

The Detector Safety System

a.k.a. the reason why the detectors in the biggest accelerator in the world don't set on fire.

Germinario Andrea (BE-ICS-SAS)

13/09/2024



What is DSS?

What is DSS?

The **Detector Safety System (DSS)** is a control system that detects abnormal and potential harmful situations and minimizes the consequent damage to experiment's equipment by taking protective actions (equipment protection).

It complements but not duplicate other existing systems, such as the Detector Control System (DCS) and CERN Safety System (CSS).

It was first presented in ICALEPCS 2003

Proceedings of ICALEPCS2003, Gyeongju, Korea

UPS ▲ OPC server / gateway

functionality also plays a role for safety, by limiting the possibility 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

Proceedings of ICALEPCS2003, Gyeongju, Korea

- the DSS, which is embedded in the experiment's Alarm-Action-Matrix, the state of the actuators is determined and set. This sentence is repeated periodically.
- the Data Interchange Protocol exchange between the technical services, and

IMPLEMENTATION

The DSS implementation Front-end, to which the safety task is delegated, and a Back-End through a SCADA interface-communication is performed server gateway PC.

Figure 3: Hardwired Safety

All digital sensors follow the "high level" (16-3 levels (0-5V)) level of automatic assumptions entered through normal in the case of an analog sensor.

The OPC Server

The communication is routed through a SuperServer 5013 data exchange is implemented in this PC [7].

The PLC commands the DSS network of the special Siemens gateway PC, redundancy of the using the ISO protocol.

The communication standard CERN network.

Back-end Architecture

The Back-end, and the JCOP interface for the operator. It is used for configuration and as a gateway to the Front-end.

Figure 2: General DSS Hierarchy

Front-end Architecture

The implementation of the Front-end standard used for such as a PLC system. All parts of the to the relevant safety norms.

The PLC continuously monitors using hardwired informatics and analogue sensors (e.g. status signals of sub-detectors, systems). Only hardwired sensors, since networked informatics, are not used.

The PLC: The core of the Front-end PLC system S7-400 H is certified for SIL 2 application. CPUs constantly compare the detected abnormalities. In the "good" branch continues to operate.

Both 414-411 CPUs of the same "Process Code". The data blocks can be modified via operation itself. Therefore, smoothly evolve to cover future needs.

Both CPUs scan the input signals. All values are filtered and corrected.

Proceedings of ICALEPCS2003, Gyeongju, Korea

THE CERN DETECTOR SAFETY SYSTEM FOR THE LHC EXPERIMENTS

S. Lüders*, R.B. Flockhart, G. Morgurgo, S.M. Schmelzing, 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 (JCCP), 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:

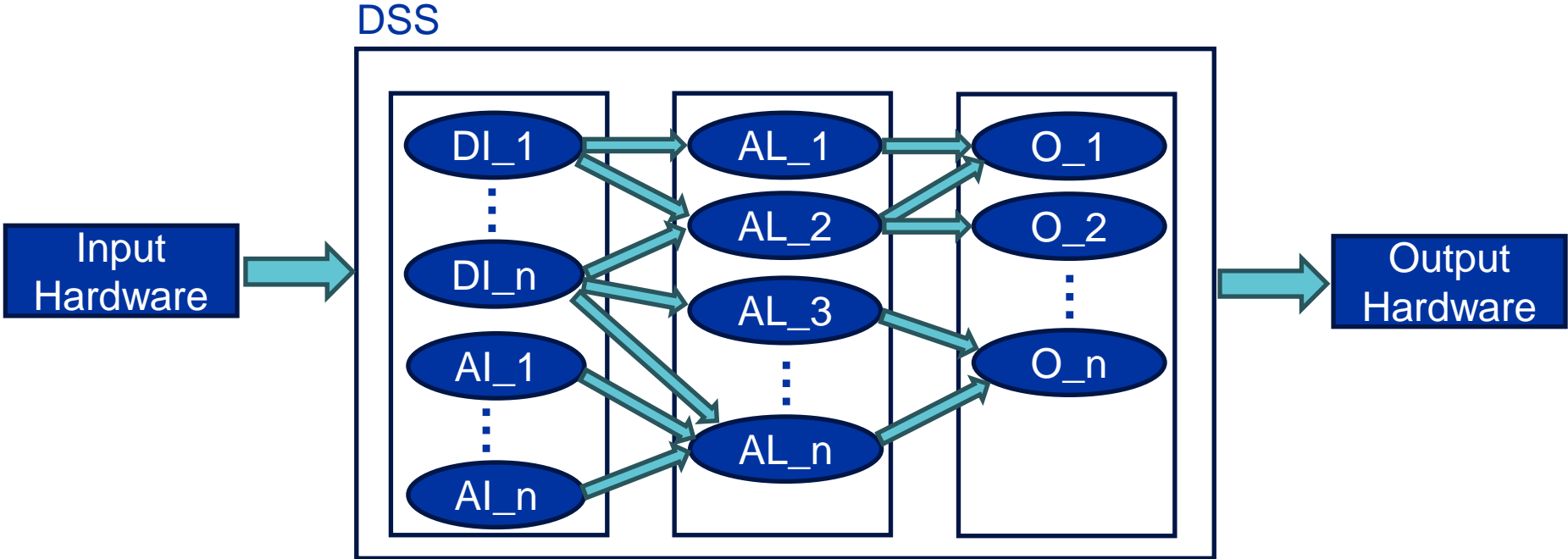
- the equipment that is acted upon, i.e. primary services, and the equipment under control of the experiment,
- the DCS, which is a coherent multi-level control system running together with its own front-end and which might take corrective action to maintain normal operation,
- the CSS together with 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

569

How does DSS work?

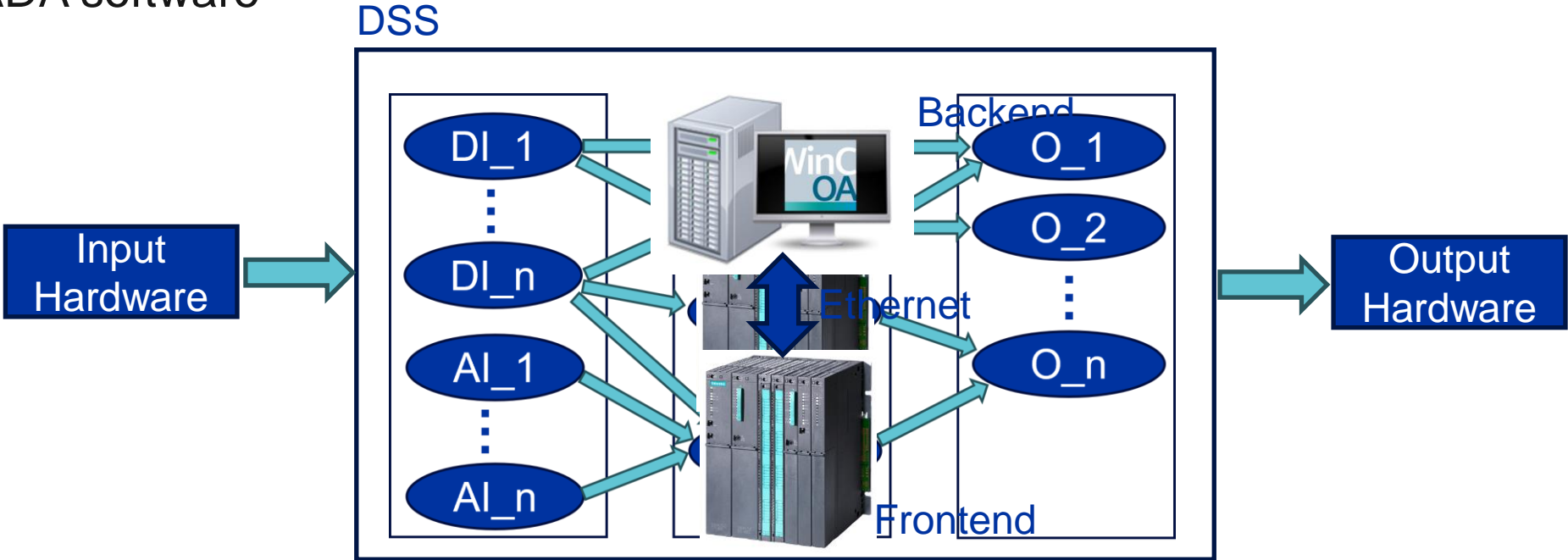
- 1. Declare and configure **sensors** to check the status of the Detector
- 2. Define **alarms** that trigger when specific conditions based on the sensors verify
- 3. Declare and configure **actuators** that activates when an alarm triggers



How does DSS work?

The DSS comprises two main components:

- **Frontend** : PLC application, running on a set of redundant Siemens PLCs
- **Backend**: SCADA Application, based on the Siemens/ETM WinCC Open Architecture SCADA software



Challenges

Challenges

My goal is to maintain and refactor the SCADA (Supervisory Control and Data Acquisition) layer of DSS. However, the system makes us face some challenges:

- Critical system (Users expect 24/7 uptime)
- Users are very reluctant to change but upgrades are required
- Hardware is physically close to application
- Deployment possible in small time windows (end of year shutdown, etc..)

Common problems in the industrial control world!

Solutions

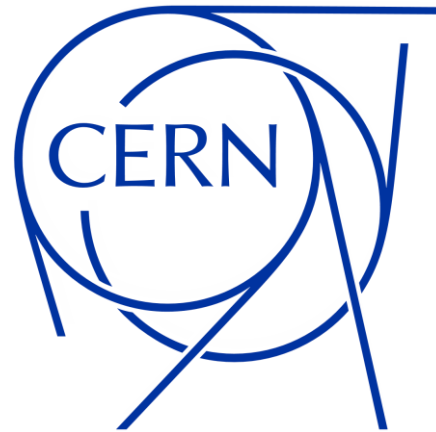
- Critical system (Users expect 24/7 uptime)
 - Test every change in a perfect physical copy of the system before deploying
 - Be ready to roll-back quickly
- Users are very reluctant to change, but upgrades are required
 - Put nice-for-developer changes with nice-for-users ones
 - Make the new feature look more appealing
- Hardware is physically close to application
 - Perform remote operations as much as possible
- Deployment possible in small time windows (end of year shutdown, etc..)
 - Book these slots well in advance and be flexible with dates
 - Make the users desire the upgrade

Conclusions

Engineers like to work on latest technologies

Real world projects are legacy and have constraints

It is possible to reduce the gap between industry and modern software development!



Thank you!