CERN

Detector Control System

For an LHC Experiment

User Requirements Document

Issue:	1
Revision:	0
Reference:	ALICE/98-03:LHCB/98-005:IT-CO/98-01-01
Created:	12th May 1997
Last modified:	11 May 1998
Prepared by:	ALICE/LHCb Teams

This document has been prepared using the CERN PSS-05 Templates. The CERN PSS-05 Templates have been prepared by the Information and Programming Technology Group, ECP Division, CERN (The European Laboratory for Particle Physics) and conform to the PSS-05 Software Engineering Standards (ISBN 0-13-106568-8) defined by ESA (European Space Agency) BSSC (Board for Software Standardisation and Control).

Abstract

The purpose of this document is to provide the user requirements for a detector control system kernel for the LHC experiments following the ESA standard PSS-05 [1]. The first issue will be used to provide the basis for an evaluation of possible development philosophies for a kernel DCS. As such it will cover all the major functionality but only to a level of detail sufficient for such an evaluation to be performed. Many of the requirements are therefore intentionally high level and generic, and are meant to outline the functionality that would be required of the kernel DCS, but not yet to the level of the detail required for implementation. The document is also written in a generic fashion in order not to rule out any implementation technology.

Document Status Sheet

Table 1 Document Status Sheet

1. Document Title: ALICE/LHCb DCS User Requirements Document			
2. Document Reference Number: ALICE/98-03:LHCB/98-005: IT-CO/98-01-01			
3. Issue	**4. Revision**	**5. Date**	**6. Reason for change**
1	0	22 January, 1998	First official release

Document Change Record

Table 2 Document Change Record (of changes made since issue ...)

Document Change Record	**DCR No.**	
	Date	
	Originator	
	Approved By	
1. Document Title	DCS for an LHC Experiment URD	
2. Document Reference Number	ALICE/98-03:LHCB/98-005:IT-CO/98-01-01	
3. Document Issue / Revision Number	Issue 1, Revision 0	

4. Page	**5. Paragraph**	**6. Reason for Change**

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Purpose of the document

The purpose of this document is to provide the user requirements for a detector control system kernel for the LHC experiments following the ESA standard PSS-05 [1]. The first issue will be used to provide the basis for an evaluation of possible development philosophies for a kernel DCS. As such it will cover all the major functionality but only to a level of detail sufficient for such an evaluation to be performed. Many of the requirements are therefore intentionally high level and generic, and are meant to outline the functionality that would be required of the kernel DCS, but not yet to the level of the detail required for implementation. The document is also written in a generic fashion in order not to rule out any implementation technology.

Once a development strategy has been chosen, and as more information about the experiment needs becomes available, this document may be required to be updated to add more detail to the requirements in order that the document is sufficiently detailed for the kernel DCS to be developed from it.

As stated above, the intention of this document is to describe a kernel for the DCS of the LHC experiments. However due to its generic nature it is believed that the kernel described here could also be used as the basis of other control systems in the LHC environment, e.g., run control.

1.2 Scope of the software

The system described in this document is intended to provide a common DCS kernel for all LHC experiments. As such the kernel DCS will provide the common functionality necessary to monitor and control the operation of an LHC experiment. The kernel DCS shall be able to be configured for any LHC experiment through the development of detector specific applications and equipment specific support software.

Furthermore, if agreement can be reached between the experiments to support standard hardware then, analogous to an operating system, the kernel DCS will also provide a set of standard device drivers for this equipment and a corresponding standard set of high level applications.

1.3 Definitions, acronyms and abbreviations

1.3.1 Definitions

Action

An action can be initiated by the user or the DCS itself and can modify the behaviour of the DCS, the experiment equipment or cause an interaction with an external system. It can be initiated either by the user at any time, within the normal rules of DCS operation, or by the DCS itself on the occurrence of an alarm/event.

Alarm

An alarm is generated when a piece of equipment deviates from the desired operation. Several levels of alarm are possible.

Alarm Condition

An alarm condition is an expression which is evaluated by the DCS and if found to be met causes an alarm to be generated.

Booking of Equipment

A user can book a piece of equipment to work on and this means that he has sole write access to that piece of equipment during the period in which the equipment is booked.

Command

A command is defined to be an action which can change the state or operation of experiment equipment, e.g., switch on/off, change from one mode of operation to another, change a set-point. A command can be issued by the user or by the DCS itself.

Command Procedure

A command procedure is a combination of commands that a user can initiate through a single action. It allows the users to perform complex actions in an easy and efficient manner.

Configuration Parameter

A configuration parameter is a parameter which defines a configurable value for any device, e.g., alarm limit, set-point, scan frequency, etc.

Derived Parameter

A derived parameter is a parameter which is calculated by the DCS from a combination of measured or other derived parameters.

Detector Control System (DCS)

The DCS is the sum of the kernel DCS configured for a particular detector together with the experiment specific applications.

Device

A device is a piece of experiment equipment for which the behaviour is monitored and controlled by the DCS. A device can have a number of defined states, e.g., on/off, nominal, off-nominal, and will have one or more parameters associated with it. Figure 1: Detector Hierarchy gives an overview of the detector hierarchy.

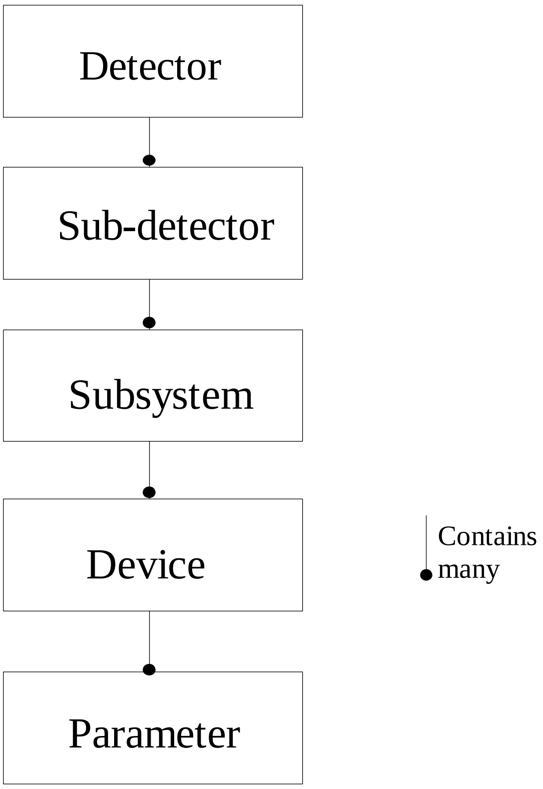

Figure 1: Detector Hierarchy

Event

An event is defined to be a situation that arises after whose occurrence an action should be initiated, e.g., change of a sub-detector from one defined state to another might initiate the change of alarm limits or an alarm condition becoming active.

Measured Parameter

A measured parameter is an individual piece of information which is read by the DCS from a device. A measured parameter may be Boolean or analogue. Each measured parameter will have a unique identification within the DCS.

Parameter

A parameter may be measured, derived or configuration.

Subsystem

A subsystem is a collection of devices.

Sub-detector

A sub-detector is comprised of a number of subsystems.

User

A user is anyone authorised to use the DCS. There will be different classes of users with different levels of privilege.

Widget

Widgets are components which can be used to build displays and which contain associated configuration information such as the identification of any parameter or object that it is linked to.

1.3.2 Acronyms

ESA

European Space Agency

CERN

European Laboratory for Particle Physics

HEP

High Energy Physics

LAN

Local Area Network

1.3.3 Abbreviations

API

Application Program Interface

DCS

Detector Control System

FSM

Finite State Machine

H/W

Hardware

LHC

Large Hadron Collider

MMI

Man Machine Interface

PID

Proportional Integral Derivative Controller

S/W

Software

tbd/c

To Be Defined/Confirmed

UR

User Requirement

URD

User Requirements Document

WYSIWYG
What You See Is What You Get

1.4 References

[1] ESA Software Engineering Standards, PSS-05, Issue 2, 1991

1.5 Overview of the document

The document is broken down according to the PSS-05 suggested table of contents as follows:

The first chapter of the document describes:

1. the purpose of the document
2. the scope of the software
3. definitions, acronyms and abbreviations
4. references

Chapter 2 describes:

1. project perspective
2. general capabilities
3. general constraints
4. user characteristics
5. the operational environment
6. assumptions and dependencies

Chapter 3 contains the specific requirements:

1. capability requirements
2. constraint requirements

2 General Description

2.1 Product perspective

The kernel DCS described in this document is intended to be the basis of a new generation detector control system to be used for the LHC experiments.

In the past many detector control systems have been developed to support experiment activities at CERN. These control systems were largely developed independently from each other. As an example four different DCSs were developed to support the LEP experiments (ALEPH, DELPHI, OPAL and L3), which naturally meant duplication of effort, higher development costs and greater maintenance effort.

For the LHC era, developments for all experiments should be common as far as possible in order to reduce the overall costs, to optimise the use of the available resources and to reduce the maintenance effort required during the operational life-time of the LHC. The DCSs for the LHC experiments require essentially the same functionality and as such provide an obvious area for common development.

Therefore, a common kernel should be provided which can serve as the basis for each DCS helping to reduce the overall effort required to develop the four LHC DCSs and subsequently to ease maintenance over the life-time of the LHC. Such a kernel control system could also be used as the basis for other LHC control systems.

2.2 General capabilities

2.2.1 Overview

The DCS kernel shall provide the basic functionality as required of all LHC DCSs without the experiment specific elements. As such, it must support a variety of users in the operation of an experiment or parts thereof

Normal Operation:. During normal operation, i.e., during a period of data taking operation with the LHC, the DCS would be operated in a well defined state. That is to say, once the detector has been configured for a run, switched on, and brought into its operational condition (by switching between defined states), the operator would monitor the operation of the experiment or sub-detector and would generally only take action in the event of an anomaly situation. As such the interaction with the DCS during a run should be fairly limited. It should, however, be noted that the process of switching on, and initialising the detector, is likely to be a multi-stage operation whereby the detector passes through a number of states. Furthermore, much of the operation of the detector will be very much state dependent (e.g., alarms, events, commanding, etc.).

Non-operational Phases: The DCS will also be used during phases where the LHC is not running (e.g., commissioning, shut-down, machine development). During these phases the DCS will be operated in a completely different fashion, in that individual sub-detectors or even subsystems will be required to be operated in a stand-alone manner. In this case, the DCS will have to support not only an integrated operation of the detector as a whole, but also stand-alone operation of sub-entities of the detector. During these periods the equipment configuration may be changed. That is to say that existing equipment may be modified or removed and that new equipment may be added. The user will wish to perform these modifications in a simple fashion without impacting other parts of the DCS. During these non-operational phases it is possible that some sub-detectors, or subsystems, will also need to be continually monitored and controlled in a closed loop fashion.

User Operations: At the highest level, the DCS is required to provide a user with all relevant functionality to monitor and control the operation of an experiment, or parts thereof, in an orderly manner. As such, it must provide the user with information about the status of the experiment as a whole and also of all component parts, and must notify him when anomalies occur. It must furthermore allow the user to control the operation of the experiment as required. That means switching equipment on/off, switching between different operating modes and setting appropriate values. In short, the DCS will permanently monitor the health and status of the equipment and inform the users when anomaly situations arise.

User Privileges: The DCS will be used by a variety of users with the responsibility for performing different tasks and therefore requiring different privileges. As an example, a user might be required to operate the experiment as a whole and as such would need no detailed knowledge of the individual sub-detectors. He would only require high level information on the health and status of the complete experiment, and be able to perform standard operations on all parts of the experiment. However, he would not require detailed information about each sub-detector and would only have limited privilege for controlling these. On the other hand, another user may be a sub-detector expert and only be required to operate one sub-detector. As such, he would not need information about other sub-detectors, nor have the privilege to control them, but would require access to all information pertaining to his sub-detector to a very detailed level. An expert would need to have sufficient privilege to control all aspects of the sub-detector operations.

Types of Access: As stated above, it is expected that the DCS will be used by a number of different classes of users with a range of responsibilities. However, in order to guarantee the performance of the DCS, access must be restricted to authorised users only. Therefore the kernel must provide facilities to identify all users, and depending on their role, and hence, their level of privilege, control the level of functionality available to them. In general this will be a restriction on which commands are possible. Furthermore, it is envisaged that the DCS may be accessed from a variety of locations including a central control room, other locations in CERN, from institutes external to CERN and even from users' homes. Different privileges will be available to a user depending on the access location, and also the kernel will have to provide facilities to ensure that conflicts do not arise as a result of multiple users operating the detector, or parts of it, at the same time.

Equipment Monitoring and Control: The prime function of the DCS is to monitor and control experiment equipment. That is to say, to acquire equipment parameters, perform processing on these where necessary and to issue commands to the equipment, either as a result of closed-loop control or commands originating from the user or other equipment. Much of this will be experiment specific, but nonetheless the kernel DCS should provide standard services in support of this, and a suitable interface to allow integration of the experiment specific software into the kernel DCS. A typical sub-detector may have up to 100,000 input/output parameters and a complete detector in the order of 1,000,000. To ease the definition of the process control for experimental devices the kernel should support a number of general process control concepts, e.g., Finite State Machine (FSM), PID controller**.**

Alarm Handling: In order that the users of the DCS can efficiently monitor the status of the detector and react quickly to anomalies, an alarm handling capability must be provided. The purpose of this alarm handling is to inform the user about unexpected behaviour of the detector equipment, and of the DCS itself, in a fashion which allows the user, or an expert system application, to be able quickly to identify the source of the anomaly and take corrective action. Alarms should be generated automatically by the DCS when detector equipment deviates from the desired status and/or value. The user will then be able to access further information pertaining to the alarm in question in order to determine what action is required to be taken. Additionally, it must be possible for automatic actions to be generated by an alarm to either perform automatic recovery from the alarm situation or to perform a safe shutdown. There will be different users of the DCS who will in general require knowledge about only a subset of alarms. Furthermore, multiple alarms may be generated due to a single malfunction and the volume of alarms generated in such cases could mask the true source of the problem. Therefore, certain processing of the alarms must be possible to be able to present to the user only that information which is relevant. During the life-time of the DCS operation the experiment equipment will evolve, and quite likely the operation philosophy as well. Therefore, it must be possible for a user to define, modify and verify alarm conditions on-line in a straight-forward manner without negatively influencing the operation of the DCS or the detector equipment.

Man Machine Interface: The user will interact with the DCS via a MMI. As such, the MMI must be a powerful aid to him in performing his duties, and provide him with a set of tools and services which allow him to work in an efficient manner. The MMI will provide not only the graphical interface for monitoring the status of the detector, but also the interface to all tools required by the user to configure the kernel DCS for an experiment and to perform an analysis of experiment parameters. As many of the users will not be very familiar with the use of the DCS, the MMI must be intuitive to use, i.e., the users must be able to perform all tasks necessary for the operation of the detector with minimal training. Different classes of users will use the DCS and will correspondingly require different views of the detector. These views will in general be experiment dependent and as such not within the scope of the kernel DCS. However the MMI provided by the kernel DCS must nonetheless provide the capability for these views to be developed, preferably in a very straight-forward and quick manner. Furthermore, the capability must exist for experienced users of the DCS, with the appropriate level of privilege, to be able to configure their own displays. Additionally, the MMI provided by the kernel DCS should include a number of tools to allow the users to perform analysis of the control parameters, e.g., real-time and historical trending, histograms, data tables. The information seen by the various users must always be consistent, e.g., a parameter viewed by any user in the DCS has the same value**.**

Archiving and Retrieval of Data: In order to allow detailed trouble-shooting and to allow long term monitoring of the experiment equipment it will be necessary to access the history of measured parameters. Therefore, all measured parameters must be archivable to facilitate later retrieval and analysis. The user will be able to control which parameters are to be archived. The archival frequency will typically be dependent on the rate of change of a particular parameter, but may be changed in the event of an alarm condition or on request of the user. A user wishing to retrieve data from the archive should be able to do this in a flexible manner by applying a wide range of selection criteria to his request.

Logging of Data: In order to enable users to reconstruct certain events within the experiment or DCS, logging capabilities should be provided for alarms, operator interactions and state transitions with an associated time stamp. In the case of user actions, the log should also identify the user concerned. Furthermore, it should be possible for the user to add comments to the log, e.g., to indicate any action he may have taken in response to an alarm situation. It must be possible for the users easily to select and sort information from the various logs.

Masking of Equipment: The DCS will be run for long periods of time during which devices may fail or not be required for a particular run. In such cases the user will wish to be able to mask the equipment in order to suppress unwanted alarms from that equipment.

Multi-user Development Environment: The kernel DCS will need to be customised to the needs of each individual experiment. This will be done by one or more teams working at geographically distributed locations world-wide. Typically each sub-detector will have a team responsible for the control aspects of that sub-detector and therefore responsible for configuring the kernel to their needs. These sub-detector teams must be able to work independently from each other, but in a way that ensures that a coherent overall DCS results. As such, the kernel should provide a development environment which supports a multi-user, multi-location development strategy. Furthermore, it is advantageous if a team can implement changes to its DCS configuration, and incorporate these into the operational system, without the need to re-boot the system.

Configuration Definition and Management tools: An important aspect of the customisation for the individual experiments is the management of the experiment configuration. Each experiment will have in the range of 100,000 to 1,000,000 input/output parameters, which together with their usage in displays, alarm conditions, whether they are to be archived, etc., will have to be defined for a DCS. As such suitable configuration definition and management tools must be provided for efficient and rapid configuration of the DCS.

API and External Interfaces: It is extremely important that the kernel DCS has a full and flexible API. To enable the kernel DCS to be customised for the experiments, a flexible API is required to interface experiment specific applications easily with the kernel, and also to allow other off-the-shelf S/W to be utilised in conjunction with the DCS. Furthermore, in order for an experiment to operate efficiently and safely, and to collect high quality scientific data, a number of systems must work closely together. The DCS is one of these systems and will need to exchange data with many other LHC systems, including LHC accelerator control system, experiment run control, DAQ/Trigger, safety system, as well as infrastructure systems such as cryogenics, cooling and ventilation and electrical distribution (tbd).

2.2.2 Access Control

Access to the DCS should be restricted to authorised users only. As there will be different classes of users with different privileges, it will be necessary for the kernel to provide the capability to be able to identify the user in order to grant the appropriate level of privilege.

At any one time there are likely to be many users of the DCS, some of which will have the privilege to write to the same equipment. In normal circumstances it is undesirable for two or more users to be modifying the operation of a piece of equipment at the same time. Therefore the kernel must ensure that such conflicts do not arise. Furthermore it is undesirable that a user may modify the operation of a device during a physics data taking period without the knowledge, and approval, of the person operating the detector as a whole.

However, it is possible that after a period of operation the level of access control will be relaxed. In the case of an LHC experiment, access control is considered more as a means to prevent users from making mistakes rather than to prevent users from sabotaging the detector or the associated equipment.

2.2.3 Types of Access

Users of the DCS will not all access the system from a central control room. In fact the majority of the users will access the DCS from outside of the central control room. Therefore the kernel should allow access from a number of different locations. These locations would include the central control room, auxiliary control room (if applicable), offices at CERN, offices within the institutes participating in the experiment collaboration, experiment equipment areas, and even from the homes of sub-detector, subsystem and device experts.

Access rights will generally depend on the location from which the DCS is accessed, e.g., a subsystem expert may have lesser privileges from home than he would do in the experimental area. When accessing the DCS from a remote location it must be possible to do this without the need for specialised hardware or software, e.g., via the web.

2.2.4 Users

All users will be assigned a set of privileges by the DCS Administrator. Privileges may be dependent on the location from which the users accesses the DCS. The privilege will determine whether a user can write to a particular device, modify configuration information, access command procedures or modify the operation of the DCS. Access filtering must be provided through read/write/modify type protection capabilities for all parameters in the DCS.

2.2.5 Definition and Configuration of Experiment Equipment

The kernel DCS will be configured for each experiment. Part of this process will be to define all experiment equipment which is to be monitored and controlled by the DCS. The kernel DCS should provide the facilities for this to be done in an efficient manner. In general this will be done off-line before the commissioning of the experiment. However, it is expected that experiment equipment will change during the course of the detector operation and it will be necessary to take this into account. These changes will generally be made during shut-down periods of the LHC, but nonetheless it will still be necessary from time to time to make such changes during the operational period of the LHC. The kernel DCS should allow for changes to the detector configuration to be made also during the operation of the DCS.

The kernel DCS should provide the capability to perform consistency checking when modifications are made to the detector configuration store and issue a warning in the event of an anomaly. Examples would be the re-use of a parameter identifier, use of a non-existing parameter in an algorithm, or the setting of high alarm limit bands narrower than low limit bands.

The user shall be able to define a hierarchy of control which itself reflects the hierarchy of the detector to simplify the operation of the detector. For instance he should be able to perform control actions on a power supply rather than having to control each of the individual parameters which comprise the power supply. Similarly, he should be able to perform control of a complete subsystem or sub-detector in a similar fashion. In this vein, the definition of experiment equipment should be at a device level and not at an I/O parameter level.

Tools should be provided to allow the user to define devices in a simple manner. These tools should also allow the user to define multiple versions of a device type without having to enter all information for each device individually. The configuration should be stored in such a way that the user can easily search for a particular device, for groups of devices, for names of devices, etc., together with the corresponding I/O parameters that belong to a device. Furthermore, it should be necessary to input any information only once into the system. As an example the name of a device may be of interest in conjunction with may aspects of its behaviour, e.g., alarms, display, commanding, etc., however it should be entered and stored uniquely in the configuration store and linked to, or referenced from, all other related information.

Authorised users should be able to modify configuration information in the operational DCS without the need to stop and re-start the system. Such changes should come into effect as soon as they are activated.

2.2.6 Definition of Commands and Procedures

In order to modify the operation of experiment equipment a basic set of instructions, covering all types of operation that a DCS user would need to perform on the equipment, should be provided. It should also be possible for users to easily create other basic commands as and when required for specific devices.

Furthermore, in order for the user to be able to operate a detector, sub-detector or subsystem efficiently, it will be desirable that he can execute complex actions with a single command. As an example he should be able to put a complete sub-detector into a desired state with a single command. This command would execute a number of defined commands and/or procedures in a controlled manner to modify the condition and/or state of experiment equipment.

The user should be able to define complex command procedures in a straight-forward manner. That is to say that the user shall be able to define not only sequences of commands, but also criteria which have to be met before a command, or set of commands, is initiated. It is desirable that a tool is provided which aids the user in building command procedures. Two possible examples might be that the user can select commands and criteria from a pre-defined set or that an State Notation Language (SNL) type of tool is available for the user to build the procedures. Furthermore, the user should be able to modify and test the correct operation of command procedures.

The set of basic commands shall include at least the following:

- Timer, e.g., setting of a defined delay before the command is executed
- Sequencing, e.g., an instruction is only executed after the termination of a previous command
- User acknowledgement, e.g., the command is only initiated after a user confirmation
- Conditional execution, e.g., the command is executed only if defined conditions are met

The following execution handling facilities should be provided for command procedures:

- Execution monitoring, i.e., the user must be able to monitor the execution of the procedure to see how the procedure is progressing
- Error handling, i.e., if an execution error is detected the execution flow is terminated and control handed back to the user
- User control, i.e., the user should be able to perform the following actions on a command procedure; Halt, Continue, Step, Abort, Show Value

2.2.7 Hardcopy & Report Generation

The users will wish to extract information from the DCS, in What You See Is What You Get (WYSIWYG) format. This may be displayed data or data from a log or archive in either a text or graphical format. The user should be able to perform basic functions such as output device selection and configuration.

The user will wish to define reports which should then be automatically generated and output. The user should be able to define the format and content of such a report, the frequency with which it should be generated and the device which should be used for output. It should be possible to define a backup output device in addition to the default output device.

2.2.8 Alarm handling

2.2.8.1 Alarm Definition and Generation

An alarm is generated when a previously defined condition is violated. Consequently, it will be necessary for the DCS to continually compare a parameter's value/status, or that of a complex expression, with the nominal value/status.

This implies:

- Analogue parameters may have upper and lower alarm thresholds which can be defined. When the parameters goes outside one of these thresholds an alarm of the corresponding severity is generated, e.g.

  - For a sensor which provides a single analogue value, a set of upper and lower limits can de defined. If the measured value is outside the specified region, an alarm with an associated level of severity will be generated. Different regions may be defined depending on the state of the device, sub-detector or detector.

- Alarm conditions with binary values must be compared with requested values, e.g.,

  - If a device which can be in two states ("on" or "off") is not in the *desired* state, this should also generate an alarm. A typical example is a VME power supply. Both states, "on" or "off", are possible desired states. However, if the power supply switches spontaneously from one state to the other, then an alarm should be generated.

- Arithmetic and logic operations must be possible on alarms in order to create groups and hierarchies, e.g., definition of "complex" devices and filtering, e.g.,

  - An alarm condition may be an algorithm which depends on the status of many parameters, both measured and derived.

  - An alarm condition may depend on the operational mode or state of the experiment, e.g., the limits for a voltage may depend on whether the experiment is in shutdown, stand-by or data-taking mode. Alarm conditions may be valid only in one state.

  - To ease the later handling of alarms it should be possible to define relationships between alarms, e.g., to group alarms or to arrange alarms in a hierarchical fashion.

  - More complex devices or subsystems can have quite sophisticated algorithms to determine if the device should or should not generate an alarm. As an example we can imagine a set of three temperature sensors which provides redundant temperature information of a physical object and generate only an alarm when the majority of the sensors is indicating a temperature which is outside the normal limits.

  - In some cases it may be necessary to automatically suppress an alarm for a period of time. An example of this would be a piece of equipment that requires a period of time to reach the required state/value, e.g., high voltage supply needs to ramp up to the required voltage over a period of time

- For a device which can be in one of a set of states, one or more of which would be error states. An alarm should be generated when one of these error states is entered

- For a device, the behaviour of which is modelled as a finite state machine, there will be one or more states which indicate that there is a problem. Transition to one of these states should generate an alarm. A typical case is a HV power supply. If the current limit is exceeded, then the power supply trips by itself and goes to the state “tripped”. This should generate an alarm.

The user will wish to also define and modify alarm conditions during the operation of the DCS. It must be possible to perform these actions without affecting the operation of the DCS or the experiment equipment.

2.2.8.2 Alarm Management

a) In general many users will be using the DCS at any one time, and they will be interested in different alarms. It shall be possible for each user to be notified of only those alarms which are of interest to him, i.e., that the alarms are filtered before being brought to his attention.

b) Complex relationships can exist between equipment. The fact that a device is in a given state may affect the state of one or many others devices. In general the user would not want to be notified of such alarms and it should be possible to suppress both alarm notification and logging in these cases:

   - If the mains of an electronics rack is off, then all equipment in that the rack will be off. In this kind of situation, it is more important to report to the operator that the real problem is the that the rack is off and not that 10 different power supplies are not in the desired state.

   - If the mains of a rack containing measuring devices (i.e., gas distribution rack) goes off, then the measured parameters will be wrong and that will generate alarms despite the fact that the physical quantities (e.g., pressures) have not changed.

c) It will be necessary to disable or mask alarms for equipment which is known not to be working properly. The DCS should provide facilities to do that for individual devices or groups of devices. The user should be able to easily determine which alarms are disabled.

d) Alarms must be single logical entities within the DCS. That means that the same information about an alarm is available to all users and when an alarm is acknowledged or deleted by one user, this information is available to all other users.

2.2.8.3 Alarm Display

It must be possible for users to easily view the alarm information which is of interest to them without it being cluttered with other information. The reporting mechanism should be adequate for interacting with humans, e.g., a flashing lamp, audible noise, etc. Once the alarm is reported to the operator, he has to have the means of getting all the information and details of the alarm (time, severity, subsystem, how to handle it, etc.).

Alarms which are reported to the operators need to be acknowledged. Alarm notifications are suppressed automatically when the cause of the alarm has disappeared or by the operator taking a responsible action, although in certain cases an alarm must be acknowledged before the notification is suppressed. Alarms will be logged when they are generated and also during the changes which occur during their life-cycle (acknowledgement, deletion, masking, etc.).

2.2.8.4 Alarm Testing

The user will need to be able to test all alarm conditions, when they are defined or modified, and at regular intervals, without interfering with the operation of the DCS or the experiment equipment. In its normal state the detector does not produce alarms and it is very often undesirable to introduce abnormal situations by radically changing physical conditions (pressure, temperature, leaking gas, smoke, etc.) to force parameters into alarm. Therefore, testing the response of the DCS to multiple, complex alarm combinations is only possible if they can largely be simulated. To best verify the response of the DCS to such conditions, the alarms would need to be simulated as close to the beginning of the alarm handling chain as possible. Any additional software/hardware used to test alarm conditions must not interfere with the normal operation of the DCS or experiment and should in general be fully disabled during normal operation.

2.2.9 Acquisition and Processing of Measured Parameters

The acquisition of measured parameters is largely experiment specific. That is to say hardware interface and driver dependent. However, the kernel DCS must provide standard functionality to support experiment specific hardware.

The user should be able to perform acquisition of parameters either in a synchronous or in an asynchronous manner. Furthermore, the user should be able to define the acquisition frequency (in the case of polling) or the dead-band range (in the case of change driven acquisition). The user should also be able to request the acquisition of a parameter, in order to view the current value, outside of the normal acquisition cycle for this parameter.

The kernel DCS should provide some basic process control function blocks that can be selected for building a process control application for a particular device, e.g., Proportional Integral and Derivative (PID) controller. Furthermore, all parameters, measured or derived, shall be handled in an identical manner by the DCS, as such it should be possible to display, trend, archive derived and measured parameters.

2.2.10 Commanding

The user must be able to issue commands to the experiment equipment. A user initiated command can either result in a single command for an individual device or as many commands at the device level.

2.2.11 Operational Modes and Event Handling

The DCS will be used to control both a detector with all or a subset of sub-detectors, as well as sub-detectors and subsystems individually. Furthermore, for different physics data taking periods different combinations of sub-detectors may be required. Therefore many different configurations will need to be operated, and potentially even multiple configurations at the same time.

It must be possible to define and save the parameters for each configuration. The user should be able to easily retrieve a particular configuration, together with all default set-values for that configuration.

The user shall be able to define events after whose occurrence defined actions are initiated, e.g., a sub-detector changes state which might be required to cause another sub-detector to change states.

2.2.12 Archiving and Retrieval of Data

All measured and derived parameters must be archivable with a time stamp. It must be possible to define which parameters are to be archived. Whether a parameter should be archived and the frequency at which it should be archived should be variable, either manually by the operator, or automatically triggered by events or alarms.

The user will wish to retrieve data to support troubleshooting activities or to perform some analysis on the archived data, e.g., trending. In principle the user should be able to retrieve data based on the value or condition of any parameter defined in the DCS, including those input from external systems. The user may wish to retrieve the data to data files, to histograms, to X-Y plots, to trending displays or to standard tools such as a spreadsheet application.

2.2.13 Logging

The kernel DCS shall provide automatic logging of commands, events, alarms, and actions. The purpose of these logs is both to support the users of the DCS in their day to day activities, and also to support troubleshooting activities in the event of problems. As such the log entries should be time-stamped and should include all necessary information required for these purposes. Of particular importance, in the case of user actions or user initiated commands, is that the user concerned is indicated in the log entry.

It must be possible for the user to easily view only selected information. All information in the logs must be the same for all users from all locations, i.e., that all information is logically unique in the DCS.

2.2.14 Operator Support

2.2.14.1 Operator Display

User displays will in general be experiment specific and therefore not part of the scope of the kernel DCS. However, the kernel DCS should provide the tools for displays to be developed in a straight-forward manner and with the same ‘look and feel’. As an example there could be a library of elements which could be used to build a display window. Displays should have:

- Same representation of alarm states, state of devices, masking, etc.
- A standard set of symbols and dialogue boxes
- A standard menu structure and command item naming
- A standard method to open, close, iconise, move and re-size windows

The following capabilities are required:

- Create displays using widgets from a DCS kernel provided widget library
- Configure displays both on-line and off-line
- Create interactive displays
- Define links between windows (e.g., hyperlink style)
- Multiple windows
- Quick navigation between windows

2.2.14.2 Operator Assistance

Many of the users of the DCS will not be experienced users and may not have received detailed training in its use before arriving at the experiment from their home institute to operate the detector. To compensate for this the kernel DCS shall provide an extensive on-line help facility which will provide the user with a complete set of information necessary to operate the DCS.

Most of the information will be experiment specific. Nonetheless, the kernel DCS should foresee a help facility to which the detailed information can be added by the experiment experts. The help facility should be context sensitive to simplify its use and to allow the user to obtain information in a specific area easily and quickly. Furthermore, an electronic log book should be provided.

The detectors and the interactions between elements of the experiment equipment will be very complex. This means that the true source of an anomaly situation will not always be clear and may take extensive investigation to identify. Furthermore, such investigations will often require very detailed knowledge about one or more elements of the experiment equipment. To assist in the diagnosis of such complex anomaly situations and to aid recovery from them, access to an expert system should be provided.

2.2.15 Development Environment

The kernel DCS will be configured for the needs of each experiment. Each experiment will have a number of sub-detector teams which will be responsible for the specific configuration for their own sub-detector. It must be possible for these teams to work largely independently during the development phase, i.e., the work being performed by one sub-detector team should not influence the work being performed by another sub-detector team. Furthermore, it must be possible for the people working in a sub-detector team to work in a multi-development environment, i.e., without interfering with each other.

As such, the kernel DCS must provide a development environment that supports this way of working, i.e., multi-user access to data in a controlled fashion, separately accessible data for different sub-detectors, configuration control of data and applications, etc.

The development environment should provide sophisticated facilities for debugging and testing of applications developed using the tools provided by the kernel DCS and for simulating aspects of the operation of the detector such as complex alarm conditions.

2.2.16 Supervision of DCS

The DCS will be comprised of a number of hardware items (workstations, VME crates, etc.) with software applications running on them. To ensure good operation of the experiment equipment it is essential that the DCS also performs as desired. Therefore, it will be necessary to monitor the behaviour of the DCS and its components, to highlight anomalies to the user when they arise and for the user to be able to take corrective action as and when necessary.

2.2.17 External Interfaces

To enable the kernel DCS to interface not only to external systems but also to experiment specific applications and equipment, an Application Programming Interface (API) providing a full range of functionality shall be provided. This API will allow the user to access the full range of the kernel DCS functionality and data contained in the DCS from external applications. Furthermore, the API will provide the possibility to exchange data with all other LHC systems.

The DCS must exchange information with different external systems as given in section 2.5.2. In general this will be status information which is required by the DCS or of the DCS by other systems.

2.3 General constraints

The kernel DCS will be used as the basis for the DCS for each of the LHC experiments. As such, it must be easily configurable and allow for experiment specific applications to be easily interfaced. The configuration of the kernel and the development of experiment specific applications will be done by many teams working in parallel. The kernel DCS must provide a multi-user development environment and allow for sub-sets of the final DCS to be developed independently from each other, but ensure that these developments can easily be integrated in a final system.

The LHC DCSs will be required to support the operation of the LHC experiments over a long life-time and during this period experiment hardware will be changed. Hardware will be added, removed, upgraded or modified. The DCS will have to accommodate such changes. Therefore, the kernel DCS must be easily configurable for the various needs of the LHC experiments, it must be easy to maintain over the long operational life-time, and must enable changes to the experiment configuration to be easily accommodated.

Furthermore the requirements on the DCS are likely to change both during the development and also during the operational life-time of the LHC. As such, the kernel DCS should be developed, where possible, in a way that would allow changing requirements to be accommodated with the minimum impact.

The kernel DCS must be designed, and documented, in such a way as to minimise the resources required for maintenance of the DCS during its operational life-time. Therefore, it is desirable that the DCS, wherever possible, uses the same underlying technology as the DAQ system, e.g., processors, networking, etc.

The long experiment life time requires technologies and products to be used which will be supported, adapted and maintained throughout the life time of the experiment.

2.4 User characteristics

The operational concept, and therefore type of users, is not yet well defined and is also likely to be modified. Therefore, the below gives only a possible scenario as an indication of what will be required.

In general all users of the DCS will have scientific backgrounds and considerable computer and programming experience.

Detector Operator. A shift operator responsible for running the detector as a whole. In general he will have an overall knowledge of the detector, perhaps detailed knowledge of one sub-detector, but no detailed knowledge about the other sub-detectors. He will be a physicist from the experiment collaboration who will act as a shift operator during infrequent short periods of time, and will not have a detailed knowledge of the DCS before commencing his duty.

He will require information about the overall status of the detector and to be informed of anomaly situations via alarms. In alarm situation he will need to be able to obtain sufficient information to be able to decide what action needs to be taken. In general he will call in a sub-detector expert to perform the detailed trouble-shooting and to perform corrective action. He will have access to all data but only to a sub-set of commands necessary for the day-to-day running of the detector.

Sub-Detector/Subsystem/Equipment Expert. He is an expert for a particular *sub-detector/subsystem* and is responsible for maintaining that sub-detector/subsystem/equipment in the desired operational condition. He will have detailed knowledge of his sub-detector/subsystem/equipment and will also be well trained in the use of the DCS. His privileges are limited to a sub-detector/subsystem/equipment.

Sub-detector/Subsystem Configuration/Maintenance Expert. An expert responsible for the maintenance of the DCS configuration database. He will be well trained in the use of the DCS. He will be responsible for a single sub-detector/subsystem and will have access to the configuration database. He will be able to modify the database in the case of changes to the sub-detector/subsystem configuration and verify those modifications.

DCS Expert. He is a person with detailed knowledge of the DCS and its operation. He will be responsible for maintaining the DCS during the life-time of the experiment. As such he will perform trouble-shooting and fix problems with the DCS software and perform upgrades when necessary.

DCS Administrator. He is a person who will be responsible for creating and maintaining user accounts with the appropriate level of privilege.

Collaboration Member. Any other member of the collaboration who wishes to monitor the status of the detector. He will have access to monitored data, but will not have access to any command capability. In general a collaboration member will not have a detailed knowledge of the DCS.

2.5 Operational environment

2.5.1 Operational concept

The *normal* way of operating the experiment will be with a limited number of people on shift (2 or more) sitting in the control room with some global directives on how the experiment has to run as a whole but without a deep understanding of all the equipment which is under their control. The normal way of operation covers the day-to-day physics data taking during the periods of nominal LHC operation.

The rest of the year, which accounts for a similar order of magnitude of time, the DCS will be used in a less organised way. There will be periods of maintenance, new developments, commissioning, debugging or shutdown. It is desirable to have some degree of autonomy between individual sub-detectors or subsystems. In such cases the interference between subsystems should be minimised. The people working with the equipment will typically be in different geographical locations: at the detector, in the control room, in an office at CERN or even at the home institute.

The people on shift will be confronted with alarms, misbehaviours of the detector equipment, and other abnormal situations from time to time. They need to have instructions associated with the alarms and error conditions. In many cases they will need the help of an expert in the domain where the problem occurred (sub-detector or subsystem expert). The domain expert is not necessarily the developer or integrator for this domain. These experts will be called in and requested to intervene in order to diagnose and eventually fix the problem. They have the knowledge of which devices or equipment are part of their domain. For example, they know how many power supplies their sub-detector has and where they are physically located. This information is valuable in order to localise a broken power supply and replace it. The sub-detector expert will interact with the control system from different places: down in the experimental area, in the control room, in an office at CERN or possibly even from home.

The different sub-detector or domain specific process control will be integrated or developed by a team of people which are very knowledgeable of needs in their domain. They will set-up the subsystem and commission it. They will need a very low access level to the equipment in order to be able to debug it. Their access will be using physical addresses which they map directly to physical cables. They will work very close to the physical equipment.

2.5.2 External interfaces

The efficiency and performance of a HEP experiment depends on the operation and interaction of a large number of systems. These systems each have a specific task to perform, but to do so need to receive data from, and to pass data to, some of the other systems. The DCS is no different in this respect. The DCS must interact not only with the detector hardware it is controlling, and the end user, but also the following systems:

- Run Control - the purpose of the interface is to allow information on the status of the DCS to be passed to run control and to allow data providing information on the status of the experiment run to be received

- DAQ/Trigger - the purpose of the interface is to allow slow control data required for data reconstruction and calibration to be passed to the DAQ/Trigger system

- Equipment Safety System - the purpose of the interface is to receive data providing information pertaining to equipment safety which would influence the operation of the experiment

- Personnel Safety System - the purpose of the interface is to receive data providing information pertaining to personnel safety which would influence the operation of the experiment

- Accelerator Control System- the purpose of the interface is to allow data providing information relating to the characteristics of the beam to be received and to provide the accelerator control system with information regarding the status of the experiment and whether it accepts the beam

- Infrastructure control systems (i.e., power distribution, cooling, ventilation, cryogenics) - the purpose of this interface is to allow data providing information on the status of these systems to be received

- Magnet Control System - interface tbd

The kernel DCS must therefore provide a flexible Application Program Interface (API) which allows data to be exchanged with the above named systems, and for experiment specific applications to be interfaced to the kernel DCS.

A context diagram, with accompanying text, should be included here once the interfaces to other systems are clear.

2.5.3 Hardware architecture

The DCS will operate in a distributed environment. Multiple front-end machines will provide the interface to the experiment hardware and these will be connected via a LAN to a number of client/server workstations.

Due to the dynamic nature of the experiments, the DCS will undergo continuous modifications and extensions. Consequently, prime features of the architecture must be scalability, modularity and openness.

2.6 Assumptions and dependencies

This document assumes that a common control system kernel will be provided for the four LHC experiments. This control system kernel will be used as the basis of all the DCS systems, but potentially could also be used for other applications such as run control.

It is assumed that the first issue of this document will be used as the basis for an evaluation of different development strategies/products. As the experiment development proceeds and more knowledge about the control needs becomes available the requirements in this document may be expanded to include more detail. However, the document will remain experiment independent. The experiment specific requirements would have to be addressed in additional URDs.

It is assumed that the safety of personnel and the basic safety of experiment equipment is guaranteed by a separate system and does not depend on the correct operation of the DCS.

3 Specific Requirements

It should be noted here that due to the current scope of this document, many of the user requirements given in the following sections are not true URs in the PSS-05 sense, i.e., they are not verifiable. This is intentional for the current version of the document.

The URs are composed as shown below:

Explanatory text

UR Identifier

UR Text

Each has a unique identifier and associated requirement text and may also be proceeded by explanatory text in italics

3.1 Capability Requirements

3.1.1 General System Features

3.1.1.1 Access Control

Access to the DCS must be restricted to only those users which are authorised to use it. As such the kernel DCS must include security features which require a user to identify himself, e.g., login. The user will then be able to access only the functionality to which he has an appropriate level of privilege.

ACC001

The kernel DCS shall require all users to identify themselves.

ACC002

Only authorised users of the kernel DCS shall be able to gain access to it.

ACC003

The user shall only be able to perform actions corresponding to his level of privilege at the time.

In general multiple users of the DCS will have the necessary privilege to access a piece of equipment and modify its behaviour. It is undesirable that two of more users should be modify the behaviour of a piece of equipment at the *same time, and as such the kernel DCS should prevent this occurring. As a minimum, the kernel DCS should generate a warning of the conflict. Furthermore, a user should be able to 'book' a piece of equipment to work. However, during periods where this facility is deemed not to be required it should be possible to disable this feature.*

ACC004

The kernel shall provide facilities to prevent users from modifying the behaviour of equipment simultaneously.

ACC005

A user shall be able to book equipment, whereby no other user can have write access to that equipment during the period it is booked.

ACC006

It shall be possible to disable the booking feature of the kernel DCS.

To avoid the situation where a user has control of experiment equipment or DCS resources and cannot be contacted, and thus hinders the work of others, it must be possible to log him out of the DCS remotely. This should be done on request from the control room.

ACC007

The kernel DCS shall allow for a user to be logged out of the DCS from the control room.

3.1.1.2 Types of access

It must be possible for users to access the DCS from locations other than a central experiment control room.

ACC008

The kernel DCS shall provide the capability for a user to be able to access the DCS from a variety of locations:

a) experiment dedicated areas - central detector control room, auxiliary control rooms, experimental equipment area

b) remotely - CERN office, office at the institute of a member of the experiment collaboration, from home

Different users will wish to interact with the detector, or parts thereof, at different levels, e.g., the detector operator will be interested in the detector as a whole, whereas a sub-detector expert will only be interested in one particular sub-detector. At the lowest level, during configuration and/or troubleshooting a user may be interested in accessing a device at the physical layer, i.e., the physical I/O addresses of a specific parameter.

ACC009

The user shall be able to access the kernel DCS at different levels of abstraction.

It is envisaged that users who would normally access the DCS using a group account, e.g., detector operators, in the control room should not be entitled to the same level of privilege when accessing the DCS from outside of the control room. In such a case any user accessing the DCS from outside of the control room using a group account should have a lower level of privilege.

ACC010

The user's level of privilege shall be configurable depending on his location.

In general many users will wish to interact with the DCS at any time. The users wish to be able to interact with the kernel DCS without being aware that other users are interacting with the DCS, e.g., only the user issuing a command should be informed of a transmission failure, i.e., the kernel DCS should provide the facility to establish a "session" with each user accessing the DCS individually. However, this should not apply to global actions such as alarm acknowledgement.

ACC011

The kernel DCS shall provide the facility to establish an individual session with each user.

3.1.1.3 Users

A user of the DCS will be granted a set of privileges which is dependent on his responsibilities. The DCS Administrator will have the capability to define user accounts with the appropriate level of privilege.

USE001

The DCS Administrator shall be able to define user accounts and assign the appropriate level of privileges to them.

USE002

When accessing the DCS the user shall have a set of privileges assigned to him, which shall be dependent on his responsibility and the type of access.

The set of privileges assigned to a user will define to which devices he has write access, i.e., the ability to modify the behaviour of a device, which configuration parameters he can modify, which command procedures he can initiate or which operations of the DCS he can influence.

USE003

The user's privileges shall define the following:

- which devices he has write access to
- which configuration parameters he is entitled to modify
- which commands he can initiate
- which functions he has access to

The user may wish to work with a lower level of privilege to avoid making mistakes. In this case he should be able to select a lower level of privilege at any time.

USE004

A user shall be able to select a sub-set of his privileges to work with.

USE005

The DCS expert shall be able to define actions for which an acknowledgement is required before the action is executed.

3.1.1.4 Definition and Configuration of Experiment Equipment

The kernel DCS will have to be configured for each experiment individually. Part of this process will be to define the devices which have to be monitored and controlled. This has typically been a very time consuming task for previous experiments. The kernel DCS should provide sophisticated tools to simplify this task. For instance if there are 50 similar devices being controlled, e.g., high voltage power supplies, it should be possible to define one and to duplicate it. The duplication process should also duplicate all associated configuration information. Furthermore, it is desirable that the tools allow for automatic generation of parameters that are unique for each device, e.g., parameter IDs, following a pre-defined schema during the duplication process.

DEF001

The sub-detector/subsystem configuration/maintenance expert shall be provided with tools that allow him to define and modify the equipment to be monitored and controlled.

DEF002

These tools shall provide powerful facilities to allow the user to define and configure experiment equipment in an efficient manner.

DEF003

These tools shall perform consistency checks on the configuration information being defined or modified, e.g.,

- Ensuring that parameter names are unique
- Ensuring that all information is self consistent, e.g., that high limit bands are larger than low limit bands
- Ensuring that referenced parameters exist
- Ensuring that all the required information has been entered

It is envisaged that the control of a detector will be organised in a hierarchical fashion and that the operations will be defined for devices or groups of devices rather than individual I/O parameters. It should be possible to define actions which can be performed on such object and the sequence of control resulting from these control actions.

DEF004

The user shall be able to define objects representing the behaviour of some part of the detector.

DEF005

The user shall be able to define control actions which can be performed on such objects.

DEF006

The user shall be able to define the sequence of control which results from each control action.

DEF007

The user shall be able to define a hierarchy of control corresponding to the detector hierarchy for such objects.

The detector equipment configuration is likely to continually change during the life-time of the detector and as such the configuration held in the DCS will have to be modified. The kernel DCS must allow for such configuration changes to be made on-line without the need to stop part or all of the operation of the DCS.

DEF008

The kernel DCS shall allow authorised users to modify configuration parameters (add, modify or delete a device) without the need to stop the DCS.

3.1.1.5 Definition of Commands and Procedures

COM001

The user shall be provided with a standard set of commands for monitoring and/or modifying the operation of the experiment hardware

The list might not cover the needs of all devices that can be foreseen for the LHC experiments and therefore it should be possible to define additional commands to add to the list of standard commands in a straight-forward manner.

COM002

The user shall be able to define and add new commands to the list of standard commands.

In order to simplify the operation of the detector a user should be able to perform standard complex actions without the necessity to initiate all the necessary commands individually.

COM003

The user shall be able to define commands which invoke a command procedure.

Whether a command in a command procedure should be executed, and when, can be dependent on one, or more, factors. Therefore, the user should be able to define the criteria to be met in order for the command to be executed.

COM004

The user shall be able select from a set of basic conditional commands which shall include at least the following:

- Timer, e.g., setting of a defined delay before the command is executed
- Sequencing, e.g., an instruction is only executed after the termination of a previous command
- User acknowledgement, e.g., the command is only initiated after a user confirmation
- Conditional execution, e.g., the command is executed only defined conditions are met

Before being accessible to the user via the operational system each command and command procedure should be fully tested to ensure its correct operation.

COM005

The user shall be able to test the correct operation of a command or command procedure.

The user will wish to monitor the progress of a command procedure to ensure that it is proceeding nominally. Furthermore, in the event of problems being detected he would like to be able to pause or halt the command procedure. During testing he will wish to perform interactive debugging of command procedures.

COM006

The user shall be able to access the following execution handling facilities for command procedures:

- Execution monitoring, i.e., the user must be able to monitor the execution of the procedure to see how the procedure is progressing
- Error handling, i.e., if an error exists the execution flow is terminated and control handed back to the user
- User control, i.e., the user should be able to perform the following actions on a command procedure; Halt, Continue, Step, Abort, Show Value

COM007

The user shall be able to obtain the current value of a parameter.

3.1.1.6 Hardcopy & Report Generation

The user will need to output information from the system or copies of screen shots during the course of his work. The output could be to a number of different devices, including printers, plotters and files.

REP001

The user shall be able to perform a WYSIWYG screen output at any time.

REP002

The user shall be able to select data from any data source within the system for output.

The user will require the capability to perform basic functions such as output device definition and configuration.

REP003

The user shall be able to perform basic functions such as output device selection and configuration.

User will need to output information concerning the status of the detector, or a subset thereof, on a regular basis. To simplify this task the user should be able to define the contents of reports and request that they be generated and output automatically.

REP004

The user shall be able to define reports for outputting which include any information available within the DCS (parameters, graphs, log entries, etc.).

REP005

The user shall be able to include spreadsheet calculations within the report.

REP006

The user shall be able to define when the report is to be generated, either at a specified time and/or at a specified frequency.

3.1.1.7 Alarm Handling

3.1.1.7.1 Alarm Definition and Generation

A facility should be provided which allows the user to define and modify alarm conditions in a straight-forward manner. An example of what is meant by straight-forward might be a graphical tool or programming language which allows the users to define complex alarm conditions (parametric algorithms), to define relationships to other alarm conditions, to assign alarm levels, and to define alarms which are state dependent by selecting from a set of pre-defined objects/using standard features of the language.

ALM001

The user shall be able to define and modify alarm conditions for detector equipment and the DCS in a straight-forward manner.

ALM002

The user shall be able to define alarm conditions which include complex relationships between parameters.

A device may have a behaviour which requires the definition of many alarm conditions, e.g., whether it is in the correct state, i.e., on or off, and whether a voltage is within a set limit. It may be necessary to set multiple limits for parameter corresponding to different levels of alarm severity.

ALM003

The user shall be able to define multiple alarm conditions for a piece of equipment.

A piece of equipment may have a different expected behaviour in different operational states, not only its own state but also that of other devices, subsystems, sub-detectors, or the detector itself, e.g., a voltage limit may depend on whether the detector is off, in stand-by, or in data taking mode

ALM004

The user shall be able to define alarm conditions which are state dependent. The alarm condition may be based on the state of an individual piece of equipment, a subsystem, a sub-detector or the experiment itself.

Not every alarm situation will have the same level of importance/urgency. Therefore it will be necessary to define several levels of alarms to allow the user to easily sort the alarms by priority level when they occur.

ALM005

The user shall be able to associate one of a number of alarm severity levels to each alarm condition.

ALM006

The number of alarm severity levels shall be configurable.

It is desirable that alarms can be handled in an organised manner, e.g., hierarchically or in groups. As such it should be possible to define such relationships between the various alarm conditions.

ALM007

The user shall be able to define relationships between alarms.

ALM008

The user shall be able to define alarm handling based on the relationship between alarms.

ALM009

An alarm shall be automatically generated when an alarm condition is detected, except in the case defined in ALM010.

In certain circumstances it is known that after commanding a device will require a certain time to reach its desired state or value. During this period the user will not wish to be notified that the device is not in the desired state.

ALM010

The user shall be able to define conditions for which an alarm generation is suppressed for a defined period of time.

3.1.1.7.2 Alarm Management

The users of the DCS require different information. Furthermore, they wish to see alarm information in a manner which allows them to quickly identify the real source of the anomaly.

ALM011

The kernel DCS shall provide facilities to filter, merge or summarise alarms.

ALM012

The user shall be able to manage alarms in a hierarchical manner.

In the case where one anomaly situation gives rise to multiple alarms it is desirable that only the alarm which is a direct result of the anomaly situation is shown to allow the user to more quickly identify and deal with the real cause of the anomaly situation.

ALM013

The user shall be able to define conditions in which alarm logging and notification of one or more alarms is suppressed if another specified alarm is active.

In the case where a piece of equipment is known to be faulty or missing the user will not want to receive alarms from it. Therefore he may wish to mask all alarms originating from this equipment. However he will need to be able to view which alarms are masked at any one time in order not to forget.

ALM014

The user shall be able to mask alarms from individual pieces of equipment or defined sets of equipment.

ALM015

The user shall be able to view all masked alarms with the current value and/or status of the parameter/device for which the alarm corresponds.

In some case it may be desirable for a certain action to be initiated automatically in an alarm situation, e.g., to switch a piece of equipment off, to initiate some procedure, to generate an Email or telephone call to the person responsible.

ALM016

The user shall be able to define automatic actions to be performed in the case of an alarm condition being detected.

It is important that the same information about an alarm is available to all users of the DCS, e.g., whether it is active or not, whether it has been acknowledged or not, i.e., the status of the alarm should be consistent for all users.

ALM017

Alarms shall be handled as single logical entities by the DCS.

3.1.1.7.3 Alarm Display

The main purpose of an alarm is to report an anomaly situation to the users so that he takes action to fix the problem. This notification should gain his attention, e.g., bell, buzzer, flashing light.

ALM018

The user shall be notified of alarms in a manner which is suitable to gain his attention.

There may be times where the user is confronted with too many alarms to handle. In such cases he may wish to switch off alarm notification in order to deal with a particular problem without being interrupted.

ALM019

The user shall be able to switch off alarm notification.

In general when an alarm condition has disappeared the user will not want to be notified about the alarm any further. However, in exceptional cases it may be important for the user to be aware that an alarm has occurred even if the alarm is no longer active.

ALM020

Alarm notification shall cease as soon as the alarm condition has disappeared, except in the case described in ALM021.

ALM021

The user shall be able to define alarms for which acknowledgement is required before alarm notification can cease.

In general the user will only be interested in a sub-set of alarms.

ALM022

The user shall be able to select the alarms he is to be notified of from pre-defined subsets of alarms.

ALM023

The user shall be able to acknowledge alarms either individually or in groups.

In order to deal with an alarm a user may require additional information about that alarm. It should be possible for him to access further information, including a description of the action that should be taken.

ALM024

For each alarm the user will be able to request further information detailing what action is required to be taken.

The alarms should be logged with their associated history, e.g., when it became active, if and when it was acknowledged, if and when it ceased to be active.

ALM025

The alarms shall be logged and each alarm entry shall indicate all changes which occurred to the alarm during its life-cycle.

3.1.1.7.4 Alarm Testing

Before a new or modified alarm condition is entered into the operational system it must be possible to test its correct operation. The testing should be done in a way that is representative of the real alarm, e.g., through the simulation of the device behaviour. However, it must be ensured that the test activity does not interfere with the operation of the detector.

ALM026

The user shall be able to test alarms in a straight-forward manner without interfering with the operation of the DCS or the detector.

ALM027

The method of testing alarms shall be such that it is as representative of the true alarm situation as possible.

3.1.1.8 Acquisition of Measured Parameters

Acquisition of control parameters will be performed automatically by the DCS. The user must be able to define how the parameters should be acquired. This might be a set scan frequency (polling) or event driven (only when a parameter changes by more than a set limit) or a combination of the two.

ACQ001

The user shall be able to define a parameter’s acquisition either based on a set scan interval or event driven or a combination of the two.

ACQ002

The user shall be able to define the scan rate for parameter acquisition.

ACQ003

The user shall be able to define different scan rates for different parameters in a defined range.

At times the user will wish to view the current value of a parameter. That is to say to force a parameter to be read directly from the device outside of the normal scan operation.

ACQ004

The user shall be able to obtain and view the current value of a measured parameter.

3.1.1.9 Processing of Control Parameters

The kernel DCS should provide the user with a set of standard building blocks from which he should be able to build his process control algorithms, e.g., PID controller.

PRO001

The user shall be able select from a standard set of process control function blocks to build a process control algorithm for a device.

PRO002

The user shall be able to select any parameter in the DCS to be included in a process control algorithm.

3.1.1.10 Commanding

It is important for the user to be provided with a confirmation of a command's execution or on the other hand with any problems with its transmission and/or execution.

COM001

The user shall be able to verify the correct execution of his command.

COM002

The user shall receive a notification if the transmission or execution of a command fails.

3.1.1.11 Event Handling

The user will want the kernel DCS to have the capability to initiate actions when certain specified conditions are meet (events). For example, this action may be to modify the behaviour of a device or higher level object.

EVE001

The user shall be able to define events after whose occurrence defined actions are to be automatically initiated.

EVE002

The user shall be able to define actions to be associated with each event.

The action to be taken on the occurrence of an event can depend on the current state of the detector or a sub-detector.

EVE003

The user shall be able to define different actions depending on the state of a sub-detector or the complete detector.

3.1.1.12 Operational Modes

The detector will be run in a number of operational modes. It will be necessary to sometimes run a sub-detector in a stand-alone mode for testing purposes, as well as running the detector in an integrated mode. Even in the integrated mode it may be possible that one or more of the sub-detectors are not required for a particular run, and it may even be the case that one or more sub-detectors are required to be operated in a stand-alone mode in parallel to the integrated operation of the detector.

OS001

The user shall be able to run each sub-detector independently.

OS002

The user shall be able to run all or a chosen set of sub-detectors in integrated mode.

OS003

It shall be possible to run multiple configurations in parallel.

It must be possible for the user to define/select the run configuration in a straight-forward manner. Furthermore, to avoid the necessity to always have to define the run configuration, it should be possible to store a run configuration to be selected at a later date.

OS004

The user shall be able to define a run configuration.

OS005

The user shall be able to store the run configuration (recipes).

OS006

The user shall be able to select a run configuration from a stored recipe.

When a piece of equipment is known to be faulty or not present, or when the equipment is being handled locally, it should be possible to mask it. Masking a piece of equipment implies that the DCS is no-longer aware that the equipment exists, i.e., no alarms are generated for this equipment and no commands are sent to it.

OS007

The user shall be able to mask equipment.

3.1.1.13 Archival and Retrieval of Data

The user should be able to define which parameters are to be archived, at which frequency and on what conditions.

ARC001

The user shall be able to select which parameters are to be archived.

ARC002

The user shall be able to define for any parameter an archival interval or condition upon which archiving is performed.

ARC003

The archive entry shall include value, time and parameter identification.

ARCO04

The user shall be able to define whether a parameter is archived only upon change or at a set scan rate.

Due to the likely large amount of information in the archive it must be possible for the user to easily retrieve only that data which is of interest to him.

ARC005

The user shall be able to retrieve only that data which is of interest to him.

3.1.1.14 Logging

To assist in the day to day operation of the detector and to support troubleshooting certain information should be logged and be accessible to the users. Although all information should be logged by default, it will be possible to suppress alarm logging in certain circumstances, see ALM013.

LOG001

All user or DCS generated commands, alarms, events and operator actions influencing the operation of the DCS shall be logged.

The log entries should include supporting information to allow the user to identify what occurred and why. In particular, in the case of user initiated operations, the user concerned should be identified in the log entry.

LOG002

Each log entry shall be time-stamped.

LOG003

Log entries shall include defined supporting information.

LOG004

User generated commands and operator actions shall indicate the user concerned.

The user must be able to browse and sort the log applying defined filter criteria to allow him to view the information he is interested in without being overwhelmed with unnecessary information. He must also be able to select a subset of the entries for output (printer, file, etc.)

LOG005

The user shall be able to select for viewing only that information which is of interest to him.

LOG006

The user shall be able to sort selected log entries based on defined criteria.

LOG007

The user shall be able to select entries from the logs for output.

3.1.1.15 Operator Support

3.1.1.15.1 Operator Displays

To develop his displays a user shall be able to select from a library of pre-defined objects and symbols. He shall be able to associate monitor or control actions with these objects or symbols. That is to say he shall be able to associate a command with a button, which when pressed initiates the associated command. Similarly he shall be able to associate a monitor parameter with a symbol which changes depending on the value of the parameter. This change may be to show a representation of the value of the parameter, or to indicate the state of the device represented by the parameter, e.g., colour change. The set of pre-defined objects and symbols should cover the majority of the needs of a user when building a display. However, the user shall also be able to define additional objects where necessary and add these to the library. To this end an extensive range of graphics drawing capabilities should be available for the user.

DIS001

The user shall be able to build displays using pre-defined widgets from a library.

DIS002

The widgets shall have configurable control and monitor actions associated with them.

DIS003

The user shall have access to an extensive range of graphics drawing capabilities.

DIS004

The user shall be able to create new widgets and add these to the library.

In general displays will be configured by the users off-line. However, it should also be possible to modify displays also during DCS operation.

DIS005

The user shall be able to configure displays both on-line and off-line.

In general the displays should allow the users not only to monitor the behaviour of the detector, or components thereof, but also to perform control actions.

DIS006

The user shall be able to build interactive displays.

The user may use many displays during the execution of his duties. To most efficiently perform these duties he will need to be able to move between displays quickly, i.e., it should be possible to move from one window to any other window within 3 second (tbd). The speed at which this is possible is dependent not only on the speed of the physical process involved in selecting another window, but also in the ease of finding it.

DIS007

The user shall be able to navigate quickly between windows (< 3 secs tbc).

To improve the navigation between windows with a logical connection it should be able to define links between windows (e.g., hyperlink style).

DIS008

The user shall be able to define links between windows.

The user will wish to have multiple windows open at the same time.

DIS009

The user shall be able to have multiple windows displayed simultaneously.

DIS010

The user shall have access to the following analytical tools:

- statistical plots
- histograms
- trending charts (including historical and real-time data)
- standard spreadsheet functionality

The user will need to view many charts on a single display. The maximum number required is yet to be defined.

DIS011

The user shall be able to include up to multiple trending, X-Y or histogram charts in a single display.

DIS012

The user shall be able to modify the ranges shown on each axis in a straight-forward manner.

DIS013

The user shall be able to enlarge a single chart into full screen mode.

3.1.1.15.2 Operator Assistance

An on-line help facility should be available providing information concerning the operation of the DCS. This will cover the information necessary to operate the kernel DCS and utilise the full range of user facilities provided. It should also allow for experiment specific information to be added as the kernel DCS is configured for the needs of a particular experiment. The help facility should be context sensitive, i.e., the user is automatically provided with help information relevant to what he is currently doing.

ASS001

The user shall be able to access an on-line electronic help facility.

ASS002

The help facility shall include a context sensitive capability.

ASS003

The help facility shall provide all information required by the user to be able to operate the kernel DCS.

ASS004

The user shall be able to add additional information to the help facility.

Extensive documentation will be available regarding the operation of the detector and its constituent parts. This information can be of interest to users of the DCS. Therefore if should be possible to access such documentation from the system.

ASS005

The user shall be able to access all on-line documentation.

The user will wish to note information for later reference whilst using the system. Therefore he should have access to some form of electronic log book. To simplify the use of the log book a date stamp and the user name should be automatically added. The user shall be able to manipulate the information in the log book in the same way as other logs. See LOG006-8.

ASS006

The user shall be provided with an electronic log book.

ASS007

When entries are made in the log book a time stamp and the user name shall be automatically added.

Due to the nature of the detector an alarm situation may not be easy to interpret, and may require some expert knowledge of the detector and its equipment to do so. The majority of the users will not have this expert knowledge and will often need to call in experts. To reduce the reliance on such experts the kernel DCS should provide access to an expert system to aid in the diagnosis of complex anomaly situations and to eventually perform the appropriate corrective action.

ASS008

The user shall be able to call upon an expert system to support in the diagnosis and resolution of anomaly situations.

3.1.2 Development Environment

The development will be performed by many teams working in a geographically distributed manner. Therefore, the kernel DCS must by its inherent architecture or through provided facilities, allow this method of working to be performed in a way that allows the various developments to be integrated and to work together in a coherent fashion. These tools must identify inconsistencies between the developments performed not only between different teams, but also for developments performed within a team.

DEV001

Multiple teams of users shall be able to perform development in parallel in a consistent manner.

DEV002

The kernel DCS shall allow development of one part of the DCS to be performed without affecting development in other areas.

DEV003

Members of one sub-detector team shall be able to work independently from each other.

DEV004

The kernel DCS shall provide a configuration management facility.

DEV005

The kernel DCS shall allow data and applications developed by teams working separately to be integrated and tested.

DEV006

The kernel DCS shall provide facilities to check the consistency of data and applications during integration.

DEV007

The kernel DCS shall provide facilities for managing conflicts between multiple users of the same data.

The development environment should provide sophisticated facilities for debugging and testing of applications which have been developed using the tools provided by the kernel DCS and for simulating aspects of the operation of the detector such as complex alarm conditions.

DEV008

The kernel DCS shall provide facilities for debugging and testing of applications.

DEV009

The kernel DCS shall provide facilities for simulating experiment equipment in order to verify the correct operation of user developed applications.

3.1.3 Performance Aspects

The following gives a first list of performance issues that need to be addressed.

- Total number of measured parameters
- Rate of acquisition of measured parameters
- Number of alarm conditions that shall be evaluated per second
- Maximum number of simultaneous alarms that shall be handled (avalanche handling)

- Response time from the generation of an alarm to user notification
- Maximum time to bring up the DCS
- Maximum time to boot a DCS station and bring it into an fully operation state
- The response time for changing a display page shall be less than 1 second - tbc.
- The time from a change in a measured parameter being detected to the change being displayed
- The response time for the execution of a command from the time it is issued shall be less than 1 second - tbc.
- Maximum archival rate
- Archival duration
- The response time for the retrieval of data
- The time for a configuration change to take effect
- Precision of time-stamps - (1 second - tbc)

3.1.4 Supervision of Control System

3.1.4.1 Monitoring of DCS

MON001

The DCS shall check its internal operation on a regular basis.

MON002

The user shall be able to define the frequency at which the DCS monitors its internal working.

MON003

The DCS shall generate and report internal anomalies in the same fashion as alarms (see section 2.2.8).

MON004

The handling of DCS anomalies shall be done in an identical fashion to alarms (see section 2.2.8).

MON005

The user shall be able to view the current status of the DCS.

3.1.4.2 Control of DCS

CON001

The user shall be able to re-set defined parts of DCS without interfering with the operation of the rest of the DCS.

CON002

Loss of part of the DCS, client or front-end station, shall be recoverable without a complete re-boot of the DCS.

CON003

Commands to modify the behaviour of the DCS shall be subject to the same security measures as equipment commands.

3.1.5 External Interfaces

EXT001

The kernel DCS shall allow for data to be exchanged with the following external systems:

- Run Control
- DAQ/Trigger
- Equipment Safety System
- Personnel Safety System
- Accelerator Control System
- Infrastructure control systems (i.e., power distribution, cooling, ventilation, cryogenics
- Magnet Control System

EXT002

The kernel DCS shall provide a fully documented API.

EXT003

The API shall allow all functionality and data in the DCS to be accessed from external applications.

EXT004

The API shall perform exception handling in a way consistent with that of the application utilising the API.

EXT005

The ease of use of the API shall be similar to the use of a shell scripting language.

EXT006

The API shall allow synchronous and asynchronous utilisation.

EXT007

The API shall allow for re-synchronisation after asynchronous usage.

3.2 Constraint requirements

3.2.1 Adaptability

ADP001

It shall be possible to replace a single DCS front-end station without a loss of functionality of any other front-end station.

ADP002

It shall be possible for the functionality of a client or server station to be transferred to another station within 30 minutes (tbc).

ADP003

The kernel DCS shall allow full scalability up to the order of one million I/O parameters.

3.2.2 Maintainability

MAN001

The kernel DCS shall be maintainable for a life-time of 15 years (tbc).

MAN002

The kernel DCS shall be maintainable by a team of engineers who were not necessarily directly involved in the development.

MAN003

It shall be possible to upgrade the kernel DCS whilst maintaining compatibility with existing applications.

3.2.3 Availability

AV001

The kernel DCS shall be available 7 days per week 24 hours per day for periods of several months between scheduled maintenance.

3.2.4 Portability

In the life-time of the LHC experiments it is expected that the H/W will change. Therefore, it must be possible to easily port the kernel DCS to other H/W platforms and operating systems.

3.2.5 Documentation

DOC001

The kernel DCS URD shall be produced according to PSS-05.

DOC002

All kernel DCS documentation shall be available electronically.

DOC003

All kernel DCS documentation shall be available in English.

3.2.6 Standards

STD001

The kernel DCS shall comply to industry standards in the following areas:

- API
- Communications
- Programming languages
- Programming tools
- Database access

STD002

The kernel DCS shall be Year 2000 compliant.

3.2.7 Communications Interfaces

CIF001

The kernel DCS shall support the following field-buses:

- CAN
- Profibus
- WorldFip

CIF002

The kernel DCS shall support one of the following LANs:

- Ethernet
- ATM
- FDDI

CIF003

The kernel DCS shall support the following communication protocols:

- TCP/IP

3.2.8 Hardware Interfaces

The DCS will have to operate with a defined set of hardware. The final hardware is yet to be chosen.

HIF001

The client software shall be able to run on one of the following platforms:

- PC- tbc
- HP - tbc
- SUN - tbc

HIF002

The front-end system shall be able to utilise the following hardware:

- VME - tbc
- PLC - tbc
- PC - tbc

HIF003

The kernel DCS shall provide the following standard hardware drivers:

- tbd

3.2.9 Software Interfaces

SIF001

The kernel DCS shall run under a commercial operating system.

SIF002

The client software shall be able to run under UNIX and/or Windows NT.

SIF003

The front-end software shall run under at least one of the following real-time operating systems:

- LynxOS
- VxWorks
- OS9
- Windows NT

SIF004

The kernel DCS shall provide an API capable of interfacing to the following programming languages:

- C/C++
- Java

SIF005

The API shall be compliant with a recognised international standard

SIF006

The API shall not have to be changed as a result of changes in the experiment configuration.

SIF007

User application shall not have to be re-compiled as a result of changes to the API.

SIF008

The kernel DCS shall provide an API capable of interfacing to the following DBMSs:

- Oracle
- Objectivity

SIF009

The kernel DCS shall utilise a commercial RDBMS.

SIF010

The kernel DCS shall allow integration of commercial packages to perform the log book function.

SIF011

The kernel DCS shall allow commercial expert systems to be integrated.

3.2.10 User Interfaces

UIF001

The kernel DCS shall support multiple simultaneous users. The maximum number is still to be defined.

UIF002

The kernel DCS shall support independent development teams.

UIF003

The kernel DCS shall provide data driven displays.

UIF004

The kernel DCS MMI shall be configurable for the English language.

Given that users will wish to access the kernel DCS from may different locations, including home, it is undesirable that specialised hardware or software is required for this.

UIF005

The user shall not require specialised software or hardware to access the kernel DCS remotely.

3.2.11 Schedule

SCH001

The kernel DCS shall be available no later than … tbd.

4 List of User Requirements

A [Appendix Heading]