systems lies a gap, the protection of equipment in abnormal and potentially dangerous operating conditions. This is covered by the Detector Safety System (DSS), which is the subject of this paper.

The definition of the DSS was established together by the four LHC experiments in the frame of the Joint Controls Project (JCOP) and the implementation was done by the CERN controls group IT/CO [4].

In the following, first the requirements are summarized and then an overview of the architecture and its implementation is given. The main part of the paper describes the usage of the DSS by ATLAS, in particular its configuration and the operational model. In the end some operational experience is reported.

2 General requirements and architecture

In general, when designing a safety or control system a choice has to be made concerning the conflicting requirements:

a) Extreme robustness and reliability, predictability, 100% available;

b) Flexibility, ease of reconfiguration, ability to perform complex operations.

The technical implementation depends very much on these aspects. The tasks mentioned above are such that the CSAM belongs to case a) and relies essentially on hard-wired connections. The DCS, which falls in category b), has been implemented mainly by higher level software running on PCs. The DSS, however, combines requirements from both a) and b), which strongly influenced the choice of its implementation.

For high energy physics experiments additional challenges need to be met such as dealing with:

- Extreme conditions (e.g. underground, confined spaces, extreme temperatures or pressures);
- Complex detector structures acting individually as well as together;
- Very sensitive sensor elements.

The detailed requirements of the DSS are:

- High availability; the system must operate continuously. During scheduled maintenance periods of DSS special arrangements must be made to ensure the safety of the ATLAS detector;
- Robustness of operation; the system must have a certain level of redundancy built-in in order to avoid single points of failure. Continuous internal diagnostics are also essential;
- Stand-alone capability; there must be no influence of other control systems on the DSS. It should have its own sensors detecting hazards and actuators to bring equipment in a safe state. It should be independent from external services such as computer networks or general electricity distribution;
- Flexibility to allow evolution with time; the commissioning of the different detector elements extends over a time period of about three years and supervision of components needs continuously be added without disruption of the supervision of already running equipment. The safety procedures will need to be adapted with the operational experience gained;
- Self-documentation; it must be possible to see online not only the status of the DSS, but to also access all definitions. All changes of the set-up and all actions of the DSS must be automatically documented.

A set of recommendations for the usage of the DSS in ATLAS has been laid out in [5]. The overall strategy of the DSS is to put (parts of) the ATLAS experiment into a safe state in case an abnormal and potentially dangerous situation arises. These shutdown procedures shall not be harmful for the detector. To this end there must not be any need for further actions by an operator.

However, a human intervention will always be necessary to analyse and to remove the fault and to bring the equipment back in operation, i.e. the DSS would never switch equipment back on automatically. The definition of DSS actions should be independent of the operational status of the experiment such as data taking, maintenance, etc., as equipment safety is independent of this.

The DSS consists logically of three parts:

- Sensors to detect an abnormal and potentially dangerous situation;
- Alarms, created by a programmable logic using the sensor signals;
- Actions to put equipment in a safe state.

The implementation is factorized in two components:

- Front-End (FE) to which the sensors are connected, where the alarms are established, and which triggers the actuators;
- Back-End (BE) with operator interfaces, allowing configuring the FE, to view the DSS status, and to reset alarms and actions.

The FE consists of several I/O stations which are connected by redundant cabling to the supervisor, which is implemented using two redundant Programmable Logic Controllers (PLC). All safety-related functions are executed in the FE and "positive safety definition" is used throughout, which means that in case of missing information (e.g. sensor disconnected) or internal DSS problems the relevant actions will be executed. All FE equipment runs from Uninterruptible Power Supplies (UPS) and does not need any computer network. A "gateway" PC connects directly to the PLC and provides the connection to BE PCs via the ATLAS control network. These BE stations, distributed at several locations, allow easy and user friendly setting up and operation of the DSS.

3 Implementation in ATLAS

The DSS architecture as described above is identical for all four LHC experiments, whereas the actual configuration is tailored according to the specific needs and risks of each detector.

3.1 Sensors and actuators

Potential hazards in ATLAS are overheating, either due to faults in the equipment itself or because of malfunctioning of the related cooling system, fire, and leaks of gases and cryogenic liquids. Dedicated sensors have been installed to detect such possible dangerous situations at an early stage.

An air sampling "sniffer" system collects the air from many locations inside the detector via 139 pipes and analyzes it for presence of smoke, flammable gases, CO2 and for deficiency of oxygen. Additional flammable gas detectors are placed close to the end-cap muon chambers and inside their gas distribution racks. Oxygen deficiency detectors are positioned underneath the detector and in the trenches, where heavy gases like argon or CO2 would accumulate in case of a leak. Smoke detectors control the ambient air of the different experimental areas, counting rooms and service zones. The racks housing the detector electronics are equipped with a thermal switch which cuts directly the power to this rack in case of overheating, and with smoke detectors connected to the

Table 1. Number and attribution of DSS inputs (left) and outputs (right).

	Inputs	
DIGITAL	Cooling	13
	Cryogenics	4
	FG detection	20
	ODH detection	12
	Sniffers	164
	Rack smoke detection	276
	Ventilation	24
	Gas systems	5
	Environment smoke detection	64
	BCM	8
	ATLAS OFF button	1
	UPS power	2
	Magnets	4
ANALOGUE	4 to 20 mA	
	Ventilation	10
	PT100	
	Muon system	4
	TDAQ room	4
TOTAL		615

	Outputs	
DIGITAL	Cooling	10
	Rack interlock	234
	Switchboard interlock	19
	Minimax	31
	Power supply interlock	44
	Magnet	4
	Gas	1
TOTAL		343

DSS. A status line from each cooling system is connected to the DSS in order to signal any malfunctioning. In addition, for several subdetectors and for some common services, signals indicating abnormal behaviour of their equipment are connected to DSS. Examples are vacuum problems in the cryogenic systems or a ramp-down of the magnet systems.

Digital sensors are implemented as an opto-isolated current loop, which has to be closed to signal normal conditions. Analogue sensors supply a standard 4 mA–20 mA signal. Most of the sensors connected to the ATLAS DSS are of the digital type, while a few analogue sensors provide temperature, flow, and pressure information of critical zones. Following the principle of “positive safety”, disconnection of a sensor always results in an alarm condition. The actuators are normally implemented as opto-coupled switches and, if higher currents are needed, as relays. Again, to achieve “positive safety”, these switches are closed for normal operation and trigger an action on the equipment connected by opening. Details of the input and output channels are listed in table 1.

3.2 Front-End system

The overall layout of the ATLAS DSS is shown in figure 1. The Front-End equipment is organized in Detector Safety Units (DSU), located in the different electronics rooms and is interconnected by redundant cabling using the PROFIBUS protocol. Two DSU are placed in each of the three counting rooms underground USA15L1, USA15L2 and US15L2 and one in the surface computer

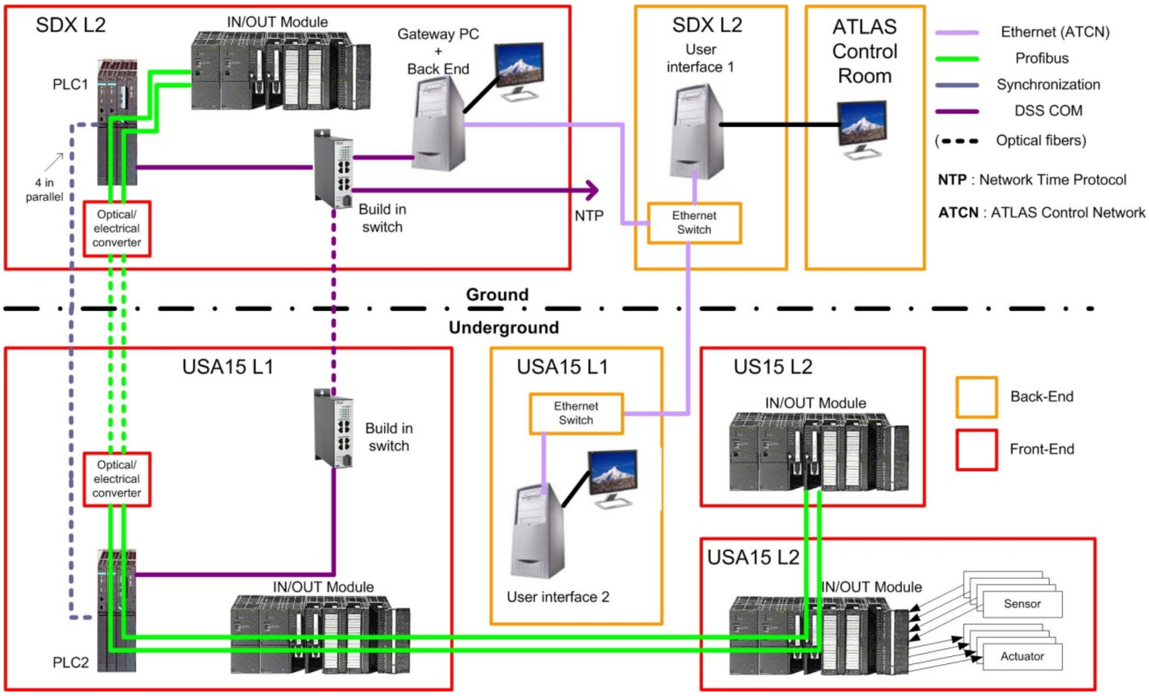

Figure 1. Overall hardware layout of DSS in ATLAS.

building SDX1. This distribution has been chosen to match the I/O requirements at each location and to minimize the cable lengths. In case of further needs more DSU can be added up to a total of 16 units.

Each DSU is a standard electronics rack, divided into two parts. The lower part holds the patch panels for the connection of sensors and actuators and the upper part contains I/O modules, the equipment for communication and a local UPS. This UPS has autonomy of at least one hour and is connected to the secured electricity network, which is backed up by a Diesel generator. Each DSU can be equipped with a mix of input and output modules according to the needs at each location. A DSU comprises typically the order of 300 digital I/O channels and a small number of analogue input channels.

The DSS PLC consists of two redundant CPUs which are located in the DSU in SDX1 and in USA15L1. These locations — one on surface and one underground — have been chosen to be as independent as possible. Both CPUs run identical programs to analyze all sensor information and to trigger the corresponding actuators. It takes typically 500 ms to cycle over all sensors, depending on the number of I/O channels and the complexity of the processing. Therefore the reaction time of the DSS to any abnormal situation is guaranteed to be less than one second. The internal states of the two CPUs and the results of the processing are compared at various steps, and, in case of problems detected, the faulty CPU would shut down. The other one would continue normal operation of the DSS. The DSU in SDX1 also contains the gateway PC which interconnects the PLCs with the DSS BE PCs.

3.3 The Alarm Action Matrix

The rules for the conditions to trigger actions are defined in the Alarm-Action-Matrix (AAM): all DSS input signals can be combined by logical operations to trigger any actuator in a matrix-like fashion. This proceeds in the following steps. First, a sensor indicating a fault sets an alarm. As an option, it can be requested that the sensor is in fault state for up to 30min in order to filter short fluctuations or to allow short interventions which should not affect the operation of the systems. The alarms triggered by several sensors can be combined using logical operations (e.g. “and”, “or”, “n out of m”) in order to trigger an action. Before its execution, i.e. setting the DSS output, a delay of up to 30min can be programmed. This is used for either sequencing actions within the DSS or for enabling the DCS to execute procedures before the DSS takes the action.

3.4 Back-End system

The Back-End (BE) system has two main tasks: configuring the DSS and serving as user interface (UI) for operations. As it is not directly involved in the safety procedures proper, its implementation does not need the same level of redundancy and robustness that the FE requires. The hardware platforms for the BE are PC. One machine serves as gateway for the communication between the PLC and several machines provide the User Interface (UI). All PC run the Windows operating system and use the commercial controls software PVSSII [6], which is also the basis of the DCS.

The BE software [7] is provided by the central JCOP team, including the user interface and tools to program the AAM. The ATLAS safety experts provide the configuration and the synoptic views of the ATLAS detector.

Setting up an AAM element consists of defining a logical relationship between input and output channels of DSS to establish alarms and to trigger actions. Before being accepted and sent to the PLC, all settings are checked for consistency. In this way the BE plays a role for safety as well. Once accepted the settings are stored online in an Oracle database for documentation.

The information about sensors triggered, alarms and active actuators is displayed by the UI using both tables and synoptic panels, which are specific for the ATLAS experiment. An active alarm also triggers a sound in the ATLAS control room, sends an e-mail and an SMS to the different subsystem experts, creates an entry in the logging database, and triggers a telephone service, which keeps calling people from a predefined list until someone has been reached and accepted to follow up the problem. The e-mail and SMS notification use external mailing, which is independent from the DSS alarm settings in order to minimize interacting with the DSS proper.

Backup and archiving functionalities are handled by the BE part of the system. The former allows restarting the system using the last valid AAM configuration, e.g. in case of an internal system failure, and the latter allows displaying the up-to-date definition of the AAM. The system also logs any alarm generated and all actions taken. The database can be inspected using the GLANCE tool [8], which also allows viewing the history of definitions and which describes the procedures for the operator to follow in case of DSS actions and the corresponding recovery procedures.

The BE sends the information about DSS alarms and actions over Ethernet using the CERN proprietary Data Interchange Protocol (DIP) to the DCS, which distributes it to all subdetector systems in order to enable them to execute shutdown procedures. In this way the relevant DSS information is also injected in the overall ATLAS status and alarm display, which is handled by the DCS. There is no software information going into the DSS from any systems in order to ensure that the DSS is as independent as possible.

4 System configuration

Setting-up sensor signals, alarms and actions in the DSS requires well defined procedures and interaction between with the DSS team and the different subdetector experts.

As a first step a risk analysis is performed for each subdetector, covering the risks coming from the subdetector itself as well as all risks created by neighbouring systems, missing services or general environmental problems. This analysis includes also possible risks the subdetector under inspection may present to other systems. The next steps are to define sensors which are able to detect such situations as early as possible and to define procedures to bring the subdetector in a safe state. These findings are documented in a report which has to be approved by the DSS team and the subdetector experts. After the implementation of the sensors and actions and the programming of the AAM a test covering the full chain from sensor to action is performed and this action is then documented as commissioned. Any further change needs new approval of the subdetector responsible and of the Group Leader In Matters Of Safety (GLIMOS) and possibly new commissioning. All these steps are documented in the CERN Engineering & Equipment Data Management Service (EDMS).

5 Operation

If an alarm is triggered, all corresponding DSS actions programmed in the AAM are executed and the detector is put in a safe state. A detector expert has to analyze the reason(s) of the failure, remove the fault and start the recovery procedure, together with the Shift Leader In Matters of Safety (SLIMOS). For each DSS action a corresponding recovery procedure is defined and documented in GLANCE.

The SLIMOS acknowledges the alarm when the reason for it is understood. After this acknowledgement the alarm is automatically removed from the alarm list, once the cause of the alarm is no longer present. Finally, after consultation with relevant (sub-) system expert, the SLIMOS can then proceed to acknowledge the action. After this step the subdetector can be brought back into operation. This may need complex procedures and may also require interaction with the GLIMOS and the ATLAS shift leader.

As mentioned above the DSS has to be continuously operational. A service team provides an on-call service to cure faults of the DSS itself and it also takes care of the regular maintenance of the DSS.

6 Performances and operational experience

The DSS is in operation since 2006, when the installation of the ATLAS detector has started. It has been continuously growing as detector elements were added and has by now reached its current implementation with 615 sensor inputs, 570 alarms, and 343 actions defined. The important feature of un-interrupted operation of the DSS during the process of adding further actions has always been fulfilled. Not a single unexpected behaviour of the DSS has been observed to date after more than three years of operation. Whenever an abnormal situation was signalled to the DSS, it took the corresponding action(s) as defined. In accordance with the concept of “positive safety” there were three occurrences where the DSS has correctly shut down the full ATLAS experiment because of an "internal" failure: once the DSS emergency button was pressed by mistake, once the DSS lost power because the back-up generator did not start up, and once because the redundant cabling was broken by mistake when adding a new DSU. However, these "unnecessary" actions did not cause any harm to the detector hardware of ATLAS.

During the set-up phase of the DSS substantial functionality has been added to the BE system, also enhancing its user-friendliness. The most important additions concerned logging in the data base for both documentation purposes and keeping track of operations.

Initially, the biggest part of the alarms which the DSS needed to deal with was caused by front-end cooling problems — around 70 alarms in the first two years. The actions triggered by these alarms were switching off power in electronics racks, interlocking detector power supplies, etc., thus preventing damage to the equipment due to overheating. Other actions were triggered by anomalies in the environmental conditions, e.g. smoke caused by welding work. Since ATLAS operations started, most DSS actions are triggered by operational problems with the gas.

7 Conclusions and outlook

In the more than three years of operation of the DSS in ATLAS its sound design and implementation has been fully proven. It fulfills all requirements, has never failed, and has always taken the actions that had been defined, thus guaranteeing the safe operation of ATLAS. The procedures of defining and maintaining the definitions of actions are well established.

The separation into a FE and a BE part is vital for the safe operation. The FE has — at any time — a valid definition of the AAM and is hence able to guarantee autonomously the safety of the ATLAS detector. The ability to add definitions to the system without interrupting it turned out to be crucial during the installation of the detector. Due to its data driven architecture and predictable response time no bottlenecks can occur, even when all elements of the AAM are solicited concurrently.

The decision to design and build a system for all LHC experiments in common did not only save implementation effort, but also allowed exchange of experience and will be beneficial for future maintenance. The DSS is flexible enough to be configured to fulfil the needs of each experiment. Purpose-built user interface panels can be easily prepared and further synoptic views will be added to help the operator.

Acknowledgments

We would like to thank the members of the CERN controls group IT/CO for the professional implementation of the DSS and for their continuous help in setting it up. The fruitful and pleasant collaboration with our colleagues from the safety teams of the experiments ALICE, CMS and LHC-b is gratefully acknowledged.

References

[1] ATLAS collaboration, G. Aad et al., *The ATLAS Experiment at the CERN Large Hadron Collider*, 2008 *JINST* **3** S08003.

[2] A. Barriuso Poy et al., *The Detector control system of the ATLAS experiment*, 2008 *JINST* **3** P05006.

[3] CSAM, http://st-proj-csam.web.cern.ch/st-proj-csam/.

[4] S. Lüders, R.B. Flockhart, G. Morpurgo and S.M. Schmeling, *The CERN Detector Safety System for the LHC experiments*, in proceedings of *ICALEPCS03*, Gyeongju, Korea, October 13–17 2003, CERN-OPEN-2007-019.

[5] H.J. Burckhart, *Recommendations for the usage of the Detector Safety System in ATLAS*, ATLAS documentation, EDMS Id 754656 (2006), ATC-TY-EN-0012.

[6] PVSS II SCADA Product, ETM, http://www.pvss.com.

[7] G. Morpurgo, R.B. Flockhart and S. Lüders, *The software for the CERN Detector Safety System*, in proceedings of *ICALEPCS05*, Geneva, Switzerland, October 10–14 2005.

[8] GLANCE, http://atglance.web.cern.ch/atglance/DSS/.