Practical Series

PRACTICAL SERIES AUTOMATION LIBRARY

VALIDATION PLAN

AUTHOR: MICHAEL GLEDHILL

Published By: Practical Series of Publications
Published in the United Kingdom
mg@practicalseries.com

Copyright 2021 Michael Gledhill

Document No.: PS2001-5-0121-002

Document Template: PS2001-5-nnnnn-nnn R02.00 SHORT GxP Blank (Ind-Calisto)

LICENCE This document and associated software are made available under the MIT License:

Based on template: PS2001-5-nnnnn-nnn R02.00 SHORT GxP Blank (Ind-Calisto) — Indexable PDF format WebIndex:ber

DOCUMENT AUTHORISATION

	NAME	POSITION	SIGNATURE	DATE
Author	Michael Gledhill	Lead Engineer	M Gledhill	26 May 2022

The signature of the author confirms that the document has been prepared in accordance with an approved document management process, that all content is technically complete and that all relevant material has been included.

Reviewed by	Frank Greenwood	Project Manager	F GreenWood	26 May 2022

The signature of the reviewer indicates that the document has been checked for technical content and that it complies with the technical standards, specifications and conventions.

Approved by	Christopher Wish	Quality Manager		26 May 2022

The signature of the Approver indicates that the document has been checked for compliance with the quality management Procedures.

THIRD PARTY AUTHORISATION

	NAME	POSITION	SIGNATURE	DATE
Approved by	Alfred Featherstone	Operations Director	A Featherstone	26 May 2022

The signature of the Approver indicates that the document satisfies the Project quality and validation requirements of the Third Party's quality system.

REVISION

REVISION	DATE	REVISED BY	DESCRIPTION
R02.00	26 May 2022	Michael Gledhill	Properties standardised across all documents
R01.00	05 Jun 2020	Michael Gledhill	First release for use

CONTENTS

1. Introduction 7

1.1 Scope and purpose of this document 7

1.2 Ownership, status & relationship to other documents 8

1.2.1 Ownership of the document 8

1.2.2 The status of this document 8

1.2.3 Relationship to other documents 8

1.2.4 The Project Registry 8

2. Approach 10

2.1 Objective and benefits 12

2.2 Compliance determination 12

2.2.1 GxP requirements 13

2.2.2 Good Automation Manufacturing Practice (GAMP) classification 13

2.2.3 Software classification 15

2.3 Regulations and standards 16

2.3.1 Software standards 16

2.3.2 Software regulations 16

2.3.3 Electrical and instrumentation standards 17

2.4 Policies and procedures 17

2.5 Assumptions 17

3. The validation Strategy 18

3.1 Planning phases 19

3.1.1 Planning phase — deliverables and responsibilities 20

3.2 Requirements phase 21

3.2.1 Requirements phase — deliverables and responsibilities 22

3.3 Design phase 23

3.3.1 Design phase — deliverables and responsibilities 28

3.4 Build phase 29

3.5 Test phase 29

3.5.1 Test phase — deliverables and responsibilities 31

3.6 Deployment phase 31

3.7 Qualification phase 32
3.7.1 Qualification phase — deliverables and responsibilities 34
3.8 Training & Use phase 35
3.8.1 Qualification phase — deliverables and responsibilities 36
3.9 Acceptance criteria 37
3.10 Document revision in references 37

4. References and glossary 39
4.1 References 39
4.2 Glossary of terms 40

Appendices 43

A Risk assessments 45
A.1 Simultaneous software build and test 45
A.1.1 Description of the process and overview of the risks 45
A.1.2 Existing controls 45
A.1.3 Assessment details 45
A.1.4 Quantifying the risk 46
A.1.5 Initial risk assessment 47
A.1.6 Remedial actions 48
A.1.7 Final risk assessment 49
A.1.8 Conclusions 49

1 Introduction

This document is the *Validation Plan* (VP) for the *Practical Series Automation Library* of software modules (the PAL)) project, (hereafter referred to as the Project).

This Validation Plan has been issued to describe the validation activities required to qualify the control system software and associated hardware developed under the requirements of this Project.

1.1 Scope and purpose of this document

This Validation Plan is applicable to the following phases of the Project:

① System design

② Testing

③ Qualification

Specifically, the validation activities will consist of the following:

- Design review and design review report
- Software and hardware factory acceptance testing
- Installation and operational qualification

The purpose of the Validation Plan is to ensure that the control system, its software and hardware, developed and built as part of this Project is validated, that is to say, that the system does precisely what it was designed to do; specifically, it is the exercise of correctly and traceably documenting every requirement of the system and making sure that that requirement is formally and exhaustively tested

It ensures that the finished and installed system satisfies all the requirements of the original specification, is fully documented and is fit for its purpose.

1.2 Ownership, status & relationship to other documents

This document (the Validation Plan) is a fundamental document for the Project, the ownership of the document (those whom control it and are able to modify it), its status within the Project and its relationship to all other primary documents are important factors and are explained below:

1.2.1 Ownership of the document

This Validation Plan has been produced, and is controlled and maintained by the Practical Series of Publications (PSP).

This Validation Plan is subject to the change control management procedures for this Project; these are detailed in the *Change control and configuration management* section of the Project Quality Plan, *[Ref. 002]*, § 3.3.

1.2.2 The status of this document

The Validation Plan (*this document*) is a contractual document and is a deliverable item under the terms of the project. The Validation Plan is an approved document and this approval must take place prior to the commencement of any Project design activity.

The document must be approved by the Practical Series of Publications Quality Manager and by the Customer or Customer's representative.

1.2.3 Relationship to other documents

The Validation Plan is a primary document for the Project. The full document flowpath for the Project including the Validation Plan is shown in Figure 1.1.

1.2.4 The Project Registry

A full list of all Project documents and their current revision status is maintained in the Project Registry *[Ref. 020]*.

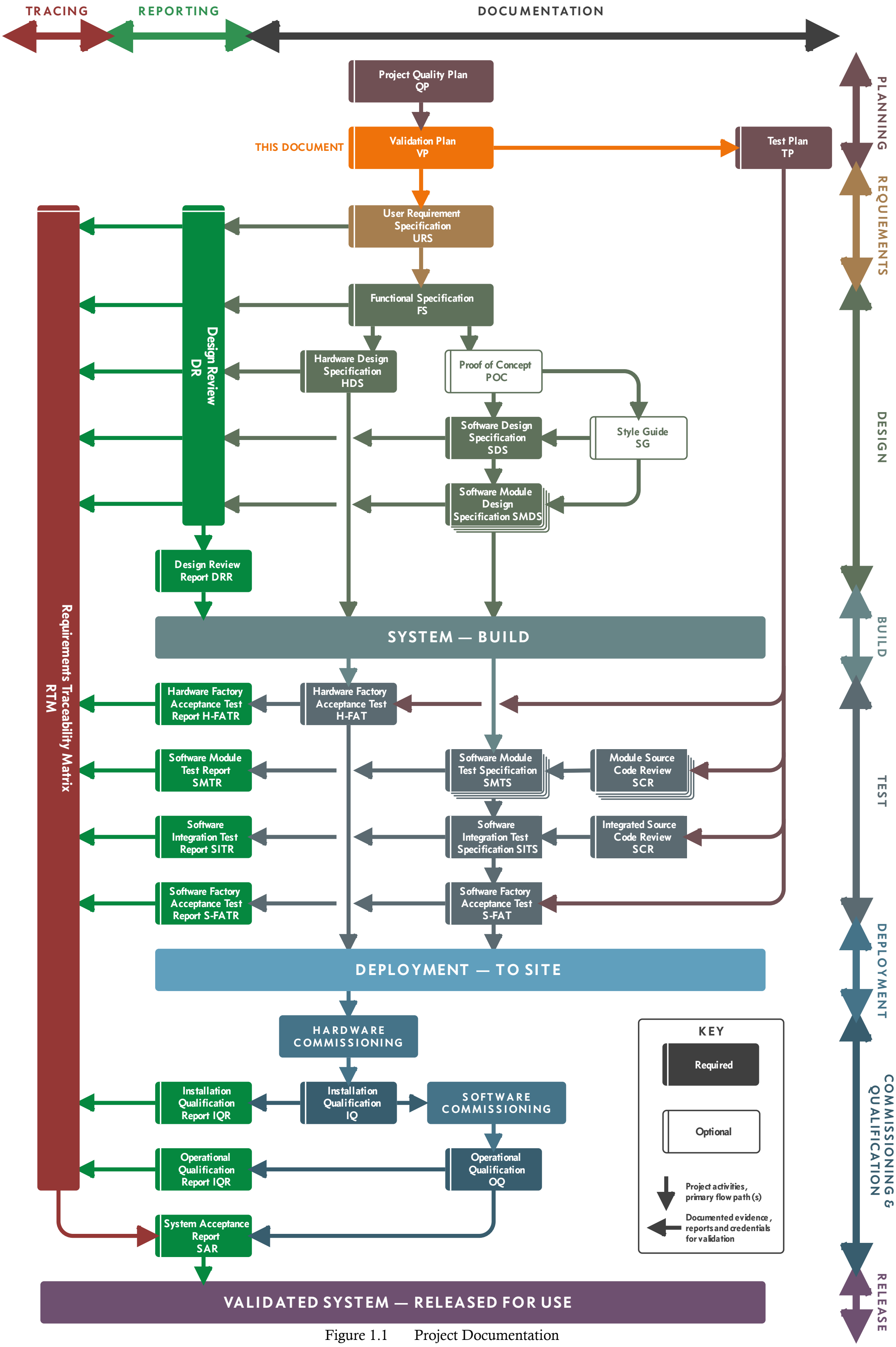
TRACING
REPORTING
DOCUMENTATION
Project Quality Plan QP
THIS DOCUMENT
Validation Plan VP
Test Plan TP
User Requirement Specification URS
Functional Specification FS
Hardware Design Specification HDS
Proof of Concept POC
Software Design Specification SDS
Style Guide SG
Software Module Design Specification SMDS
Design Review DR
Requirements Traceability Matrix RTM
Design Review Report DRR
SYSTEM — BUILD
Hardware Factory Acceptance Test Report H-FATR
Hardware Factory Acceptance Test H-FAT
Software Module Test Report SMTR
Software Module Test Specification SMTS
Module Source Code Review SCR
Software Integration Test Report SITR
Software Integration Test Specification SITS
Integrated Source Code Review SCR
Software Factory Acceptance Test Report S-FATR
Software Factory Acceptance Test S-FAT
DEPLOYMENT — TO SITE
HARDWARE COMMISSIONING
Installation Qualification Report IQR
Installation Qualification IQ
SOFTWARE COMMISSIONING
Operational Qualification Report IQR
Operational Qualification OQ
System Acceptance Report SAR
VALIDATED SYSTEM — RELEASED FOR USE
KEY
Required
Optional
Project activities, primary flow path (s)
Documented evidence, reports and credentials for validation
PLANNING
REQUIEMENTS
DESIGN
BUILD
TEST
DEPLOYMENT
COMMISSIONING & QUALIFICATION
RELEASE

Figure 1.1 Project Documentation

2 Approach

The Practical Series Automation Library (PAL) Project is a library of software modules and templates that are to be made available for the Siemens Simatic S7-1500 range of Controllers (and to a lesser extent the S7-1200 range).

The PAL software structure is to be designed to be applicable to virtually all industrial applications that are generally controlled by a programmable logic controller (PLC).

The wide range of possible applications of the software includes regulated environments such as the pharmaceutical industry.

The approach taken to validating the systems designed and built under this Project will ensures that the required deliverables are prepared and supplied in accordance with the conventions and practices laid out in the GAMP 5 (*Good Automation Manufacturing Practice*) guidance document *[Ref. 016]* and have adopted the GAMP 5 life-cycle[1] model for this project; illustrated in Figure 2.1:

[1] GAMP 5 refers to "life-cycles" in different capacities: for a plant it could be the initial concept, through a project to build and deliver the plant, the operation of the plant for its expected life time and finally the retirement (decommissioning) of the pant.

More precisely in the context of this Project, the term "life-cycle" refers to the life-cycle of the Project itself, from establishing the initial requirements, designing a system to satisfy those requirements, building the system, testing it, deploying the system and qualifying (validating) the final system., these are shown in Table 3.1

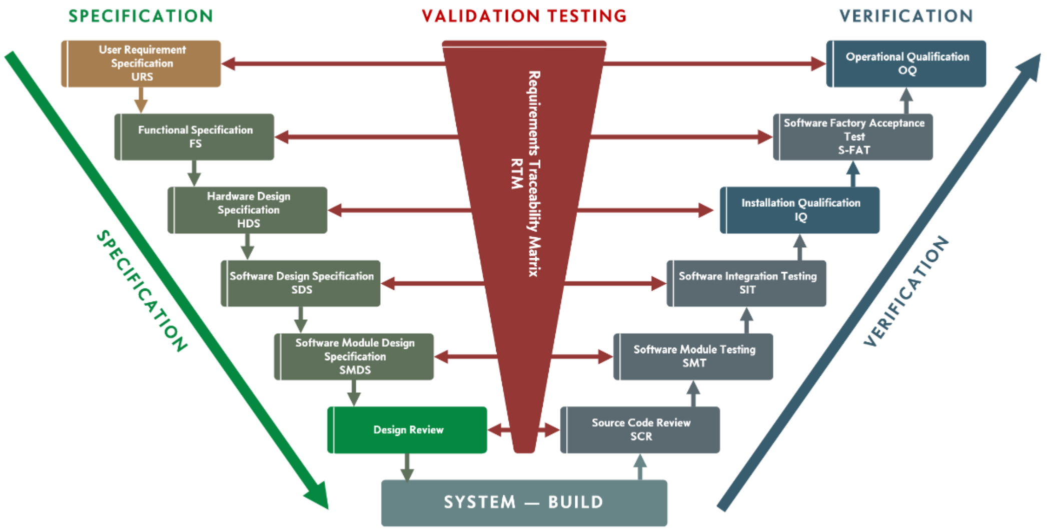
SPECIFICATION
VALIDATION TESTING
VERIFICATION
User Requirement Specification URS
Functional Specification FS
Hardware Design Specification HDS
Software Design Specification SDS
Software Module Design Specification SMDS
Design Review
Requirements Traceability Matrix RTM
Operational Qualification OQ
Software Factory Acceptance Test S-FAT
Installation Qualification IQ
Software Integration Testing SIT
Software Module Testing SMT
Source Code Review SCR
SPECIFICATION
VERIFICATION
SYSTEM — BUILD

Figure 2.1 Project Life-cycle

This approach uses a Requirement Traceability Matrix (RTM), this forms the basis of the design review processes; the RTM takes the requirements of the design documents, starting with the originating document: the User Requirements Specification (URS). Each requirement in the URS is identified (by section number and paragraph) and listed in the RTM, where each of these requirements is addressed in the subsequent design documents (listed above), this document is also entered in the RTM along with the relevant section or section and paragraph number.

The design review process uses the RTM to ensure that all the Project requirements specified in the URS have been correctly addressed in the design process. I.e. that the design meets the requirements demanded of it; this is summarised in a Design Review Report (DRR).

During the testing phase, the RTM is expanded such that one or more individual tests are allocated to each requirement and subsequent design points within the RTM. Once all the tests for a particular requirement are satisfactorily complete, it establishes that the particular requirement has been met. Once all the tests are completed satisfactorily for all requirements, the system will be validated.

A more detailed explanation of this process is given in section 3 of this document.

2.1 Objective and benefits

The object of the Project is to provide a library of *standard*, validated software modules that can be used within a project without further module testing (the modules having already been validated).

The only modular level testing of these *standard* modules would be to confirm that they are identical to the original released PAL modules, and this is easily done with the existing facilities within the Siemens Simatic TIA Portal programming environment.

The benefits of this approach is that subsequent projects that use the Practical Series Automation Library of software modules do not require the extensive design and documentation stages needed to develop software modules in the first place, neither do the modules require testing, nor the documentation needed to test them. This will have already been done as part of this Project and will be issued in verifiable form by this Project.

2.2 Compliance determination

The environments within which the PAL software can be used include pharmaceutical, food and beverage, chemical and oil and gas applications; all of which require some degree of regulatory compliance.

The most onerous of these compliances is that required of the pharmaceutical applications (others applications, such as chemical and oil and gas, require regulatory compliance in the type of equipment provided e.g. safety systems, equipment rated for explosive environments, ATEX zoning, &c. and this compliance is generally achieved by the use of the correct devices and physical isolations: e.g. safety rated relays, hazardous area instrumentation, physically separating the electrical system from hazardous environments &c.)

These physical requirements (explosive environments &c.) can also apply to pharmaceutical applications; however, this Project is associated with the software required to control a plant; and generally, if software has been written and tested to the stringent requirements of a pharmaceutical system, it will be suitable for most other applications (and indeed all the applications listed earlier).

2.2.1 GxP requirements

The regulatory compliance of the control system is determined by a positive response to one of the following statements:

POINT	STATEMENT	RESULT
1	The system is used to monitor, control or supervise a GxP drug manufacturing or packaging process	Yes
2	The system is used for GxP analytical quality control	Yes
3	The system is used to monitor, control or supervise warehousing or distribution with a GxP implication	Yes
4	The system supports the maintenance of GxP systems	No
5	The system manipulates data, or produces reports, to be used by GxP quality related decision authorisation/approval processes	Yes
6	The system is used for GxP batch processing or batch records	Yes

Table 2.1 GxP compliance table

Where GxP is any of: Good Clinical Practice (GCP),
Good Distribution Practice (GDP),
Good Laboratory Practice (GLP),
and Good Manufacturing Practice (GMP).

Clearly, regulatory compliance is required and the system must be validated.

2.2.2 Good Automation Manufacturing Practice (GAMP) classification

This Project will comply with, and be written to, the standards necessary for *Good Manufacturing Practice* (GMP), generally referred to as GxP. These are the most rigorous standards used for control systems software and hardware development and use.

The GxP requirements are encapsulated in the International Society for Pharmaceutical Engineering (ISPE) guidelines, referred to as Good Automation Manufacturing Practice (GAMP), currently at revision 5 (GAMP 5), listed here as *[Ref. 016]*. Systems that are written to the standards in GAMP 5 are said to be *compliant* systems.

This compliance allows the system to be formally *validated*.

Validation is the process of making sure a computerised system (such as a PLC and its software) does precisely what it was designed to do; specifically, it is the exercise of correctly and traceably documenting every requirement of the system and making sure that that requirement is formally and exhaustively tested.

This Project, the Practical Series Automation Library, will be written to the standards specified in GAMP 5, it will be a validated and fully compliant GMP Project.

The GAMP 5 specification categorises both software and hardware in terms of risk with the risk increasing as the software or hardware moves from standard components to customised and ultimately bespoke components.

Hardware classification

GAMP 5 provides two hardware categories:

CATAGORY	DESCRIPTION	EXAMPLE	REQUIREMENTS
1 Standard hardware components	Commercially available equipment	Instruments, PLCs, valves, drives, inverters &c.	Record: Version, model No., Serial No. &c. Verify installation
	Assembled equipment using standard components	Electrical panels	Terminal schedules &c.
2 Custom built hardware components	Specialist laboratory equipment Hardware design specifically to suit the process	Custom interfaces non-standard instruments bespoke valve or drive	As category 1 plus: URS Supplier assessment Tests against URS

Table 2.2 GAMP 5 hardware classifications

All hardware used within the Project will be of category 1, i.e. standard hardware components.

Standard components are often referred to as *"commercial, off-the-shelf"*, indicating that these are common, commercially available items that have not been specifically designed or built for this particular application. Such items are readily available, can easily be replaced and allow for spares holding.

2.2.3 Software classification

GAMP 5 provides five software categories:

CATAGORY	DESCRIPTION	EXAMPLE	REQUIREMENTS
1 Infrastructure Software	Layered software (i.e., upon which applications are built) Software used to manage the operating environment	Operating System Database Engines Programming languages Statistical packages Spreadsheets	Record version Verify installation
2	**Category 2 is no longer used**		
3 Non-Configured Software	Run-time parameters may be entered and stored, but the software cannot be configured to suit the process	Firmware- Commercial off the shelf software	As category 1 plus: URS Supplier assessment Tests against URS
4 Configured Software	Software, often very complex, that can be configured by the user to meet the specific needs of the process. Application software code is not altered.	Data acquisition systems: • SCADA • HMI • ERP • MRPII	As category 3 plus: Verify supplier QMS Design specs. (DS) Tests against DS Procedures for: • Data management • Maintenance
5 Custom (bespoke) Software	Software custom designed and coded to suit the process.	Bespoke IT applications Bespoke control systems Custom ladder logic Custom firmware Spreadsheets (macro)	As category 3 plus: Full life cycle docs: FS, DS, SDS, HDS, SMDS &c. Source code review Structural testing: SMT, SIT, FAT, IQ, OQ

Table 2.3 GAMP 5 software classifications

The control system being developed as part of this Project is a bespoke system and, under the GAMP 5 classification system, is a category 5 system.

Such bespoke systems are developed to meet the specific needs of the Project. The risk inherent with custom software is high, there being no user experience or system reliability information available. The GAMP 5 life cycle approach (Figure 2.1) will be used to accommodate and mitigate this risk.

2.3 Regulations and standards

The British and international standards detailed within this document, provide the minimum required standards that should be applied to the controls and instrumentation systems provided under the scope of this Project. Software standards

2.3.1 Software standards

The Practical Series Automation Library software will be written to the standards set down in the *International Electrotechnical Commission* (IEC) publication 61131-3: Programmable controllers - Part 3: Programming languages, listed here as *[Ref. 017]*.

2.3.2 Software regulations

There are two specific sets of regulations that apply to control systems in pharmaceutical environments:

• CFR 21 Part 11	US Code of Federal Regulations, Title 21, Food and Drugs, Part 11 – Electronic Records, Electronic Signatures [Ref. 018]
• EudraLex Vol 4 Annex 11	EU Regulations Volume 4: Pharmaceutical legislation – Medicinal Products for Human and Veterinary use – Good Manufacturing [Ref. 019]

Generally, if a system is compliant with GAMP 5 it will satisfy the EU Regulations Volume 4, Annex 11[2].

CFR 21 Part 11 is concerned with the accuracy, reliability and storage of electronic signatures; this is more relevant to supervisory systems rather than the Controller software of this Project; however, were applicable the PAL software will comply with these regulations.

[2] There are some additional documentation requirements and these are specifically addressed in § 3.8.

2.3.3 Electrical and instrumentation standards

The electrical installation, instrumentation and all associated equipment must comply with the following standards and regulations where necessary:

Electrical Equipment (Safety) Regulations 2016	
BS7671	IET Wiring Regulations 17th Edition
BS EN60204	Safety of machinery - Electrical equipment of machines
BS6739	Code of Practice for Instrumentation in Process Control Systems: Installation Design and Practice
BS EN60439-1	Specification for low voltage switchgear and control gear assemblies.
IEC61508	Functional safety of electrical/electronic/programmable electronic safety related systems

2.4 Policies and procedures

The Project will operate under the policies and procedures specified in detail, in the Project Quality Plan *[Ref. 002]*; this explains how the Project fits into and satisfies the requirements of the PSP Quality Management System (QMS), the detail of which are given in the Quality Manual *[Ref. 001]*.

2.5 Assumptions

It has been assumed the Project, the design, build and installation of the system, will all fall under the regulations and legislative requirements of the United Kingdom

3 The validation Strategy

The validation process applies at all phases within the Project (summarised below):

PHASE	PURPOSE	DELIVERABLES
PLANNING	The planning phase establishes how the project will be controlled, how it will define the requirements of the system, how the system will be built and how the system will be tested and validated	Quality Plan (QP) Project Schedule (PS) Validation Plan (VP) Test Plan (TP)
REQUIREMENTS	Establishes the fundamental requirements of the system in a precise and quantifiable format	User Requirements Specification (URS)
CROSS PHASE	Establishes those aspects of the project that apply to all subsequent phases: Requirement Traceability Matrix, change control and incident management	Requirements Traceability Matrix (RTM) Change Control Management (CCM) Incident Management (IM)
DESIGN	Establishes the necessary function of the system. Provides the design specifications for the system needed to meet and satisfy those functions. Provides a review mechanism to ensure the design satisfies all the requirements of the system	Functional Specification (FS) Hardware Design Specification (HDS) Software Design Specification (SDS) Software Module Design Specification (SMDS) Design Review (DR) Design Review Report (DRR)
BUILD	The physical construction of the system: electrical panels, equipment procurement, site construction &c. The writing of the system software: software modules, integrated software, network and device configurations &c.	Physical hardware (panels, equipment &c.) Developed and configured software
TEST	Testing of the system before site installation including: • Hardware testing of the physical panels and networks • Software source code reviews • Software module testing • Software integration testing • Software factory acceptance testing	Hardware Factory Acceptance Test (H-FAT) Source Code Review (SCR) Software Module Test (SMT) Software Integration Test (SIT) Software Factory Acceptance Test (S-FAT)
DEPLOYMENT	Deploy the system to site: site installation of all equipment, networks, hardware, devices field wiring &c.	Calibration and installation certification O&M manual with instructions, configurations, drawings and supporting documentation
QUALIFICATION	Controlled progression from its basic plant installation to a fully working, commissioned, tested and operable system. Performed in stages: • Hardware commissioning • Installation Qualification • Software Commissioning • Operational Qualification	Installation Qualification (IQ) Operational Qualification (OQ) Site Acceptance Report (SAR)
TRAINING & USE	Formal training of personnel in the use of the system	Standard Operating Procedures (SOPs) Training manual User guides

Table 3.1 Formal project phases

3.1 Planning phases

The planning phase of the project establishes the mechanisms for controlling the Project. It determines the approach that is to be taken towards quality, validation and testing; and establishes the overall governance of the system, i.e. does it fall under the constraints of GMP &c.

The planning phase will also determine the programme schedule for the Project and identify the key deliverable items.

The following are the key deliverable items for the planning phase:

Quality Plan (QP)

The Quality Plan (QP) defines the way in which the Project will be controlled, it is a documented record of the quality procedures that will be used to deliver the requirements of the project.

Validation Plan (VP)

This document — defines the validation requirements of the Project, the mechanisms put in place to validate the Project and the acceptance criteria that must be met for the system to be validated.

Test Plan (TP)

The Test Plan (TP), describes the approach and methodology needed to ensure that the control system developed by the Project works correctly and perform in accordance with the necessary requirements and specifications.

Project Schedule (PS)

A detailed breakdown of the Project into specific activities and tasks, it identifies durations and resources for each task and organises the tasks and activities into a schedule. It identifies key dates, deliverable items and *"milestones"* against which the progress of the Project can be measured. It is provided in the form of a Microsoft Project Gantt chart.

Other planning items

The planning phase will also put in place the standard structures and mechanisms for the Project. It will create various registers and forms for the following:

- Document management
- Change management
- Incident management
- Version control
- Technical queries

3.1.1 Planning phase — deliverables and responsibilities

The following deliverable items will be produced during the planning phase of the Project, the purpose of each deliverable is described in the previous section.

O = Originator (author)
R = Review
A = Approve
N/A = Not applicable

RESPONSIBILITY

DELIVERABLE	Project Manager	Engineering	Quality/Validation	Customer/user
Quality Plan QP [Ref. 002]	O	R	A	A
Validation Plan VP [this document]	R	O	A	A
Test Plan TP [Ref. 005] – 1st release (without test schedules)	R	O	A	A
Project Schedule PS [Ref. 003]	OA	R	N/A	R

Table 3.2 Planning phase deliverables

3.2 Requirements phase

The requirements phase establishes the fundamental requirements of the system in a precise, quantifiable and unambiguous format.

The requirements developed in this phase will reflect the functionality that is necessary for the system, this will be from the point of view of those using the system and will capture their specific requirements. It will incorporate both business and technical requirements and will address fault and error handling.

It will establish the tracking and tracing mechanisms used to monitor progress and determine that the requirements are being met; these will form the basis of the validation processes.

The following are the key deliverable items for the requirements phase:

User Requirements Specification (URS)

This Project requires the design and development of a bespoke control system, this will be based entirely on the requirements given in the User Requirements Specification (URS) *[Ref. 006]*. The URS is the originating design document of Figure 2.1, and will be developed, written and approved in the Requirements phase of the project.

The Design phase of the project will produce the principal design document, the Functional Specification (FS) *[Ref. 008]*. The FS provides a detailed description of what the system should do, and what facilities and functions are to be provided. It will provide a list of the design objectives for the Project derived from the URS.

Requirement Traceability Matrix (RTM)

The requirements phase produces the initial composition of the Requirements Traceability Matrix (RTM) *[Ref. 007]*; initially just capturing the requirements specified in the URS.

The RTM takes the requirements of the design documents, starting with the originating document, the User Requirements Specification (URS). Each requirement in the URS is identified (by section number and paragraph) and listed in the RTM, where each of these requirements is addressed in the subsequent documents (FS, HDS, SDS or

SMDS), this document is also listed in the RTM along with the relevant section or section and paragraph number.

The design review process uses the RTM to ensure that all the Project requirements specified in the URS have been correctly addressed in the design process. I.e. that the design meets the requirements demanded of it.

The RTM is essentially a map of the system from requirements to the design documents through testing and qualification and to handover; as such, it provides a structure for the design review processes.

The RTM is expanded in further phases, mapping the requirements to specific tests and qualification activities and acts as a rationale for the validation activities. It shall, as a minimum cover all qualifications of the system (i.e. installation and operational qualifications).

Supplier Assessment

The software and hardware associated with the Project is being developed internally within the PSP — therefore a Supplier Assessment is not required.

3.2.1 Requirements phase — deliverables and responsibilities

The following deliverable items will be produced during the requirements phase of the Project, the purpose of each deliverable is described in the previous section.

O = Originator (author)
R = Review
A = Approve
N/A = Not applicable

	RESPONSIBILITY			
DELIVERABLE	Project Manager	Engineering	Quality/Validation	Customer/user
User Requirements Specification URS [Ref. 006]	N/A	N/A	N/A	OA
Requirements Traceability Matrix RTM [Ref. 007] – 1st release (URS)	R	O	A	A

Table 3.3 Requirements phase deliverables

3.3 Design phase

The design phase produces the detailed design of the system, the basis of the design is the User Requirements Specification, the design will also include those requirements imposed by the regulatory and legislative bodies under which the system falls (e.g. requirements for explosive environments, safety systems, hazardous areas, electrical standards &c.).

The design phase will split the system requirements into those that require hardware and infrastructure (hardware design) and those that require software and configuration (software design).

The design will be documented at each stage and will conclude with a formal Design Review (DR) that will determine the efficacy of the design. The design review will conclude with a formal Design Review Report that will detail the results of the Design Review with any findings and concerns noted.

The following are the key deliverable items for the development phase:

Functional Specification (FS)

The Functional Specification (FS) is the principal design document for the Project. The FS provides a detailed description of what the system will do, and what facilities and functions are to be provided. It will provide a list of the design objectives for the project and will define how the equipment will be controlled by the control system; and will do so in a clear and unambiguous manner.

The FS will define the constraints of the system (response times, hardware limitations, environmental limits, operational controls).

The FS will establish the naming conventions, nomenclature and stylistic methodology to be used throughout the Project (or, where such conventions are large in scope, these will be explained in a separate Style Guide (SG) document, referenced from within the FS).

Further detailed design documents will be produced in response to the FS, these will include, but not be limited to:

- Hardware Design Specification (HDS) *[Ref. 009]*
- Software Design Specification (SDS) *[Ref. 010]*
- Software Module Design Specification (SMDS) *[Ref. 011]*

And these are detailed below:

Hardware Design Specification (HDS)

The hardware design specification (HDS) is the coordinating document for all aspects of the hardware design, including:

- Controller hardware (processor, cards, rack arrangements)
- Device schedules
- Input/output (IO) schedules
- Network architecture
- Panel specification (construction type, materials, general arrangements and wiring diagrams &c.)
- Electrical drawings (including loop diagrams for field devices)
- Safety and area zoning
- Interlock arrangements
- Device configurations
- Maintenance and spares holding

The above list is not exhaustive, and other design aspects will be included where required. Generally, the HDS will reference other documents rather than include such documents in the HDS itself, this is particularly true of drawings.

Software Design Specification (SDS)

The Software Design Specification (SDS) is the main design document for the software, it will set out the overall architecture of the software and determine the common interfaces and approaches that are to be implemented within the software.

The SDS will determine the type and number of software modules that will be required, the detailed specifications (interfaces, data structures &c.) of each module will be specified in individual Software Module Design Specifications (SMDS), see below.

The SDS will incorporate the following:

- System architecture
- Design philosophy for the software
- Common interfaces (for software modules)
- Common system (global) data
- Common approaches to the user interfaces
- Tagging schemes and naming conventions
- Alarm and warning schedules
- Setpoint configurations
- Modes of operation
- Intersystem data transfer
- Data storage and recipe management
- Security and electronic signatures
- Archiving, backup and data retrieval

Again, these individual items may exist as separate documents, in which case, the SDS will reference them

Software Module Design Specification (SMDS)

Software Module Design Specifications (SMDSs) are subsidiary documents to the SDS, they contain the specific design details for a particular software module.

SMDSs are commonly only used on very large projects, and the SMDS information is often contained within the SDS itself. In the case of this Project, the control system contains a library of software modules; and because of this, each software module will have an SMDS, this is a practical approach to managing the Project and allows the SMDSs to serve as documentary source of information for each module.

Each SMDS will contain the following information about its associated software module:

- A detailed description of the purpose of the module and how it is intended to function
- A detailed description of all the operating modes and configurable actions applicable to the module
- Interfaces and parameters used by the module
- Any module specific timing factors
- Error and exception handling functions
- Common data required by the module
- Data structures and the internal configuration of such
- Internal data assignments, constants, temporary data &c.
- Explanatory and example usage information

Design review

Design review meetings will be carried out at various stages during the design phase; principally to ensure that the URS and specifically, the quality critical and GMP requirements have been incorporated into the design of the control system.

The various design documents will be assessed and reviewed and the RTM will be expanded to incorporate the various design document specifications; where each of the requirements in the URS is addressed in the subsequent documents (FS, HDS, SDS or SMDS), this document is also listed in the RTM along with the relevant section or section and paragraph number. This will be the second release of the RTM

The outcome of any design review meetings will be recorded and, where appropriate, will be added to the RTM either as separate points, or as expansions or clarifications to existing points.

Note: *Each level of design and specification work produced within the Project design phase may be subject to its own (localised) design review (a "walkthrough") prior to further design work taking place, this is generally at the discretion of the Lead Engineer for the Project and will be co-ordinated with the Project Manager.*

This may include experimental (prototype) testing to determine the best approaches or methodology to be adopted, it may also include some Proof of Concept (POC) works to establish that a proposed design is functional and practical.

Where such work takes place, it will be documented separately to the design documentation listed above. It will not form part of the validation process, or formal design documentation, until such time as any prototype is officially brought within the design structures of the Project (i.e. it has been accepted as part of the design philosophy).

Design Review Report (DRR)

The design review process concludes with a formal Design Review Report (DRR), this assess various factors in determining if the proposed design satisfies all the requirements made of it; these are:

- All requirements in the URS have been met by the design
- All quality and GMP requirements are satisfactorily addressed
- All actions from design review meetings have been resolved

Note: *The SMDS documents are limited in scope to individual modules (and in some limited cases, a small group of associated modules), because of this, the SMDS development can take place after the design phase (overlapping with the build phase). The DRR will however, record in the RTM which requirements are to be associated with which SMDS.*

3.3.1 Design phase — deliverables and responsibilities

The following deliverable items will be produced during the design phase of the Project, the purpose of each deliverable is described in the previous section.

O = Originator (author)
R = Review
A = Approve
N/A = Not applicable

	RESPONSIBILITY			
DELIVERABLE	Project Manager	Engineering	Quality/Validation	Customer/user
Functional Specification FS [Ref. 008]	RA	O	RA	RA
Hardware Design Specification HDS [Ref. 009] (and associated documents)	RA	O	R	R
Software Design Specification SDS [Ref. 010]	RA	O	R	R
Software Module Design Specification SMDS [Ref. 011]	RA	O	R	R
Test Plan TP [Ref. 005] – 2nd release (test schedules added)	R	O	A	A
Requirements Traceability Matrix RTM [Ref. 007] – 2nd release (design)	R	O	A	A
Design Review Report DRR [Ref. 012]	RA	O	RA	RA

Table 3.4 Design phase deliverables

3.4 Build phase

The build phase will commence at the satisfactory conclusion of the design review process.

The build phase will see the physical construction of the system hardware (panels, instrument and device purchase &c.) and the writing of the system software. The build phase will be of significant duration.

The following are the key deliverable items for the development phase:

- Electrical panel and test rig
- Control system Controller software

3.5 Test phase

The test phase of the Project will, to a limited extent, overlap with the build phase. The nature of the Project is to produce a library of software modules, each module will be written to incorporate the requirements and specification listed in its own Software Module Design Specification; each of these modules is effectively a stand-alone piece of software that can be tested in its own right and without impact on any other software module.

Once a software module has been written, it can be tested (at the module level) and its function verified. Once such a module has been written and tested, it will fall under Change Control Management and must not be further modified without the module undergoing a complete retest (at the modular level).

This approach has been taken to shorten the Project timescales; it is a decision made for practical and expedient reasons. It accepted that such an approach can increase the risk of software errors (it may be possible for the writing of subsequent modules to impact an existing, tested module adversely). A risk assessment has been carried out (see appendix A) to evaluate and mitigate any risk that this approach may generate.

The testing phase will test all the hardware and software components of the Project, broadly this includes:

① **Hardware Factory Acceptance test (H-FAT)**
Testing of the Controller hardware (electrical panel, CPU, modules, electrical connections, networks &c.)

② **Source Code Review (SCR)**
An inspection of the software to ensure it has been written to the correct standards, and is structured correctly

③ **Software Module Test (SMT)**
Discrete testing of individual software modules (ensuring software modules work in their own right)

④ **Software Integration Test (SIT)**
Integrated testing (ensuring that multiple software modules work together and correctly interface with each other)

⑤ **Software Factory Acceptance Test (S-FAT)**
System testing (ensuring the completed system with all software modules installed, works correctly)

Testing is an essential part of validation the control system; and as such a separate document has been produced to establish the approach to be taken to testing the system, this document is the Test Plan (TP), *[Ref. 005]*.

The Test Plan provides the following:

- Establishes the testing methodology
- Identifies the types of tests required
- Establishes the entry and acceptance criteria for each test
- Determines the procedures for failure and nonconformity

The TP will be accompanied by a third release of the RTM, this will link all the requirements and design specification to specific tests that will verify each requirement.

3.5.1 Test phase — deliverables and responsibilities

The following deliverable items will be produced during the test phase of the Project, the purpose of each deliverable is described in the previous section and in the Test Plan *[Ref. 005]*:

O	= Originator (author)
R	= Review
A	= Approve
N/A	= Not applicable

DELIVERABLE	RESPONSIBILITY Project Manager	Engineering	Quality/Validation	Customer/user
Requirements Traceability Matrix RTM [Ref. 007] – 3rd release (tests)	R	O	A	A
Hardware Factory Acceptance Test H-FAT and report H-FATR	R	OA	R	R
Source Code Reviews SCRs	R	OA	R	R
Software Module Test Specifications SMTS and report SMTR	R	OA	R	R
Software Integration Test Specifications SITS and report SITR	R	OA	R	R
Software Factory Acceptance Test S-FAT and report S-FATR	R	OA	R	R

Table 3.5 Test phase deliverables — see TP for test specification references

At the conclusion of each type of test, a summary test report will be issued, this will document any issues, nonconformities and test conclusions (pass or fail) and any subsequent actions that must be taken

3.6 Deployment phase

The deployment phase begins at the successful conclusion of the factory acceptance tests. In the case of this Project, the deployment phase is simply the wiring of the test rig to the electrical panel and confirming the electrical certifications and instrument calibrations.

The following are the key deliverable items for the development phase:

- Electrical certifications
- Instrument calibrations

3.7 Qualification phase

The qualification phase of the Project has two significant components, installation qualification (IQ) and operational qualification (OQ); together, these form the last component of the validation process.

There are actually four components to the qualification phase:

① Hardware commissioning

② Installation Qualification (IQ)

③ Software commissioning

④ Operational Qualification (OQ)

Unlike the other tests, in which the software and hardware test are not dependent on each other, the qualification process must take plane in the order shown in the above list:

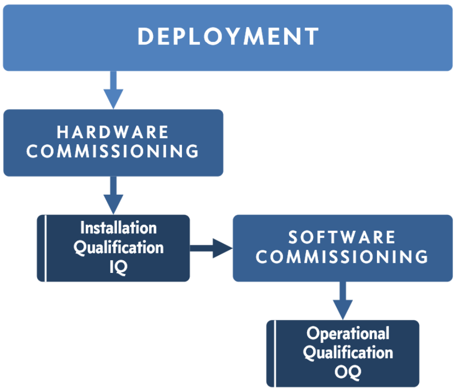

Figure 3.1 Order of qualification testing

The qualification phase will include a fourth release RTM, this will link all the requirements and design specification to specific IQ and OQ tests, giving the final verification of each requirement

The installation qualification (IQ) and operational qualification (OQ) are discussed in greater detail the Test Plan (TP), *[Ref. 005]*; however, they are summarised below as deliverable items for the qualification phase:

Installation Qualification (IQ)

The *Installation Qualification* (IQ), is the formal test of (in this case) the hardware elements of the control system (for control systems, this is the electrical installation, networks, instrumentation, devices and where applicable, pneumatic systems)

The IQ demonstrates that the hardware has been correctly installed, devices and instruments are fitted to manufacturers guidelines, all documentation is present and available, all field wiring has been tested and all electrical devices and instruments are commissioned and are operating correctly.

Operational Qualification (OQ)

The *Operational Qualification* (OQ), is the formal test of the control system as a whole under, *essentially*, live conditions

The OQ is a full test of all aspects of the system operating under the same *live* conditions that the operators of the plant would experience in normal operation and using the same procedures.

It will test all the following:

- start-up and shutdown operations
- All normal production modes
- All sequential operations
- manual operations.
- exception and fault handling
- power failure
- process faults
- device and instrument failure.

The OQ will also test data storage, recovery operations, reporting functions and security operations.

System Acceptance Report (SAR)

The qualification process concludes with a formal System Acceptance Report (SAR), this assess the outcome of the IQ/OQ process and determines that the system is ready for use, it establishes that:

- All requirements in the URS have been satisfactorily met
- All quality and GMP requirements are satisfactorily complete
- The delivered system is satisfactory

3.7.1 Qualification phase — deliverables and responsibilities

The following deliverable items will be produced during the qualification phase of the Project, the purpose of each deliverable is described in the previous section:

O = Originator (author)
R = Review
A = Approve
N/A = Not applicable

	RESPONSIBILITY			
DELIVERABLE	Project Manager	Engineering	Quality/Validation	Customer/user
Requirements Traceability Matrix RTM [Ref. 007] – 4th release (IQ/OQ)	R	O	A	A
Installation Qualification IQ and report	RA	O	RA	RA
Operational Qualification OQ and report	RA	O	RA	RA
System Acceptance Report SAR [Ref. 013]	O	R	A	RA

Table 3.6 Qualification phase deliverables — see TP for IQ/OQ document references

3.8 Training & Use phase

The training and use phase of the Project is the final phase of the Project.

The training and use phase will to some extent run in conjunction with the qualification phase; it serves two functions:

- Collate all the documentation for the Project:
    - Operation and Maintenance Manual (O&M)
    - User Guide (training manual)
    - Full document pack (all deliverable documents)
- Train personnel in the use of the system

The Operation and Maintenance Manual (O&M) and the document pack will be collated during the qualification phase and will include the final "as-built" documentation including all drawings, certificates, instruction manuals and all deliverable documents in their final versions.

The User Guide (UG) will be the formal training manual for the system, it will also be the *"written description"* of the system required by the EU Regulations Volume 4: Pharmaceutical legislation – Medicinal Products for Human and Veterinary use – Good Manufacturing *[Ref. 019]*.

The deliverable items for the training and use phase are:

Operation and Maintenance Manual (O&M)

The Operation and Maintenance Manual (O&M) contains the principal operating instructions for the system; it will also include the manufactures literature and configuration details for all equipment installed within the system

The manual will contain sections for fault finding and repair, routine maintenance and recommended spares holding

User Guide (UG)

The User Guide (UG) is a comprehensive instruction manual for the PAL software, it provides a detailed description of the software and explains how it is to be used.

The User Guide contains an example application that may be used for training purposes to demonstrate the use of the library software modules and how these modules are to be used in a practical application.

Document Pack

The document pack contains the final “as-built” release of all the Project deliverable documents including all drawings, schedules, and supporting documentation.

The document pack will also include a final release of the RTM, this will be the fully validated “as-built” version of the RTM.

3.8.1 Qualification phase — deliverables and responsibilities

The following deliverable items will be produced during the qualification phase of the Project, the purpose of each deliverable is described in the previous section:

O = Originator (author)
R = Review
A = Approve
N/A = Not applicable

	RESPONSIBILITY			
DELIVERABLE	Project Manager	Engineering	Quality/Validation	Customer/user
Requirements Traceability Matrix RTM [Ref. 007] – 5th release (final)	R	O	A	A
Operation & Maintenance Manual O&M [Ref. 014]	R	OA	R	R
User Guide UG [Ref. 015]	R	OA	R	R
As-built documentation pack	As original documents			

Table 3.7 Training phase deliverables

3.9 Acceptance criteria

The system shall be accepted for use when the following criteria are satisfied:

- Required deliverable's have been produced, reviewed, and approved
- All tests defined by the Test Plan are complete
- All change controls and incidents have been satisfactorily completed. Where they could not be completed, these have been assessed to have no adverse impact on the final system and corrective action has been identified and assigned to individuals
- All User Documentation is complete and available for use
- Training of end users is complete and documented
- The System Acceptance Report is approved

3.10 Document revision in references

Where documents are referenced from within other documents, the current revision of the document is not quoted, neither is it quoted in the References section of the document, this is to prevent every document having to be changed if a single document is modified (changing the revision of the SDS would require the reference section of all documents that referenced it to be change, this in turn would require all documents that referenced those documents to also be updated &c.).

To prevent this, document references quote the document number only, the latest revision of which is listed in the Project Registry *[Ref. 020]*. When using the document reference, the Project Registry must be consulted to ensure the correct revision of the referenced document is used.

At the end of the Project when no further document changes will take place (i.e. when all as-built documentation is released) all document references will be updated to include the as-built revisions of all related documents for clarity.

BLANK PAGE

4 References and glossary

4.1 References

The following documents are referenced in this manual:

REF	DOCUMENT NO.	AUTHOR	TITLE/DESCRIPTION
001	PS2001-5-0100-001	PSP	Quality Manual (QM)
002	PS2001-5-0101-001	PSP	Quality Plan (QP)
003	PS2001-5-0111-010	PSP	Project Schedule (PS)
004	PS2001-5-0121-002	PSP	Validation Plan (VP) — THIS DOCUMENT
005	PS2001-5-0131-003	PSP	Test Plan (TP)
006	PS2001-5-1101-001	PSP	User Requirements Specification (URS)
007	PS2001-5-1111-001	PSP	Requirement Traceability Matrix (RTM)
008	PS2001-5-2101-001	PSP	Functional Specification (FS)
009	PS2001-5-2211-001	PSP	Hardware Design Specification (HDS)
010	PS2001-5-2311-001	PSP	Software Design Specification (SDS)
011	See SDS for details	PSP	Software Module Design Specifications (SMDSs)
012	PS2001-5-2611-001	PSP	Design Review Report (DRR)
013	PS2001-5-6141-001	PSP	System Acceptance Report (SAR)
014	PS2001-5-7101-001	PSP	Operation & Maintenance Manual (O&M)
015	PS2001-5-7111-001	PSP	User Guide (UG)
016	GAMP 5	ISPE	Good Automated Manufacturing Practice
017	IEC6113-3	IEC	Programmable controllers - Part 3: Programming languages
018	CFR 21, Part 11	US CFR	US Code of Federal Regulations, Title 21, Food and Drugs, Part 11 – Electronic Records, Electronic Signatures
019	EudraLex Vol 4 Annex 11	EU Regulations	Vol 4: Pharmaceutical legislation – Medicinal Products for Human and Veterinary use – Good Manufacturing
020	PS2001-0-01-001	PSP	Project Document Registry

Table 4.1 Table of references

4.2 Glossary of terms

ABBREVIATION	DESCRIPTIONS
ATEX	Appareils destinés à être utilisés en ATmosphères Explosives (French)
BS	British Standard
BS EN	British standards (BS) adoption of a European Standard (EN)
CCM	Change Control Management
CFR	Code of Federal Regulations
DR	Design Review
DRR	Design Review Report
DS	Design Specification (general term for: FS, HDS, SDS, SMDS &c.)
ERP	Enterprise Resource Planning
EudraLex	European Union Drug Regulation Authority Legislation
EU	European Union
FAT	Factory Acceptance Test
FS	Functional Specification
GAMP	Good Automated Manufacturing Practice
GCP	Good Clinical Practice
GDP	Good Distribution Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
GxP	Collective abbreviation for GMP and GXP
HDS	Hardware Design Specification
H-FAT	Hardware Factory Acceptance Test
H-FATR	Hardware Factory Acceptance Test Report
HMI	Human Machine Interface
IEC	International Electro-technical Commission
IEC 61131-3	IEC standard for the syntax and semantics for PLC programming
IET	Institution of Engineering and Technology
IM	Incident Management
IO	Input/output
IQ	Installation Qualification

ABBREVIATION	DESCRIPTIONS
IQR	Installation Qualification Report
ISPE	International Society for Pharmaceutical Engineering
IT	Information Technology
MIT	Massachusetts Institute of Technology (Licence)
MRPII	Management Resource Planning 2
O&M	Operation and Maintenance
OQ	Operational qualification
OQR	Operational Qualification Report
PAL	Practical Series Automation Library
PLC	Programmable Logic Controller (another name for a Siemens
POC	Proof of Concept
PS	Project Schedule
PSP	Practical Series of Publications
QM	Quality Manual
QMS	Quality Management System
QP	Quality Plan
RTM	Requirements Traceability Matrix
RRN	Risk Rating Number
SAR	System Acceptance Report
SCADA	Supervisory Control and Data Acquisition
SCR	Source Code Review
SDS	Software Design Specification
S-FAT	Software Factory Acceptance Test
S-FATR	Software Factory Acceptance Test report
SG	Style Guide
SIT	Software Integration Test
SITR	Software Integration Test Report
SMDS	Software Module Design Specification
SMT	Software Module Test
SMTR	Software Module Test Report
SOP	Standard Operating Procedure
TIA	Totally Integrated Solutions (TIA Portal, a Siemens programming tool)

ABBREVIATION	DESCRIPTIONS
TP	Test Plan
UG	User Guide
URS	User Requirements Specification
US	United States of America
VP	Validation Plan

Table 4.2 Glossary

APPENDICES

BLANK PAGE

A Risk assessments

A.1 Simultaneous software build and test

A.1.1 Description of the process and overview of the risks

In order to shorten the Project timescales, it is proposed that some degree of overlap between the design phase, the build phase (the writing of the software) and the test phase (explicitly the software module tests) takes place.

The justification for this proposal is that the nature of the Project is to produce a library of software modules, each module being written to incorporate the requirements and specification listed in its own Software Module Design Specification; each of these modules is effectively a stand-alone piece of software that can be designed, built and tested in its own right and without impact on any other software module.

This approach may increase the risk of software errors, it may be possible for the writing of subsequent modules to impact an existing and tested module adversely.

A.1.2 Existing controls

All software developed within the Project is subject to change control and exists within the change control management process put in place for this project and listed in the Quality Plan *[Ref.* 002*]*.

Change control is implemented at the module level for the Project software.

A.1.3 Assessment details

This assessment has been carried out by:

	NAME	POSITION	SIGNATURE	DATE
Assessor	Michael Gledhill	Lead Engineer	M Gledhill	5 JUN 20

A.1.4 Quantifying the risk

The risk is quantified by determining various factors:

- **Possibility** Measures the likelihood of the hazard occurring (less possible is better)
- **Frequency** How often the hazard is likely to occur (less frequent is better)
- **Detectability** How easy it is to detect the hazard (easier to detect is better)
- **Severity** How serious is the hazard (less sever is better)

By assigning probability values to each of these factors and multiplying the results together, a risk rating number (RRN) can be determined, the action to be taken (measures to be put in place) is dependent on the value of the RRN.

The following table presents the possible values for the various factors and the degree of risk and the action to be taken for the range of RRN values:

Possibility (P)		Frequency (F)		Detectability (D)		Severity (S)		Risk	RRN	Action
0.0	Impossible	0.1	Infrequent	1	High	0.1	Negligible	Negligible	0-1	Tolerable risk,
0.1	Almost Impossible	0.2	Annually	2	High-medium	0.5	Minor	Very low risk	2-5	no action
0.5	Highly Unlikely	1.0	Monthly	4	Medium	1.0	Moderate	Low risk	6-10	Longer tern
1.0	Unlikely	1.5	Weekly	8	Low-medium	2.0	Major	Significant risk	11-50	action required
2.0	Possible	2.5	Daily	12	Low	4.0	Severe	High risk	51-100	Short term
5.0	Even chance	4.0	Hourly			8.0	Critical	Very high risk	101-500	action required
8.0	Probable	5.0	Constantly					Extreme risk	501-1000	Immediate action
10.0	Likely							Unacceptable risk	>1000	Stop activity
15.0	Certain							Risk rating number (RRN) = P × F × D × S		

Table A.1 Risk quantification table

A.1.5 Initial risk assessment

The following risk assessment is based upon the existing measure listed in A.1.2:

Item	Hazard	Event	P	F	D	S	RRN
1	Potential to modify or delete a tested block	• Tested block may no longer function • All tests will be invalidated for the block • Blocks calling the affected block may no longer function	2.0	1.5	2	1.0	6.0
2	Potential to modify data structures (user data types) used by the tested block	• Tested block may no longer function • Tested block will have inconsistent data • Tested block interface will no longer function	2.0	1.5	4	1.0	6.0
3	Changes to global data structures used by a tested block	• Tested blocks may no longer function • Tested blocks will have inconsistent data • Will impact all tested block (multiple block impact)	2.0	1.0	4	8.0	64.0
4	Changes to a subroutine block used by a tested block	• Tested block may no longer function • Tested block will have inconsistent data • Blocks calling the tested block may no longer function • Will impact all block that use the subroutine (multiple block impact)	2.0	1.0	4	4.0	32.0
5	Potential to overwrite an existing block with a new block (i.e. inadvertent use of the same block number)	• Tested block will be overwritten • Inconsistences in documentation • Impact to both the tested block and the new block	2.0	1.5	2	1.0	6.0

Table A.2 Original risk assessment

The result of the original assessment is that action is required for all the hazards listed in the above table.

A.1.6 Remedial actions

The following remedial actions are to be put in place

Action No	Description
1	Ensure version control is present at the module level (this will utilise the Workspace facilities of TIA Portal and version control will be maintained with the Git and GitHub version control systems (VCS) — Git and GitHub are the standard VCS used with the PSP.
2	Establish a register of software modules and data structures, this will record tested status and version number for each block and structure
3	Software module test specification will record the final version of the tested block and any associated data structure, it will also record the working memory usage of the block as a "checksum" figure that can be verified by examining the block properties
4	Establish a repository for tested blocks, under the control of a nominated individual
5	Only the nominated individual can copy a tested block or data structure into the repository. If the copy process indicates that a block or structure is to be over written, the nominated individual will stop the process and request clarification from the submitting source
6	Prior to using any subroutine or tested block, a comparison will be made against the same block in the repository (this is facility is available within the TIA programming application)
7	Global data, its data structures and data containment areas, and the modules that generate that data will be established as the first testable modules and once tested will have protected access ("write protect" in Siemens terminology)
8	Subroutine modules will be tested prior to any block that is to use them and once tested will have protected access ("write protect" in Siemens terminology)

Table A.3 Remedial actions

Note: *Actions 7 and 8 require the protection of blocks within the software using the "write protect" function. The write protect function supersedes the previous "knowhow protect" function and is generally more flexible. The knowhow protect function, while preventing the overwriting or modification of a software module, was generally inconvenient, it prevented the user from accessing, or seeing the software within the block for reference purposes. The write protect function, however allows the block contents to be freely viewed, but prevents any attempt to modify or delete the block.*

A.1.7 Final risk assessment

The following risk assessment is based upon the remedial actions listed in 0:

Item	Hazard	Applicable remedial actions								P	F	D	S	RRN
1	Potential to modify or delete a tested block	1	2	3	4	5				0.5	1.5	2	1.0	1.5
2	Potential to modify data structures (user data types) used by the tested block	1	2	3	4	5				0.5	1.5	2	1.0	1.5
3	Changes to global data structures used by a tested block	1	2	3	4	5		7		0.1	1.0	2	8.0	1.6
4	Changes to a subroutine block used by a tested block	1	2	3	4	5	6		8	0.1	1.0	2	4.0	0.4
5	Potential to overwrite an existing block with a new block (i.e. inadvertent use of the same block number)	1	2	3	4	5				0.5	1.5	2	1.0	1.5

Table A.4 Final risk assessment

A.1.8 Conclusions

The remedial activities listed in A.1.6 reduce the risks to a very low level where no further action is required.

All the remedial actions listed in A.1.6 will be put in place on the Project. The Lead Engineer will be the nominated individual listed in actions 4 and 5.