Statement of Work (SOW)

for STC2 & 3 Data Acquisition and Control (DAQ&C) System

Document Number:	**AIV-STC2_3-SOW-1004**
Issue:	**1**
Date:	**11TH July 2018**
Classification:	**Commercial in Confidence**

Contents

Introduction

Rutherford Appleton Laboratories (RAL) Space has 2 5m Diameter Vacuum Chamber in R100, referred to Space Test Chamber 2 and 3 (STC2 &3).

1 SCOPE

STC 2 &3 will be used for calibration and characterization testing of satellite instruments. The two chambers are very similar with minor differences. From now on we shall describe the system requirements for one chamber with the assumption that they are shared with the second chamber.

For the avoidance of doubt, the optional second system (for STC-2) that may be purchased should be considered as the same specification as the first system (STC-3) for the purposes of pricing.

There are 46 shroud panels covering the whole internal surface of the chamber and they provide temperatures ranging from -193C to 130C. Each shroud panel is cooled by a Liquid Nitrogen (LN2) system which involves distribution of LN2 from a LN2 tank outside R100 to the phase separator (installed on a mezzanine floor on top of the chamber) to 12 valve boxes distributed on the outside shell of the chamber. The valve boxes then feed the Liquid nitrogen to different panel zones. Each panel is heated by number of heaters which are powered by mains. Each shroud panel is instrumented with thermocouples for monitoring and control of the panel temperature. The chamber has a Cryogenic system consisting of a roughing pump and 5 Cryogenic pumps. These pumps are used to achieve operational vacuum pressures in the 1E-5 to 1E-7 mbars range. There are other systems that control operation of the chamber e.g. chamber door operation, cleanroom laser interlock and hence safety logic will be needed to prevent systems working in opposition to each other e.g. chamber door opening while cryogenic pumps are working to bring the chamber to vacuum pressures.

The scope of this document is to provide the specification for the Data Acquisition and Control (DAQ/C) System to cover the heating and cooling (done by the shroud panels) of STC 2 and 3. The DAQ/C needs to provide (See Appendix 1: STC2_3 Project Software Requirement Specification for details of software functionality to be provided):

- Control – The automatic and manual control of the chamber
- Safety – Ensure that the system complies with European Machinery Directives and Functional safety of electrical/electronic/programmable electronic safety (see section 2 for all relevant safety requirements
- Data Acquisition – Collection of required data from the Programmable Logic Controller (PLC) to be stored in a database
- Data Storage
- Security – a user configurable security system to ensure operators have access limited to their area of responsibility
- User interface to enable the operator to have visualisation and control of the processes
- Expandability- the ability of the system to interface and expand to include more and more systems e.g. interface with chamber vacuum system and door laser interlock.

- Redundancy- the system should provide redundant systems e.g. PSU's, RAID drives, data backups or possibly a live spare that can take over if primary system fails.

This system will fit in the overall management of functional safety plan. RAL space is working on a functional safety management plan, in parallel to tender, and will make this available to winning supplier before start of work. RAL space will also carry out Hazard identification and share this with winning supplier upon contract start.

To note is that LN2 safety is not within the scope of the STC2 &3 Chamber DAQ&C as such. The chambers heating & cooling controls will need to interface to the LN2 gas detection system e.g. Crowcon gas depletion system. The safety system of the chamber will interface to the Crowcon unit (or similar system). The gas depletion system will interface to the safety system of the chamber. The supplier of the controls system will need to supply a full SISTEMA document for the safety system of the chamber as per BS EN 13849 1/2 SRP/CS (Appendix has an example of a SISTEMA Plan).

2 DAQ/C SPECIFICATION

This section defines the Basic Materials and Methods provided by the Controls Contractor and used in the installation of network control products to provide the functions necessary for control of the various systems in the chamber. Please be advised that the requirements of this specification will be strictly enforced. Systems that do not meet the requirements of the specification as outlined below will not be accepted.

The proposed DAQ/ C solution shall be in compliance with the following Safety Requirements:

- BS EN 13849-1/2 Safety Related Parts of Control System- This is the standard that should be used for Chamber Heating & Cooling controls. RAL space interprets this as a system/machine in its own right. The controls system for the heating & cooling of the chamber is independent of the process in that the panel will be CE marked and supplied as a machine. It is not intended that the design of the chamber's heating & cooling system should be responsible for all safety of the process. BS EN 13849 will only be use for the safety within the heating e.g. E/stop will shut down power to heaters (Cat & PL's).
- European Machinery Directive 2006/42/EC
- EN/EC 60204 Safety of machinery. Electrical equipment of machines. General requirements
- EN/IEC 13850 Safety of machinery. Emergency Stop. Principles for design
- EN/IEC 62061 Safety of machinery. Functional safety of safety-related electrical, electronic and programmable electronic control systems
- EN/IEC 61508 Functional safety of electrical/electronic/programmable electronic safety – related systems

- The System shall include a safety PLC (Rockwell, Omron or other technically equivalent), that can be integrated within a standard PLC
- **Desirable (Not Part of the Mandatory Specification):**, Safety PLC should allow expandability via RAL space preferred Fieldbus i.e. EtherCat.
- The system shall be limited to only one fieldbus and shall have the functionality to easily add to the facility control System additional inputs/outputs, servers, laser safety and other functionality. If expansion requires any changes to proposed system configuration (except for hardware related to new functionality) these should be detailed in your response. Minimal or no changes to the configuration are preferred.
- The control system shall utilize an open, industry standard networking communication protocol and network management system to provide direct access to each device. All messaging on the system shall provide direct peer-to-peer communication capability and provide for device level interoperability. The system shall implement a logical flat, physically tiered architecture model in order to ensure interoperability and remove any closed system elements.
- No closed network communication elements will be allowed and will be strictly enforced.

No non-open communication to devices from network tools, host interfaces, or enterprise level applications will be permitted.

- All data flow on the network shall be fully published and documented. No vendor specific closed communication will be allowed.
- The system shall consist of interoperable devices, standard routers, standard network interfaces, standard IP communications (if required), and open user interfaces. No closed system components will be permitted including custom gateways (unless expressly defined below), logically tiered hardware or software architecture elements, or closed system tools.
- All systems and subsystems shall be capable of being serviced and maintained internally or by a third party service organization. Under no circumstances shall any hardware or software be implemented such that the property will not be able to provide access to a service organization of our choice.
- The contractor shall supply all hardware, software, databases, configuration tools, commissioning tools, analysis tools, and software plugins upon delivery. All tools shall be properly licensed and conveyed. All original software, software keys, and licenses shall be conveyed such that RAL space has full access and usage rights to all components.
- The contractor shall follow all industry standards and relevant guidelines for the control network, device selection, network wiring, configuration, and commissioning.
- The contractor shall demonstrate their ability and intent to fully complete this project as specified. No alternate bids or exceptions will be accepted. The contractor shall demonstrate their knowledge, ability, and experience in providing the system as specified.

3 WARRANTY

- The contractor shall provide a full and complete system warranty for a period of two (2) years commencing after final project sign off.
- Contractor warranty shall provide full system functionality, parts replacement, labor, software and hardware upgrades necessary to ensure full system functionality during the warranty period.

4 SERVICE

- Contractor shall provide service contract costing for 3 years after the end of the warranty as a separate cost. Service contract costs must be defined as an annual cost for full servicing. This cost shall be defined as an annual cost for years 1, 2 and 3 separate from the initial installation bid. The Service provision should include as a minimum: quarterly visits to evaluate performance of the equipment and make any remedial corrections that are necessary.

5 SERVICEABILITY

- The contractor shall provide a fully serviceable system with complete access to all system components, controllers, sensors, panels, wiring junction boxes. All elements of the system must be accessible by maintenance staff.
- Ensure all cabinets, enclosures, and installations are accessible without hindrance. Provide all cabinet keys with clear indications to their location.

- No contractor or vendor proprietary service tools will be allowed. All service tools shall be included as part of this bid.

6 TRAINING

- Training shall be provided on the full operation of the control system.
- Training shall be provided for all network management, commissioning tools, and network diagnostic and analysis tools.
- Training shall be provided on the system architecture, basic protocol capabilities, and servicing of the system
- Training shall be provided on all device configuration and programming tools
- Training shall be provided on site at the Rutherford Appleton Laboratory for a minimum of five members of staff

7 DELIVERABLES

7.1 A procured and installed DAQ/C system for STC-3, and an option to purchase a further system for STC-2

7.2 Training on operation of the DAQ/C system(s)

7.3 A technical file (IAW table below) for each DAQ/C system (STC2 &3) delivered.

Technical File Inclusions

Section One : Risk Assessments		Signature
1A	Safety Related Control Circuit Assessment	
1B	Risk Assessment	
1C	Support Documentation For Assessments	
Section Two : Essential Requirements		
2A	Essential Health & Safety requirements	
2B	Complete detailed drawings showing conformity with the EHSR	
2C	Calculation notes, test results showing conformity with EHSR	
2D	Electrical Checklist	
2E	Pneumatic Checklist	
2F	Hydraulic Checklist	
Section Three : Standards		
3A	The Standards used	
3B	Reports and test results required by the Harmonised Standards	
Section Four : Certification and Specifications		
4A	Any Technical specifications	
4B	Certificates or Technical Reports obtained from a competent body supporting conformity (optional)	
Section Five : Drawings		
5A	Overall Drawings	
5B	Drawing of Control Circuitry	
5C	Specific Drawings	
Section Six : Manuals		
6A	Instruction Manual in the language of the country of intended use	
6B	Maintenance Manual	
6C	Other Manuals	
Section Seven : Series Manufacture		
7A	For series manufacture internal measures implemented to ensure machinery remains in conformity with the Directive	
Section Eight : Other Documentation		
8A	Any Other Documentation Showing Support For Product	
Section Nine : Declarations/ inclusions		
9A	Declaration of Conformity/Incorporation	

EHSR: Essential Health and Safety Requirements

7.4 Warranty for DAQ/C systems

8 ACCEPTANCE TEST

- Deliver a fully functioning, complete, serviceable system.
- All devices shall be fully programmed and commissioned and all systems and subsystems shall be demonstrated to be fully operational during an acceptance

test.

9 DESIGN REVIEW MEETINGS

After placing the contract, RAL Space requests that there be two review meetings.

Preliminary Design Review

- The meeting will occur four weeks after placing the order;
- It will be held at RAL Space in order to review the system layout;
- No less than one week's prior to the meeting, the Chosen Supplier will issue provisional General Assembly drawings based on the enquiry specification as discussion documents.
- The project plan, test plan and service/maintenance requirements will be reviewed.
- The agenda for the Critical Design Review meeting will be agreed.
- The objective of the meeting is to confirm the design, project plan and the test schedule.

Critical Design Review

- The time of the meeting will be advised by the Chosen Supplier, with no less than two weeks' notice, so that the meeting takes place prior to starting manufacture;
- It will be held at RAL Space
- No less than two weeks prior to the meeting the Chosen Supplier will issue manufacturing drawings.
- The objective of the meeting is RAL Space approval for procurement.

10 SCHEDULE

Assuming a contract award of 12th November 2018, procurement and Installation of DAQ/C system for STC-3 is requested by the 30 Jan 2019 and for STC-2 the 30th May 2019 (assuming this option is taken within one month of delivery and installation of the first System). Training is to be provided NLT 10 days after delivery and acceptance of each DAQ/C system. Contractor is asked to provide a detailed project plan to show how he/she can achieve the delivery date and major milestones and tasks involved in achieving completion date.

11 APPENDIX- STC3 PROJECT SOFTWARE REQUIREMENTS SPECIFICATION (SRS)

Contents

1 INTRODUCTION

This System Requirement Specification (SRS) is written to cover the software requirement of the RAL Space R100 STC3 5-metre vacuum chamber project. It details the software requirement in terms of Programmable Logic Controller (PLC), Database and Human Machine Interface/ Supervisory Control and Data Acquisition (HMI/SCADA) in order to provide functionality in terms of Control, Safety, Data Acquisition and Storage, Security and User Interface.

1.1 Purpose

This document should be used as the reference for a Functional Design Specification which will detail the design of the system to be implemented.

1.2 Scope

Area

Whilst the scope of this project is for STC3 5m chamber, provision should be made for modular inclusion of a second chamber (STC2). This SRS is for the provision of the chamber facilities only and does not include the requirement of RAL Space customer requirements.

Equipment

The scope of equipment can be broken down into 3 distinct sections:

- PLC
- HMI/SCADA
- Database

All Servers and Client machines shall be provided by RAL Space. The PLC hardware is discussed in the User Requirement Specification for Hardware (See 1.4 - References).

Functionality

This SRS has the following functional requirements, each of which shall be covered in detail later in this document:

- Control – The automatic and manual control of the chamber
- Safety - Ensuring that the facility complies with software control safety standards
- Data Acquisition – Collection of required data from the PLC to be stored in a database
- Storage of Data – Data should not be deleted but rather archived and made readily available when required
- Security – The system should have a user configurable security system so that operators are access limited to the areas that they are authorised for and are unable to make changes outside of their areas of responsibility/access
- A user interface such an HMI or SCADA (or technically equivalent) must enable the operator to control the process, have visualisation of the process in the form of mimics, tends and/or tables. There should be a current and historical alarms page. Data shall be served from an I/O Server to client nodes which have multiple screen capability. It shall also be possible for clients to access the system remotely through a WAN

1.3 Documentation

All software shall have sufficient commenting so as to provide a clear understanding of the code for software maintenance personnel. Where possible tag names and variables should be structured and descriptive so as not to be cryptic to anyone other than the software author.

This SRS shall be the reference for a Functional Design Specification (FDS) which shall detail the Software Design and be made available to RAL Space. This in turn shall be the reference for the Software Test Specification the purpose of which is to ensure that the completed project meets all the requirements laid out in the SRS.

A user manual shall also be provided to RAL Space so that users of the document will be able to use the interface after reading this manual. The manual should also include important reference notes to maintenance personnel.

1.4 References

The software requirement in this SRS is linked to the hardware requirement detailed above in the PR18119 Specification.

1.5 Glossary

ACK	Acknowledgement (comms integrity handshaking)
CPU	Central Processing unit
DB	Database
FDS	Functional Design Document
HMI	Human Machine Interface
I/O	Input/output
Nvarchar	String characters (they take up a lot of space in databases)
PID	Proportional, Integral, Derivative
PLC	Programmable Logic Controller
PV	Process Variable
RoC	Rate of Change Control
SCADA	Supervisory Control and Data Acquisition
SRC	Silicon Controlled Rectifier (Thyristor)
SQL	Structured Query Language
TC	Thermocouple
TCP/IP	Transmission Control Protocol/Internet Protocol
WAN	Wide Area Network

2 PROCESS DESCRIPTION

2.1 General Process

The facility comprises a 5m diameter vacuum chamber which contains thermal shrouds that are used for heating and cooling of the chamber. The chamber is divided into four areas from a controls perspective (two doors and two middle sections). There are 46 shrouds in total. On each shroud either 7 or 10 thermocouples are strategically placed to provide temperature feedback. From a control perspective the thermocouples, heating and cooling located on each shroud shall be known as a “zone”. The chamber is required to work in a vacuum in the 1E-5 to 1E-7 mbars pressure range. Four vacuum pumps are available to achieve this task.

2.2 Chamber Heating and Cooling

Heating

The chamber is heated using SRC switched AC resistive heaters. These are mounted directly onto each shroud. SCRs are mounted in panels next to the chamber at mezzanine level. Heating shall be controlled up to the range of 130 °C.

Cooling

Cooling is achieved by pumping Liquid Nitrogen (LN2) through channels embedded in the shroud. Control of the flow of LN2 is achieved through two valves mounted in series. Cooling shall be controlled down to the range of -170 °C.

Vacuum

The control of the vacuum system is currently achieved through a standalone proprietary hardware controller. There is a requirement to have the functionality of said controller built into the PLC controller and operator interface available on the HMI/SCADA.

2.3 Chamber Operation

It shall be possible to operate the chamber in two modes:

1 Out-of-Job
2 In-Job

Out-of-Job operation will have most of its data kept only for a limited time and then deleted. Only Alarms shall be kept on record. If there is no job present in the job data then the status will be Out-of-Job by default.
To start a job, it shall be necessary for an authorised operator to enter in the relevant job data and start a job. Once the job is started all data shall be booked against it and stored in separate tables designed specifically for In-Job data.

3 ARCHITECTURE

3.1 Programmable Logic Controller (PLC)

The PLC shall be structured as follows:

1. Control – The control shall be broken in to different sections for each zone under a common program. Use shall be made of user data types and common functions/function blocks in order to simplify the program and give it an object orientated structure.
2. Data Collection – The data shall be collected at specific intervals and stored in an array (buffer) in order to ensure that spurious interruptions to communication do not result in data leaks. The data shall be forwarded out of the buffer as quickly as possible. This means that data shall be emptied out of the buffer faster than is can accumulate and therefore empty any backlog in the buffer. Transmitted data shall be read back into the PLC to ensure data integrity (Acknowledgement (comms integrity handshaking)-ACK). The data is only cleared from the buffer once identical data has been read from the Database (DB). Alarms and messages shall be collected from the system.
3. Job Control – The PLC shall be aware of job control and shall communicate this data to the HMI/SCADA.
4. Variable Data – Relevant data such as setpoints, internal variables etc shall be logged in the same way as (2) above.
5. Alarms & Messages – These shall be reported to the DB as an Alarm/Message Number and stored using a buffer system and transferred in the usual fashion.

6. Audit Trail Logging – Wherever it is deemed necessary operator actions shall be reported from the PLC side back to the DB. These shall be numbered in the same way as Alarms/Messages and buffered the same way as any other data.
7. Housekeeping – A section shall be created under the Data Transfer program that allows for dynamic machine configuration as well as the transfer of system data such as a heartbeat for monitoring healthy communications, timeout values etc. Alarms, Messages, Audit Trails and Configurations will all be stored in the DB and editable from screens on the HMI/SCADA.

3.2 Database (DB)

With the DB:

1. A fully licensed Structured Query Language (SQL) Server 2014 shall be used. This shall be provided on a server supplied by RAL Space.
2. Once multiple servers exist, use shall be made of replication for the avoidance of data loss in the case of equipment failure. Separate servers need to be separate physical machines not virtualised onto one hardware unit.
3. The database shall be a relational database that uses a key system for normalise as far as possible through the reduction of repeated data, particularly nvarchar data.
4. The use of stored procedures shall be made wherever possible.
5. Wherever possible use should be made of Stored Procedures. This allows for the intervention of data by using triggers and protects against the use of SQL injection attacks.
6. Tasks shall be set up to delete old data as well as make regular backups. This is only possible with a licensed version of Windows SQL Server.
7. Data shall be archived in order to speed up searches but still be available to authorised users at any time.

3.3 HMI/SCDA (Human Machine Interface/ Supervisory Control and Data Acquisition)

The HMI/SCADA shall perform the following tasks:

1) Allow an authorised user to make changes to process setpoints including but not limited to Scaling of I/O reading, selecting multiple sources of I/O, changing of PID values, changing setpoints individually or as bulk changes which can be saved and recalled from storage, display of process values and provide situational awareness mimics.
2) Display trends of current (live) data as well as historical data.
3) Display Alarms in three places:
    a. Alarm Banner – To be shown on every screen (unless specifically stated). It shall be possible to acknowledge and clear alarms from this screen
    b. Current Alarms – To be shown on a dedicated alarm screen
    c. Historical Alarms – Previous alarms should be searchable on a dedicated historical alarm screen
4) Provides an Audit Trail of actions against a logged in user
5) Has a security system that can be maintained by a high-level user from the HMI/SCADA. The user can execute password changes without having to contact an administrator.
6) Navigate easily to different parts of the project with a minimum of operator actions.

7) Allow for replication with hot swap over. This includes the provision of handling middleware and driver failures.

The design should be as follows:

1) Object orientated. Allowing for easy duplication of objects which can produce variant child objects. There should be built in functionality in order for deployment to be both area based and equipment based. Objects created in the HMI/SCADA should match objects created in the PLC.
2) Easily interface with middleware drivers which are validated by the 3rd Party supplier.
3) The architecture shall use a Server/Client structure with the server handling PLC I/O.

3 ARCHITECTURE

3.1 General

Wherever possible there shall be support for dual redundancy at each level of the design. This includes:

1) Dual ethernet routing
2) Dual switches
3) Setting up of Dual Servers. This will facilitate the complete hot swap over from one server to another in case of failure
4) Multiple clients (Provided by RAL Space)

The main 4 components of the design are:

1) PLC – At the lowest level collecting information from the field and controlling required outputs. There shall be an interface with both the HMI/SCADA and a direct connection to the database.
2) Safety PLC – The system shall meet all relevant safety regulations and therefore have correctly programmed safety PLC.
3) Database – This shall be split into two distinct entities
    a. A historian which collects data as configured in the HMI/SCADA
    b. A database to handle direct data storage from the PLC
4) HMI/SCADA – This includes built in or 3rd party drivers or middleware

Apart from field equipment which can only communicate via RS485, all comms shall be ethernet (Transmission Control Protocol/Internet Protocol (TCP/IP)).

4 FUNCTIONALITY

4.1 PLC

I/O Requirement

The PLC shall be completely configured for all the hardware which is supplied in the PR18119 Specification. Raw I/O shall be passed to internal variables. After this raw I/O shall not be used in the working code of the PLC.

Database Requirement

The PLC shall be able to insert, update and select data directly from the database. This achieves the following goals:

1) Provides redundancy for critical data
2) Provides a separate data collection model which separates internal data from client data
3) Reduces overhead on historian data
4) Eliminates the need to store data such as configuration variables in the PLC

Measurement for Control

1) Reading of Temperature and Pressure sensors
   a) Temperature readings shall be read into the PLC via input cards and be scalable with at least two correction points in the range in the hardware configuration of the PLC. It shall also be possible to set an offset value. This shall allow for calibration which shall be the responsibility of RAL Space. It shall be possible for an authorised user to affect the user variable for each thermocouple from the HMI/SCADA.
   b) It shall be possible for each thermocouple to be individually discounted from the measurement system via the HMI/SCADA by an authorised user. The selected thermocouples for each shroud shall be averaged to produce an overall mean value.
   c) Provision shall be made for thermocouple readings to be used in an externally produced algorithm (e.g. A stored procedure in a database)
   d) Pressure measurement shall entail the straightforward scaling of inputs with the same two-point calibration discussed in (a) above.

Buffering

Buffering at PLC level shall be used wherever communication takes place with any entity which logs data (e.g. Database, HMI/SCADA). Buffering shall be sufficient to cover spurious loss of communication for up to 10 seconds without data leaks.

Control

1) Heating and cooling

   The following shall apply two heating and cooling control:

   a) Heating shall have two circuits (Outputs), namely “Heating” and “Trim”. It shall be possible to control each of these outputs so that only a percentage of the output shall be forwarded to the SCR control. Cooling shall have one circuit only.
   b) Both heating and cooling shall have two modes of control:

      i) PV Control

         This shall control the SCR (Heating) or Cooling Valve (Cooling Valve) outputs such that the PV is controlled about a user defined setpoint.

      ii) Rate of Change Control (RoC)

         This shall control the rate of change in temperature in °C/hr such that the measured RoC is controlled about a RoC setpoint. The RoC shall be determined by calculating a moving average.

   From The HMI/SCADA it shall be possible to set an automatic transfer from one mode to the other depending on the error between PV Setpoint and PV. From the

HMI/SCADA it shall be possible to change the magnitude of this error. It shall also be possible to manually change between these the modes described above.
Should PID and/or TPO control be employed for temperature control, it shall be possible to change any of the parameter values via the HMI/SCADA.

2) Vacuum
The current hardwired control shall be superseded with PLC control and interface provided for by the HMI/SCADA. The PLC shall then ensure that the pressure in the chamber is maintained at pressure which is set by the operator as well as the stopping and starting of pumps.

Over-range and RoC Protection

Temperatures and the Rate of Change of temperatures shall be monitored in order that they do not fall outside of safe operating limits. There shall be two levels of detection:

1) Warning – This may be at PLC level or HMI/SCADA level or both. The warning shall clearly indicate to the operator that a zone has gone outside of its safe operating range. The condition shall be recorded in the Alarm Log (Hi or Lo Level)
2) Alarm – This shall be at PLC and HMI/SCADA level and shall automatically shut down the relevant zone (disable heating and cooling) until a reset is performed. The operator shall be made aware of the condition and the event shall be recorded in the Alarm Log. (HiHi or LoLo Level)

Short Protection

In accordance with the PR18119 Specification hardwired short circuit protection shall be provided for SCR devices. There shall be a software interface which records short circuit events and feeds this information to the HMI/SCADA and is brought to the operator's attention by means of a mimic and Alarm indication.

Communication Integrity Detection

There shall be a "heartbeat" system which determines the integrity of communications between the various components of the system. After a given time which is configurable from the HMI/SCADA, the detection shall time out and cause a safe shut down of operations. An Alarm shall be visible to the operator and an Alarm even shall be raised.

4.2 HMI/SCADA

The HMI/SCADA shall have the following functionality:

1) The SCADA software shall consist of a human machine interface (HMI) system with support for supervisory and process control, real-time data acquisition, alarm and event management, historical data collection, communications to PLC's and remote alarm notifications. The software shall be easy-to-use, with an object-oriented graphics development environment and shall have an open architecture, supported on the latest Microsoft Windows Server and Client operating systems.
2) The SCADA system software shall provide high availability for all functions within a normal SCADA controls environment.

3) The system shall be able to be modified by the end user in an intuitive manner as the system is to be re-configured regularly between operations.
4) The system shall be scalable so that a small, single application running one test chamber can easily be expanded in the future into a multi-application, multi-chamber solution.
5) The development environment shall utilize an object model to allow designing of an application which models the physical characteristics of the SCADA system. The system shall use the concept of Application Objects, these Objects shall represent real world devices such as Thermocouples, PID loops, Heaters, Motors, Pumps, Valves, etc.
6) The Development Environment shall promote code re-use by using templates to define application objects. Templates may be customized to create new application object templates and maintain parent-child relationships of the object definitions.
7) It shall be possible to configure historical logging using the same development environment as the SCADA configuration. No separate tool shall be required.
8) Multiple form factors (including tablets), screen resolutions, aspect ratios, and multi-monitor displays shall be supported (including triple head 4K screens). Content will automatically fit the target screen in a manner that allows the data presented to be read clearly by the user.
9) The system shall provide the ability to access the visualization application via a web browser with HTML5 support. Remote access from an Intranet shall be provided through a securely authenticated gateway and shall be read only so that no changes can be made.
10) The system shall be capable of securely notifying users of specific alarms and events that occur, this should be configurable on a per test facility basis. The ability to securely send emails predicting when the facility will reach a specific state shall also be possible.
11) The SCADA system software shall provide a real-time relational database historian for long-term storage of process data. If the Historian is off-line or unreachable, the data collection system shall store data locally, and forward the buffered data to the Historian complete with time stamps and quality information when the historian server is available. The data historian shall be able to transfer historical process data to the sites existing master database.

Colour Conventions

The following conventions shall be adhered to with the graphical representation of entities:

1) Grey – Inactive or disabled
2) Black – Enabled but inactive
3) Flashing between green and grey - Starting
4) Red – In Fault
5) Yellow – In manual

Navigation

Navigation shall be possible through one of three methods:

1) A navigation bar which is permanently visible from any screen
2) A home page which presents graphical links to any other screen in the application
3) A “breadcrumb” type navigation system which remembers previous screen selections and allows the user to page backwards and forwards through this history

Navigation shall be designed so as to provide a maximum of two clicks in order to navigate

to any page.

Alarms and Alarm Logging

Two kinds of alarms shall be detected and recorded:

1) PLC generated alarms which shall be communicated to the HMI/SCADA. This is so that critical alarms are handled by either the PLC or safety PLC even in the event of comms failure but should HMI/SCADA comms be healthy the event is logged and displayed.
2) HMI/SCADA generated alarms. Use shall be made of the relatively sophisticated yet easily implemented fault detection which is available in upper level HMI/SCADA packages.

From the HMI/SCADA it shall be possible to view both Current and Historical alarms as well as acknowledge alarm conditions and clear those alarm conditions once they have cleared. It shall be possible to export alarms in a common use (e.g. csv) format.

Alarm Banner

There shall be an alarm banner showing all current alarms visible from every screen. From the Alarm banner it shall be possible to perform Acknowledge and Clear functions.

Security

It shall be possible for multiple security levels to be set up for the purpose of authorisation which can be applied to HMI/SCADA objects. This shall be for the purpose of preventing operators of the HMI/SCADA from making changes they are NOT permitted to make and also to track who has performed certain actions. It shall be possible for high level administrators of the system to create new users, delete existing users and new levels of authority. It shall be possible for user to change the password of their own login. It shall be possible for a domain controller to be used to specify which users can access the system and what access levels they are assigned to. The development environment shall be similarly secured such that only authorized users can access it.

Production and Maintenance Screens

Screens shall be divided into two types:

1) Production screens - for the day to day operation of the chamber. Functions shall include the changing of setpoints and monitoring of process values.
2) Maintenance screens - for the setup of equipment such as thermocouples and protection devices and the control of software mechanisms such as PID controllers.

Both the navigation bar and navigation home page should have these two types of screens grouped together.

Changing Setpoints

As discussed previously in 4.1 PLC it shall be possible to change all setpoints in the PLC from forms which are set up on HMI/SCADA screens. When a setting is selected it shall produce a popup which allows for easy mouse or touchscreen data entry. Any field which is not accessible due to insufficient authorisation level shall be greyed out and not allow for the data entry popup to be shown.

Saving and Recalling Settings

It shall be possible to change the chamber set points in one of three ways:

1) Individual Zone Settings

The chamber shall be divided into four sections. The operator shall be able to change the following settings from the HMI/SCADA:

a) Temperature Setpoint
b) Rate of Change of temperature (RoC)
c) Maximum Output Heating
d) Maximum Output Trim
e) Maximum Output Cooling

2) Bulk Changes

A means shall be devised whereby the above-mentioned settings may be applied to a select number of nodes. It shall be possible to save the settings, the pattern of zones to which the settings have been applied together with the ability to save a combination of settings with particular zones. Wherever any of the above is saved, the following data shall be included:

a) Name (Of Setting, Pattern or Setting/Pattern combination
b) Description
c) Date of Change
d) Author

3) Configuration Save and Load

It shall be possible to save a snapshot of all the settings for each zone into memory included with the following data:

a) Name (Of Setting, Pattern or Setting/Pattern combination
b) Description
c) Date of Change
d) Author

It shall then be possible to recall this snapshot from memory.

Job Maintenance

When the chamber is being used by the customer, a job shall be created and all logged data shall be referenced to this job. A page shall be created for the maintenance of jobs. The job maintenance screen shall allow for the creation of new jobs, deletion and modification of existing jobs.
There should be a record of the following:

a) Job Number
b) Job Customer
c) Job Description
d) Creation date
e) Finish date
f) Job Initiator

Data should be saved in a database. It should be possible to pick jobs from a list.

Situational Awareness

Use shall be made of situational awareness tools for easy monitoring of zone conditions thus ensuring a quick response to out of control conditions.

4.3 Database

The database shall be a full licensed installation of SQL Server 2014 and shall reside on a RAL supplied server. The database shall:

1) Use standard security measures with mixed mode authentication. A separate user shall be created for the HMI/SCADA. Another should be created for the PLC.
2) Shall be designed in such a way as to allow for the modular addition of future chamber databases on the same server.
3) Shall be fully commented. A descriptive naming convention shall be used to distinguish area and functionality.
4) Be a normalised relational database.
5) Shall be configured for remote connection.
6) Use should be of Stored Procedures wherever possible to provide for reusability and protection against SQL Injection attacks.
7) Tables should be configured to allow for changes subsequent to initial design with the need to recreate the table.
8) Shall be configured for replication with a second backup server.
9) Shall be configured to perform regular backups.