



GAMP Good Practice Guide

A Risk-Based Approach to GxP Process Control Systems

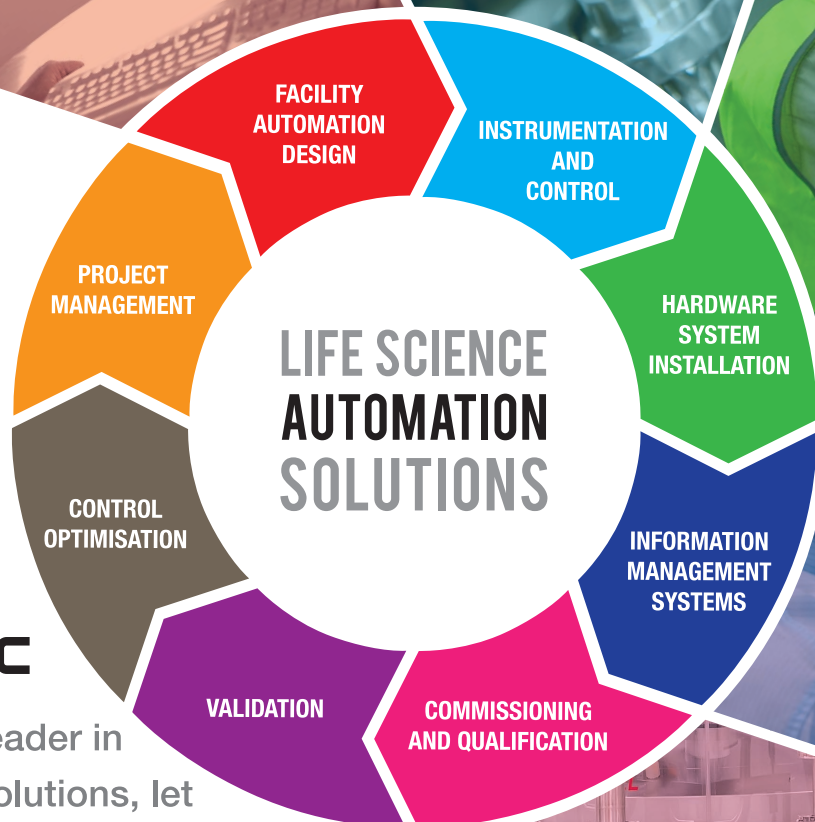
Second Edition



Documents
Document Sharing Hub



SYNERTEC



SYNERTEC

As a renowned leader in control system solutions, let us guide you through the crucial phases of your automation project with our in-depth experience in :

• Design • Integration • Validation
Complete Compliance with GAMP

Sydney
Melbourne
www.synertec.com.au

Singapore
Kuala Lumpur 
www.synertecasia.com

Documents
Document Sharing Hub



GAMP Good Practice Guide

A Risk-Based Approach to GxP Process Control Systems

Second Edition

Disclaimer:

This Guide is meant to assist regulated companies in achieving and maintaining compliant process control systems that are fit for intended use. The International Society for Pharmaceutical Engineering (ISPE) cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability

In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

© Copyright ISPE 2011. All rights reserved.

No part of this document may be reproduced or copied in any form or by any means – graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems – without written permission of ISPE.

All trademarks used are acknowledged.

ISBN 978-1-936379-05-7

Preface

This GAMP® Good Practice Guide: A Risk-Based Approach to GxP Process Control Systems provides additional guidance and examples for the application of GAMP 5: A Risk-Based Approach to Compliant GxP Computerized Systems to a range of GxP regulated process control systems.

This Guide also may be used in conjunction with the other ISPE guidance documents such as Good Practice Guides (GPGs) and Baseline® Guides.

This Guide has been produced by a GAMP® Community of Practice (COP) Task Team. This team included representatives from regulated companies and a wide range of suppliers, including OEMs, Integrators, and managing contractors.

Acknowledgements

The following Task Team, and members of the ISPE GAMP Community of Practice (COP) Process Control Special Interest Group (SIG), worked on one or more of the sections of this document and volunteered their knowledge, practical experience and precious time to provide input material, attend meetings and review the multiple drafts.

Task Team Leader/SIG Chair:

Mark Cherry	AstraZeneca	United Kingdom
-------------	-------------	----------------

Task Team Co-Leader/SIG Deputy Chair:

Hilary Mills-Baker	WSP CEL Ltd.	United Kingdom
--------------------	--------------	----------------

GAMP Council Sponsor:

Guy Wingate	GlaxoSmithKline	United Kingdom
-------------	-----------------	----------------

Special Interest Group Team:

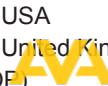
Karen Ashworth	Karen Ashworth Consulting Ltd.	United Kingdom
Roger Buchanan	Eli Lilly & Co. Ltd.	United Kingdom
Reetu Chopra	Teva Pharmaceuticals	United Kingdom
Peter Falcon	AstraZeneca	United Kingdom
David James	Invensys System (UK) Ltd.	United Kingdom
Peter Iles-Smith	GlaxoSmithKline	United Kingdom
Martin Isherwood	Eli Lilly & Co. Ltd.	United Kingdom
Malcolm Knott	Industrial Technology Systems Ltd.	United Kingdom
Walfraid Laibacher	Honeywell Building Solutions GmbH	Germany
Brian Nolan	Organon Ireland Ltd.	Ireland
Blaise Polentes	Sanofi-Aventis R&D	USA
Bo Reedtz		Denmark
George Smerdon	Industrial Technology Systems Ltd.	United Kingdom
Sue Tuxford	Emerson Process Management	United Kingdom
Rainer Van Deursen	Eurotherm Deutschland GmbH	Germany
Gerhard Werling	Rockwell Automation Solutions GmbH	Germany

The Task Team would like to acknowledge the support of their direct management and companies in this endeavor.

The Task Team leaders would like to express their thanks to the following for their contribution of additional materials and as technical reviewers of the Guide:

John Robert (Bob) Adamson*	RBQ Services Limited	United Kingdom
John Berridge	ISPE European Regulatory Affairs Advisor	United Kingdom
Joerg Block	Bayer HealthCare AG	Germany
Winnie Cappucci	Bayer HealthCare	USA
Waunetka A. Clark	Abbott Laboratories	USA
Sandro De Caris	GAMP Italiano / Consultant	Italy
Rick Gunyon*	Eli Lilly and Co.	USA
Justin Iovino	Cognizant Technology Solutions	USA
Jim John	ProPharma Group / JETT SIG of GAMP Americas	USA
Richard Lemire	Novartis Pharmaceuticals Corporation	USA
Tony Margetts	Factorytalk Co. Ltd.	Thailand
Dr. Arthur (Randy) Perez	Novartis Pharmaceuticals Corporation	USA
Gregory Ruklic	Independent Life Sciences Professional	USA
Tulsa Scott*	Commissioning Agents	USA
Jennifer Thompson	ABB (now of Durham University)	United Kingdom

*Member of the ISPE Commissioning & Qualification Community of Practice (C&Q COP)



Documents

Document Sharing Hub

Regulatory Input and Review

Particular thanks go to the following individuals for their review and comment:

Karl-Heinz Menges, Regierungspräsidium Darmstadt GMP-inspectorate (Germany)
George Smith, Office of Compliance, CDER FDA (USA)
Robert D. Tollefsen, Division of Domestic Field Investigations, ORA/ORO FDA (USA)
Malcolm Olver, MHRA (UK)

ISPE and GAMP COP Committees

Members of the ISPE GAMP COP Council and Steering Committees, along with the ISPE Guidance Documents Committees are thanked for their participation in the review of this Guide.

Editorial Team

Particular thanks to the sub-team that reviewed the industry comments, filtered and dealt with the extensive input, and edited and re-structured the Guide:

Karen Ashworth	Karen Ashworth Consulting Ltd.	United Kingdom
Mark Cherry	AstraZeneca	United Kingdom
Hilary Mills-Baker	WSP CEL Ltd.	United Kingdom
Sue Tuxford	Emerson Process Management	United Kingdom
Chris Clark	Napp Pharmaceuticals Ltd.	United Kingdom
Colin Jones	Conformity Ltd.	United Kingdom
Sion Wyn	Conformity Ltd.	United Kingdom

Many other individuals reviewed and provided comments during the preparation of this Guide; although they are too numerous to list here, their input is greatly appreciated.

Table of Contents

1	Introduction	9
1.1	Rationale for this Revision	9
1.2	Purpose.....	10
1.3	Scope.....	10
1.4	Structure of this Guide	12
1.5	Benefits	13
2	Key Concepts	15
2.1	Product and Process Understanding	16
2.2	Life Cycle Approach within a QMS.....	16
2.3	Scalable Life Cycle Activities	17
2.4	Science-Based Quality Risk Management.....	17
2.5	Leveraging Supplier Involvement.....	18
3	Features Special to Process Control Systems	21
3.1	Multiple Components and Multiple Suppliers.....	21
3.2	Interfaces to a Physical Process.....	24
3.3	Interfaces with Process Equipment.....	25
3.4	Phased Delivery.....	27
4	Process Control System Life Cycle Overview	29
4.1	Roles and Responsibilities.....	31
4.2	Process Control System Supplier Life Cycles.....	32
4.3	Leveraging Supplier Effort	33
4.4	Leveraging Supplier Effort for Different Types of Control Systems.....	34
4.5	Hardware and Software Categories.....	35
5	Quality Risk Management	39
5.1	ICH Q10 Pharmaceutical Quality System	39
5.2	ICH Q9 Quality Risk Management.....	39
5.3	ICH Q8 Pharmaceutical Development	40
5.4	Risk Management in the Life Cycle	41
5.5	Scalability of Risk Management.....	42
5.6	Step 1 – Initial Assessment and Determination of System Impact.....	43
5.7	Step 2 – Identify Functions with Impact	44
5.8	Step 3 – Perform Functional Risk Assessments and Identify Controls	45
5.9	Step 4 – Implement and Verify Appropriate Controls	47
5.10	Step 5 – Review Risks and Monitor Controls.....	47
6	Concept Phase of the Life Cycle	49
6.1	Introduction	49
6.2	Specific Considerations for Process Control Systems.....	49
7	Project Phase of the Life Cycle	53
7.1	Process Control System Validation Planning.....	53
7.2	Specification.....	57
7.3	Configuration and Coding	63
7.4	Verification	68
7.5	Reporting and Release	74

8	System Operation	77
8.1	Introduction	77
8.2	Handover	78
8.3	Establishing and Managing Support Services	79
8.4	Performance Monitoring.....	80
8.5	Incident Management and CAPA.....	81
8.6	Repair Activity	82
8.7	Periodic Review	83
8.8	Backup and Restore	84
8.9	Business Continuity and Disaster Recovery Planning.....	85
8.10	Security Management.....	86
8.11	System Administration	87
8.12	Record Retention, Archive, and Retrieval.....	87
9	Retirement Phase of the Life Cycle.....	89
9.1	Introduction	89
9.2	Overall Strategy	89
10	Supporting Processes.....	91
10.1	Supplier Assessment	91
10.2	Design Review and Traceability.....	92
10.3	Change and Configuration Management.....	95
10.4	Document Management.....	97
11	Governance for Achieving Compliance.....	99
11.1	Policies and Procedures	99
11.2	Roles and Responsibilities.....	100
11.3	Training	100
11.4	Management of Suppliers	100
11.5	Systems Inventory	101
11.6	Planning for Validation	101
11.7	Continuous Improvement Activities.....	101
12	Supplier Activities.....	103
12.1	Introduction	103
12.2	Considerations for Process Control Systems	103
12.3	Supplier Good Practices for Process Control Systems.....	103
13	Appendix E1 – Example: Categorizing Software Elements	107
13.1	Discussion on Boundaries between Categories 3 and 4	107
13.2	Discussion on Boundaries between Category 4 and Category 5 Components	108
13.3	Classification of Standard Products Involving Configured or Coded Items.....	110
13.4	Example Classification 1 – Large Distributed Control System.....	112
13.5	Example Classification 2 – PLC Control System (Custom Machine).....	113
13.6	Example Classification 3 – PLC Control System (Standard Product).....	114
13.7	Example Classification 4 – Simple PID Controller	115
14	Appendix E2 – Example: Life Cycle Activities	117

15	Appendix E3 – Example: Risk Management Process	123
15.1	Example Method for Defining System and the Functions within It.....	123
15.2	Example Method for Rating Impact or Severity	125
15.3	Example Method for Rating Likelihood	126
15.4	Example Method for Rating Detectability.....	127
15.5	Example Method for Assessing Overall Risk and Identifying Required Controls.....	127
16	Appendix E4 – Example: CQAs/CPs at Different Levels of Specification.....	131
17	Appendix E5 – Example: Assessing Different Types of Suppliers	135
17.1	Introduction	135
17.2	Original Equipment Manufacturers	135
17.3	Packaged Equipment Suppliers.....	135
17.4	System Integrators.....	136
17.5	Service Providers.....	136
17.6	Suppliers of Standard Products	137
17.7	Process Control System Manufacturers	137
17.8	Assessment of Suppliers to the Supplier	138
17.9	Certification of Suppliers.....	139
18	Appendix E6 – Example: Verification Activities	141
19	Appendix E7 – Example: The Impact of Phased Delivery	145
19.1	Introduction	145
19.2	Example of a Phased Release of Software to Site	146
19.3	Database Item Control.....	147
19.4	Example Considerations for Planning Phased Releases.....	147
20	Appendix E8 – Example: System Patches	151
20.1	Introduction	151
20.2	Components within a Process Control System.....	151
20.3	Patch Management Process.....	154
20.4	Backup.....	155
21	Appendix E9 – Example: System Retirement	157
21.1	Responsibility.....	157
21.2	Retirement Planning Considerations	157
21.3	Retirement Activities	158
21.4	Example Retirement Approaches	159
22	Appendix S1 – Process Analytical Technology (PAT)	161
22.1	Introduction	161
22.2	What is a PAT System?.....	162
22.3	Examples of PAT Systems.....	163
22.4	What Is Special About PAT Systems – Additional Risks?	165
22.5	What Is Special About PAT Systems – Life Cycle Activities?	168
23	Appendix S2 – Alarm Strategy.....	171
23.1	The Alarm System.....	171
23.2	Alarm Management Life Cycle.....	171
23.3	The Process Condition Model.....	175
23.4	Alarm Life Cycle Entry Points	175

24	Appendix S3 – Batch Control and ANSI/ISA-88 and ANSI/ISA-95	177
24.1	Understanding the Basics of ANSI/ISA-88 and ANSI/ISA-95.....	177
24.2	Understanding S95	177
24.3	Understanding S88	178
24.4	Compliance Considerations	181
25	Appendix 13 – References	183
26	Appendix 14 – Glossary	185
26.1	Abbreviations and Acronyms	185
26.2	Definitions	187



ISPE Headquarters (until 20 April 2011)

3109 W. Dr. Martin Luther King Jr. Blvd., Suite 250, Tampa, Florida 33607 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

ISPE Headquarters (effective 21 April 2011)

600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

ISPE Asia Pacific Office

73 Bukit Timah Road, #04-01 Rex House, Singapore 229832
Tel: +65-6496-5502, Fax: +65-6336-6449

ISPE China Office

Suite 2302, Wise Logic International Center
No. 66 North Shan Xi Road, Shanghai, China 200041
Tel +86-21-5116-0265, Fax +86-21-5116-0260

ISPE European Office

Avenue de Tervueren, 300, B-1150 Brussels, Belgium
Tel: +32-2-743-4422, Fax: +32-2-743-1550

www.ISPE.org

1 Introduction

This Good Practice Guide (GPG) aims to achieve process control systems that are fit for intended use and meet current regulatory requirements, by building upon existing industry good practice in an efficient and effective manner.

It provides recommended good practice based on a life cycle approach for the development and management of process control systems.

This Guide covers both regulated company and supplier Quality Management Systems, and is applicable across the full system life cycle from concept to retirement.

The Guide recognizes that Good Engineering Practice meets most of the applicable compliance requirements. The Guide also emphasizes that in order to be efficient, appropriate specification and verification activities should be an integral part of the normal system life cycle.

The Guide recognizes that many suppliers of systems now have mature quality management systems and system development, test, and support documentation. The Guide promotes the leveraging of supplier documentation and activities to avoid unnecessary duplication, cost, and waste.

Wherever possible, a range of examples across differing systems has been included to illustrate the approach and the scalability that may be applied. Examples are introduced in the body of the document, and expanded as appropriate in the Appendices.

The Guide applies science-based Quality Risk Management, as described in ICH Q9 (Reference 2, Appendix 13) and GAMP 5 (Reference 15, Appendix 13).

1.1 Rationale for this Revision

This revision has been significantly updated to align with the concepts and terminology of recent regulatory and industry developments including:

- International Conference on Harmonisation (ICH) Guidance setting out expectations for the application of science- and risk-based approaches to drug development and manufacture supported by pharmaceutical quality systems
- Product Quality Lifecycle Implementation® (PQLI®) – ISPE's global industry initiative for a practical approach to implementation of International Conference on Harmonisation (ICH) guidances Q8 (R2), Pharmaceutical Development, Q9, Quality Risk Management and Q10, Pharmaceutical Quality System (References 7, 1, 2, and 3, Appendix 13)
- FDA cGMPs for the 21st Century Initiative and associated guidance promoting science-based risk management (Reference 5, Appendix 13)
- Emerging industry standards such as those produced by the ASTM E55 Committee promoting process understanding, control and capability for drug development and manufacture (Reference 17, Appendix 13)
- ISPE Guide: Science and Risk-Based Approach for the Delivery of Facilities, Systems, and Equipment (under development at time of publication, Reference 13, Appendix 13)

Where the previous edition focused specifically on the validation of process control systems, this Guide has a wider scope. It describes good practice based on a complete life cycle approach for the development and management of compliant process control systems, reflecting the above developments.

1.2 Purpose

The purpose of this Guide is to provide a cost effective framework of good practice to ensure that process control systems are fit for intended use and compliant with applicable regulations. The framework aims to safeguard patient safety, product quality, and data integrity, while also delivering business benefit.

This Guide provides guidance and examples on the application of the principles and framework of GAMP 5 (Reference 15, Appendix 13) to a wide range of GxP regulated process control systems.

This Guide also provides suppliers to the life science industry with guidance on the development and maintenance of process control systems by following good practice.

This Guide also may be used in conjunction with the other ISPE publications such as Good Practice Guides (GPGs) and ISPE Baseline® Guides.

1.3 Scope

This Guide applies to process control systems used in GxP regulated activities, including development, manufacturing, and distribution of the product.

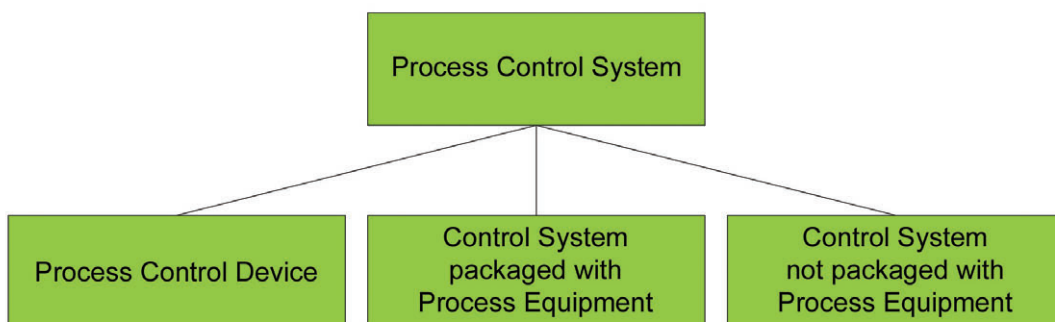
The scope covers a wide range, from basic instruments to large, complex, distributed control systems.

Process control systems may maintain electronic records and signatures subject to specific GxP regulations such as US FDA 21 CFR Part 11 (Reference 4, Appendix 13). Therefore, systems should be assessed to see if they fall within the scope of these or other applicable regulations. Detailed guidance can be found in the GAMP Good Practice Guide: A Risk-Based Approach to Compliant Electronic Records and Signatures (Reference 16, Appendix 13).

The overall IT infrastructure of the regulated company is outside the scope of this Guide. Analytical laboratory instruments are also outside the scope of this Guide. These topics are covered in separate GAMP Good Practice Guides.

This Guide distinguishes three types of process control systems. These are intended to be used in conjunction with GAMP categories to highlight system scale and complexity (often in terms of the range of suppliers involved), and to allow a common basis for presenting examples across a range of systems.

Figure 1.1: Types of Process Control Systems



Note that this division into “device,” “packaged with process equipment,” and “not packaged with process equipment” is independent of the GAMP category. Some examples are given below and more detail on categorization is given in Section 4.4 of this Guide.

Table 1.1: Examples of Process Control Systems

System Type	Process Control Device	Control System Packaged with Process Equipment	Control System Not Packaged with Process Equipment
Detail of System Type	Single device from a single supplier comprises an entire standalone process control system.	Process control elements are embedded within process equipment into a “packaged” product from a supplier where the supplier Quality Management System provides assurance of the system in effect as though it were a commodity (may comprise multiple instruments, PLCs, and SCADA/HMI components).	Process control system elements are developed independently in order to deliver a specific business process (may involve integrating multiple process control devices or packaged systems).
Category 3 Non-configured	Simple controller requiring parameter entry only (e.g., PID controller).	“Off the shelf” or “skid” equipment where each instance requires parameter entry only.	(Highly unlikely for a whole system though elements within the system – e.g., security setup – may fall into this category).
Category 4 Configured	Complex controller where library modules are selected and connected together to perform the required functions.	“Off the shelf” or “skid” equipment where each instance is configurable with appropriate library modules selected and connected together to provide the required control.	Much of a typical DCS or SCADA system may fall within this category with the process controls configured by selecting and connecting library modules.
Category 5 Custom	Custom controller with functionality coded specifically for the application.	Custom machine or “skid” equipment with functionality coded specifically for the application.	Functionality coded specifically for the application such as custom sequencing and custom interfaces.

For further discussion of typical components of a process control system and the application of ANSI/ISA-88 and ANSI/ISA-95 (Reference 11, Appendix 13), see Appendices S3 and E8.

Related facility and equipment topics, including, but not limited to the following, should be considered, but are outside the scope of this document:

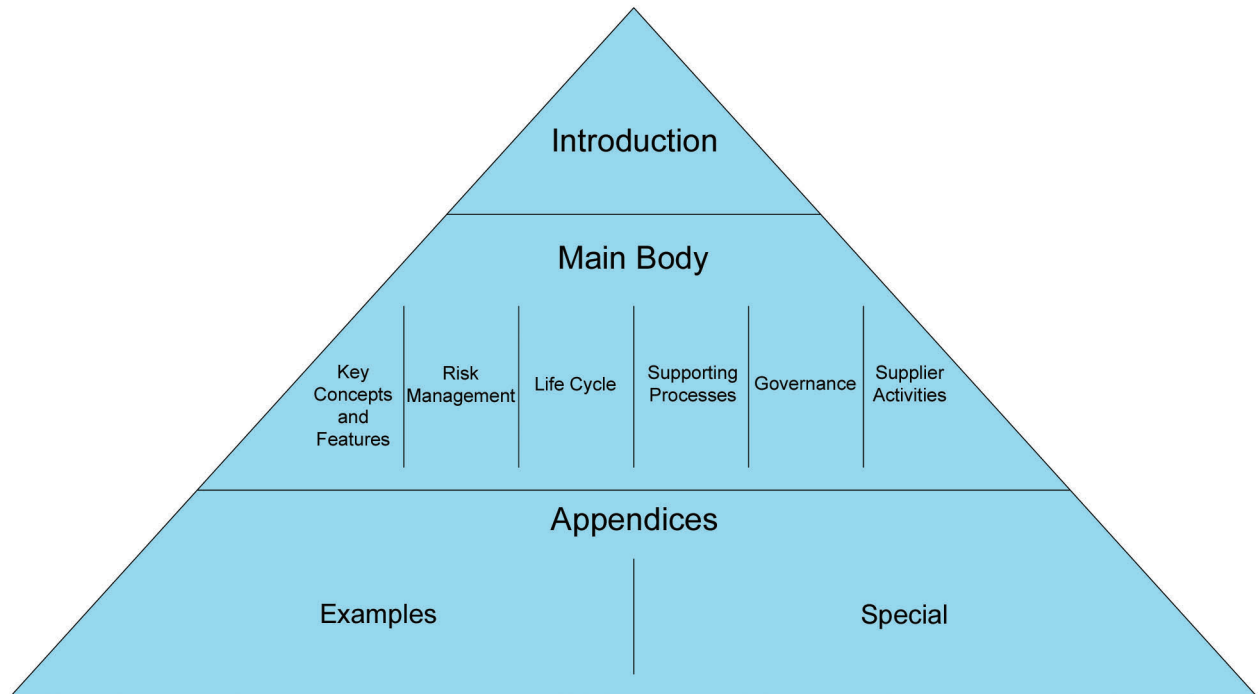
- Environmental Control
- Product Contact
- Equipment Cleaning and Maintenance
- Equipment Calibration
- Equipment Identification

For further details on these topics, see the ISPE Good Practice Guide: Good Engineering Practice and ISPE GAMP Good Practice Guide: Calibration Management (References 14 and 16, Appendix 13).

1.4 Structure of this Guide

This Guide comprises a Main Body and a set of supporting Appendices, as shown in Figure 1.2.

Figure 1.2: Structure of this Guide



The Guide concentrates on those features that are in some way special to process control systems. These features are discussed in Section 3 of this Guide. Subsequent sections describe the system life cycle from concept to retirement, providing a high level overview of the approach together with guidance on how activities might be scaled based on risk to product quality, system novelty, and complexity and other project specific factors.

These sections are supported by Appendices (E1 to E9) which provide detailed examples for those activities which are in some way special to process control systems:

- Appendix E1** Example: Categorizing Software Elements
- Appendix E2** Example: Life Cycle Activities
- Appendix E3** Example: Risk Management Process
- Appendix E4** Example: CQAs/CPs at Different Levels of Specification
- Appendix E5** Example: Assessing Different Types of Suppliers
- Appendix E6** Example: Verification Activities
- Appendix E7** Example: The Impact of Phased Delivery

Appendix E8 Example: System Patches

Appendix E9 Example: System Retirement

Some technical aspects that are relevant to process control systems are addressed in separate Special Topic appendices (S1 to S3) as follows:

Appendix S1 Process Analytical Technology (PAT)

Appendix S2 Alarm Strategy

Appendix S3 Batch Control and ANSI/ISA-88 and ANSI/ISA-95

1.5 Benefits

This Guide is intended to benefit both regulated companies and suppliers.

Adherence to a structured life cycle approach should result in a cost effective, efficient system that is compliant and meets the user's requirements.

There is significant benefit in leveraging supplier activities and documentation and avoiding duplication of effort, subject to appropriate supplier assessment. An effective science-based Quality Risk Management approach based on product and process understanding reduces risk to product quality, patient safety, and data integrity, and potentially saves time and effort.

Specific business benefits to both regulated companies and suppliers include:

- reduction of cost and time taken to achieve and maintain compliance
- early defect identification and resolution leading to reduced impact on cost and schedule
- cost effective operation and maintenance

Other benefits include:

- a comprehensive overview of current good practice for regulated process control systems
- harmonized approaches for different types of process control systems
- definition of the process control system life cycle, and discussion of the detailed engineering activities
- generation of accurate and complete user requirements with an early emphasis on product and process understanding
- guidance on functionality and structure of process control systems
- guidance on the supplier services required for regulated environments
- guidance on effective collaboration between regulated companies and suppliers
- guidance on leveraging of supplier documentation
- scalability of approach based on risk, GAMP categorization, and other factors

A standard approach and documentation set may reduce project execution, integration services, and rework costs. More efficient system start-up and more effective specification and verification may reduce time to market. Business risk for suppliers also may be reduced by following a controlled project life cycle, with clear roles and responsibilities, and with regulated companies being prepared to accept suitable supplier approaches and deliverables.

2 Key Concepts

Within this section, the key concepts from GAMP 5 (Reference 15, Appendix 13) are shown *italicized* and are followed by a discussion of the application of each concept to process control systems.

The following five key concepts are described in GAMP 5:

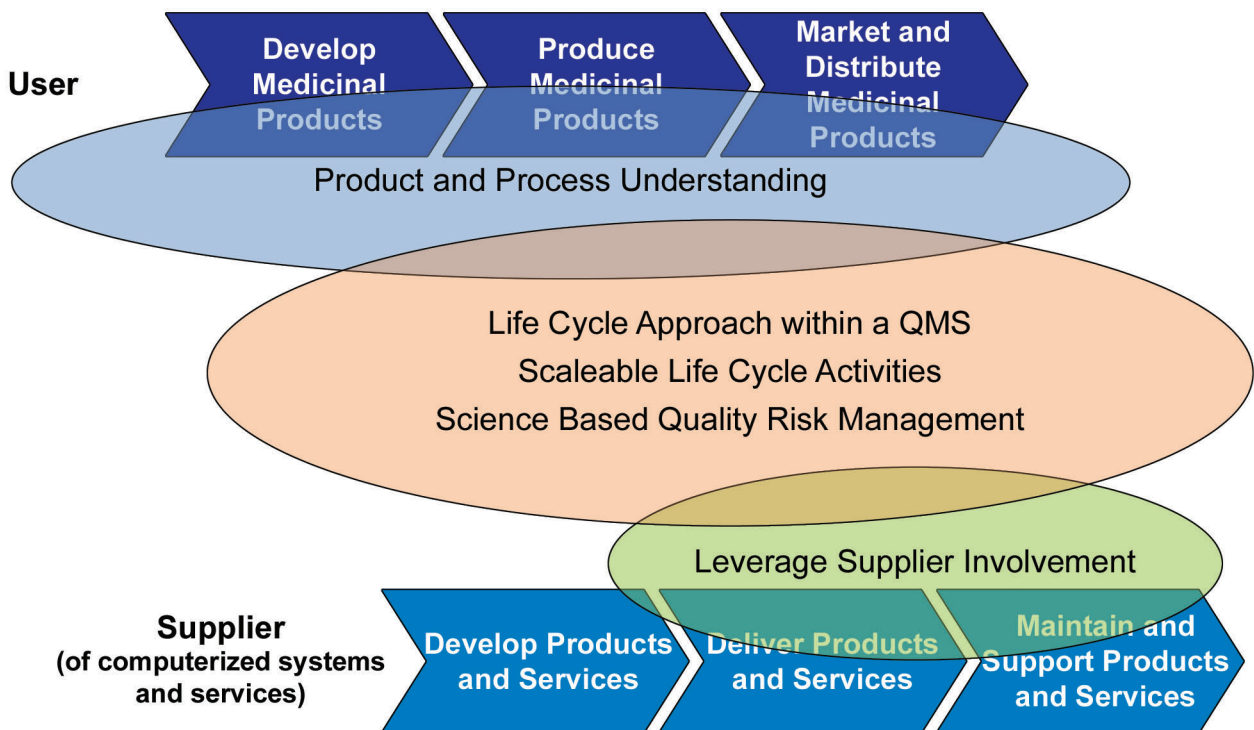
1. Product and Process Understanding
2. Life Cycle Approach within a Quality Management System (QMS)
3. Scalable Life Cycle Activities
4. Science-Based Quality Risk Management
5. Leveraging Supplier Involvement

Process control systems differ from other computerized systems in that they may physically affect or measure the process, often in real-time. Therefore, they may have potentially high impact on product quality.

This affects the practical implementation and application of these key concepts.

This and other aspects of what is special about process control systems are further explored in Section 3 of this Guide.

Figure 2.1: GAMP 5 Key Concepts



2.1 Product and Process Understanding

An understanding of the supported process is fundamental to determining system requirements. Product and process understanding is the basis for making science- and risk- based decisions to ensure that the system is fit for its intended use.

Efforts to ensure fitness for intended use should focus on those aspects that are critical to patient safety, product quality, and data integrity. These critical aspects should be identified, specified, and verified.

For some manufacturing systems, process requirements depend on a thorough understanding of product characteristics. For these systems, identification of Critical Quality Attributes (CQAs) and related Critical Process Parameters (CPPs) enable process control requirements to be defined.

Specification of requirements should be focused on critical aspects. The extent and detail of requirement specification should be commensurate with associated risk, complexity, and novelty of the system.

Incomplete process understanding hinders effective and efficient compliance, and achievement of business benefit.

Output from the pharmaceutical development process (in terms of the process and product understanding underlying the proposed control strategy) feeds through into process control system risk management. Linkages between the GAMP 5 (Reference 15, Appendix 13) life cycle and the pharmaceutical development process detailed in ICH Q8 (R2) (Reference 1, Appendix 13) are discussed in more detail in Section 5.3 of this Guide.

Requirements capture for a process control system requires input from a wide range of subject matter experts in addition to the control system designers. Requirements for product purity, e.g., may involve expertise in product/ process, clean in place, sanitization, and knowledge of regulatory requirements.

Requirements capture also will need to consider both understanding gained from the pharmaceutical development process and understanding of the system capability. For example, a temperature which may have been controllable to $\pm 0.5^{\circ}\text{C}$ in the small pilot plant reactor may not be achievable in a full scale reactor.

For systems where the process control system is packaged with the process equipment, it is more likely that the supplier will have a significant degree of understanding of the business process. In such cases, this knowledge should be leveraged.

Where process plant and its associated control system are multi-purpose, the control strategy is defined by the required process capability. As each new product is introduced to a multipurpose facility, the required capability for the product needs to be mapped onto this process capability.

2.2 Life Cycle Approach within a QMS

Adopting a complete computerized system life cycle entails defining activities in a systematic way from system conception to retirement. This enables management control and a consistent approach across systems.

The life cycle should form an intrinsic part of the company's QMS, which should be maintained up to date as new ways of working are developed.

As experience is gained in system use, the QMS should enable continuous process and system improvements based on periodic review and evaluation, operational and performance data, and root-cause analysis of failures. Identified improvements and corrective actions should follow change management.

A suitable life cycle, properly applied, enables the assurance of quality and fitness for intended use, and achieving and maintaining compliance with regulatory requirements. A well managed and understood life cycle facilitates adoption of a Quality by Design (QbD) approach.

The overall life cycle approach for the process control system needs to take into account the range of components and suppliers used. For example, process control equipment is often produced by one or more suppliers and integrated and configured by another supplier. Therefore, thought needs to be given to minimizing duplication of activities within the life cycles applied by each party.

2.3 Scalable Life Cycle Activities

Life cycle activities should be scaled according to:

- *system impact on patient safety, product quality, and data integrity (Risk Assessment)*
- *system complexity and novelty (architecture and categorization of system components)*
- *outcome of supplier assessment (supplier capability)*

Business impact also may influence the scaling of life cycle activities.

The strategy should be clearly defined in a plan and follow established and approved policies and procedures.

All GxP regulated computerized systems require some form of well-understood and well-managed life cycle.

Scalability involves tailoring the system life cycle by selecting the appropriate life cycle activities, and choosing the appropriate extent, effort, rigor, and level of documentation for these activities. Note that in this context scalability is being considered from the perspective of the regulated company system life cycle not the supplier product life cycle. Furthermore, life cycle activity scalability, and to what extent leveraging of supplier activities is appropriate, are closely related but separate decisions.

Process control system complexity and novelty varies widely – from standard, non-configured items through to highly customized applications – giving potential for appropriate scaling of activities. The GAMP categories provide a useful tool in this respect. For further details on application of these categories to process control systems, see Appendix E1.

To successfully scale the life cycle activities, the regulated company needs to be fully aware of all these complexities as well as the capabilities of the suppliers. This judgment is supported by the risk management techniques illustrated in this Guide.

2.4 Science-Based Quality Risk Management

Quality Risk Management is a systematic process for the assessment, control, communication, and review of risks.

Application of Quality Risk Management enables effort to be focused on critical aspects of a computerized system, in a controlled and justified manner.

Quality Risk Management should be based on clear process understanding and potential impact on patient safety, product quality, and data integrity. For systems controlling or monitoring CPPs, these should be traceable to CQAs, and ultimately back to the relevant regulatory submissions for manufacturing systems.

Qualitative or quantitative techniques may be used to identify and manage risks. Controls are developed to reduce risks to an acceptable level. Implemented controls are monitored during operation to ensure ongoing effectiveness.

Process control systems often contain functionality which physically affects product quality, often in real-time. Some process control system functions may, in fact, be introduced specifically to mitigate particular product quality risks: e.g., automated inspection stages.

In addition, the manufacturing process may present risks in terms of safety, health, or environmental hazards. In such cases, activities such as HAZOPs can help to determine the risk. Although the focus for these activities may be different to the regulatory risk assessment, there is an opportunity to share information.

The flexible and configurable nature of many process control systems can have a potential impact upon the risk (e.g., compare custom ladder logic versus standard library sourced sequential function charts). Risk may increase with increasing novelty and complexity of the solution.

A practical quality risk management process for process control systems is introduced and described in Section 5 of this document.

2.5 Leveraging Supplier Involvement

Regulated companies should seek to maximize supplier involvement throughout the system life cycle in order to leverage knowledge, experience, and documentation, subject to satisfactory supplier assessment.

For example, the supplier may assist with requirements gathering, risk assessments, the creation of functional and other specifications, system configuration, testing, support, and maintenance.

Planning should determine how best to use supplier documentation, including existing test documentation, to avoid wasted effort and duplication. Justification for the use of supplier documentation should be provided by the satisfactory outcome of supplier assessments, which may include supplier audits.

Documentation should be assessed for suitability, accuracy, and completeness. There should be flexibility regarding acceptable format, structure, and documentation practices.

Typically, there may be many different suppliers, each with different levels of skill (as determined by the supplier's assessments), and each may need different support and controls to achieve the standards required for leveraging their documents and activities.

Considerations specific to process control systems include:

- the degree to which the process control system is packaged with the process equipment
- the complexity of the supply chain
- the modular nature of many process control systems

For a packaged system, a higher degree of expertise and knowledge of the process equipment (and, in some cases, of the process) may reside with the supplier rather than the regulated organization. Therefore, the supplier may already have details of process capability onto which the regulated company needs to map the required capability for the product.

Such suppliers typically have increased responsibility within the risk management process and more involvement in process validation as well as system verification activities. While overall responsibility lies with the regulated organization, the appropriate split of activities between supplier and regulated company needs to be considered at an early stage together with the appropriate level of supplier assessment.

Process control system equipment is often produced by one or more suppliers (each of whom may, in turn, base their offering on standard packages or firmware produced by their own sub-suppliers), and integrated and configured by another supplier. This needs to be taken into consideration when planning supplier assessment (does a supplier assess their own sub-suppliers adequately or is additional assessment required from the regulated organization) and when planning ongoing support for the system.

The modular nature of many process control systems, both in terms of hardware and the control application, facilitates the progressive acceptance of the system and the opportunity to make use of supplier test documentation.

3 Features Special to Process Control Systems

This Guide seeks to concentrate throughout on those features of the system life cycle that are in some way special to process control systems.

Specific features include:

- multiple components and multiple suppliers
- interfaces to a physical process being controlled in real time
- interfaces to (and degree of embedding with) the process equipment
- interfaces introduced by phasing of delivery

The following subsections provide an analysis of these features, what additional product or project risks may be introduced by these features, and which mitigation strategies may be appropriate.

The examples given are illustrative only, and are intended to be neither prescriptive nor exhaustive.

Where relevant, the mitigation strategies are cross referenced to appropriate appendices where approaches are discussed in greater detail. In addition, consideration is given to key system life cycle phases affected by each feature. Section 4 provides more detail on the system life cycle and its phases.

3.1 Multiple Components and Multiple Suppliers

Compared to other system types, process control systems are often made up from many more components of different types, often supplied by more than one supplier, requiring support and input from multidisciplinary teams. This leads to a large number of additional interfaces – both in terms of interfaces between components (communications links) and in terms of interfaces between different parties involved in producing the system.

There are also many different types of documents, potentially of many different formats. These may include:

- Process and Instrumentation Diagrams (P&IDs)
- Input/Output (I/O) Lists
- Control philosophy documents
- User Requirements Specification (URS)
- Functional Specification (FS)
- Electrical and wiring diagrams
- Process descriptions
- Instrumentation specifications
- Package specifications

Suppliers may define their design in many different ways including pseudo-code, flowcharts, matrices, natural language, or state transition diagrams.

Table 3.1: Example Risks Introduced by Multiple Components and Multiple Suppliers

Element	Risk Scenario	Example Mitigation
Multiple Components of Different Types	Effort wrongly focused leading to either insufficient effort or excessive effort on a specific item	Categorization of software and hardware feeding into risk management and validation planning
Multidisciplinary Input Required	Misunderstandings and gaps in communication	Careful communication planning and definition of scope, roles, interfaces, and points of contact
Multiple Suppliers	Lack of clarity about responsibilities – particularly for interfaces – leads to inadequate functionality in final system	Care in ensuring that planning documentation sets out scope and responsibilities correctly
Many different documents and document types	Lack of maintainability and consistency between documents Difficulty in ensuring a common understanding between all parties	Allow time to perform consistency checks across the documentation set Training in formats and methods for identified team members
Interfaces between components	Interface fails to function correctly	Make use of standard interfaces and protocols whenever available Ensure specifications cover interfaces in sufficient detail Ensure adequate testing of interfaces

Table 3.2: Life Cycle Activities Affected by Multiple Components and Multiple Suppliers

Life Cycle Phase	Items for Consideration
Concept	Consider how much can be achieved with standard items/how custom elements can be minimized
Project – Planning	Communication planning and ensuring a common understanding Categorization of software/hardware (including interfaces) as early in the project as possible (see Appendix E1 for an example) Maximizing the use of standard items in order to minimize validation effort (see Appendix E2 for an example) Split of plans by supplier – care with scope and responsibilities; extent to which supplier quality plan covers validation plan requirements
Project – Specification	Ensure specifications cover interfaces in sufficient detail Rigor of reviewing the design of custom software modules and interfaces Clear definition of acceptable project documentation conventions
Project – Configuration and Coding	Rigor of reviewing code relating to custom software modules and interfaces
Project – Verification	Method and rigor of verifying custom software modules and interfaces
Project – Reporting	How final quality and handover reports from separate suppliers interlink to the overall validation or other report
Ongoing Operation	How handover from multiple suppliers will be managed How support services will be set up for all suppliers How changes will be managed when many parties may be involved How disaster recovery will be managed when many parties may be involved and there may be dependencies of one system component on another How records will be retained/archived/retrieved in a way that keeps records from different components correctly synchronized How upgrade or patching of one component affects the remaining parts of the system (see Appendix E8 for further detail)
Retirement	How retirement/replacement of one component affects the remaining parts of the system (see Appendix E9 for further detail) How data from multiple sources can be retained in readable form after retirement (see Appendix E9 for further detail)

3.2 Interfaces to a Physical Process

Process control systems differ from other computerized systems in that they may physically affect or measure the process, often in real-time. Therefore, they may have potentially high impact on product quality.

Table 3.3: Example Risks Introduced by Interfaces to a Physical Process

Element	Risk Scenario	Example Mitigation
Process Measurement Elements	System fails to measure critical parameters correctly resulting in poor control or possibly release of poor quality product	Risk assessment of scenarios that might affect critical measurements Mitigation of the effects may include independent measurements, calibration and maintenance routines, interlocks or alarms.
Process Control Elements	System fails to control critical parameters resulting in poor quality product	Risk assessment of scenarios that might affect critical control functions Mitigation of the effects may include verification of control strategies, creation of independent checking functions, interlocks, or alarms.
Failure of System Element	System malfunction or poor performance affects quality of product and/or leads to loss of data	Risk assessment to include failure of individual system elements Mitigation of the effects may include redundant components, interlocks or alarms, disaster recovery procedures, preventive maintenance requirements.
Process Fluctuation	Change in environmental or process input conditions moves system outside its ability to produce good quality product	Risk assessment of scenarios that might take critical parameters outside the limits for good quality product Mitigation of the effects may include process or equipment design features, additional controls on process inputs, interlocks or alarms.
Process Knowledge	May not know required process capability (e.g., if this is a multi-purpose facility)	Design facility with specified capability against which new processes can be assessed to determine suitability

Table 3.4: Life Cycle Activities Affected by Interfaces to a Physical Process

Life Cycle Phase	Items for Consideration
Concept	Approach may differ if Process Analytical Technology (PAT) is applied (see Special Appendix S1)
Project – Planning	Initial assessment and determination of system impact (Risk Assessment step 1, see example in Appendix E3)
Project – Specification	Identifying functions with impact on patient safety, product quality and data integrity, and performing functional risk assessments to identify required controls (Risk Assessment steps 2 and 3, see example in Appendix E3) Traceability of critical parameters within specifications (see example in Appendix E4) Use of ANSI/ISA-88 in structure of specifications (see Special Appendix S3)
Project – Configuration and Coding	Implementing appropriate controls of identified risks (Risk Assessment step 4, see example in Appendix E3)
Project – Verification	Verifying appropriate controls of identified risks (Risk Assessment step 4, see example in Appendix E3)
Project – Reporting	Reviewing risks and monitoring controls (Risk Assessment step 5, see example in Appendix E3)
Ongoing Operation	How changes to the system will be managed to avoid impacting the integrity of the process How upgrade or patching of the system will be managed to avoid impacting the integrity of the process (see Appendix E8 for further detail)
Retirement	Whether there are any links to/from other systems that might affect the process when one is removed (see Appendix E9 for further detail)

3.3 Interfaces with Process Equipment

Process control systems differ from other system types because they need to interface to the process equipment. The control system can be embedded within the equipment, and the degree of embedding will depend on the type of system being considered.

Table 3.5: Example Risks Introduced by Interfaces with Process Equipment

Element	Risk Scenario	Example Mitigation
Supplier/ Regulated Company Interface	Much more of the process expertise resides with the supplier who may be unfamiliar with working in a GxP environment.	Supplier assessment process Planning process needs to be clear about the split of responsibilities between regulated company and supplier. Joint risk assessment process by regulated company and supplier

Table 3.6: Life Cycle Activities Affected by Interfaces with Process Equipment

Life Cycle Phase	Items for Consideration
Concept	Consider existing solutions with control system already embedded with the process equipment.
Project – Planning	Supplier assessment process should take account of the extent to which process and equipment knowledge resides with the supplier (see example in Appendix E5). Care is needed in determining the split of responsibilities between regulated company and supplier (and ensuring that all required activities are covered between the regulated company validation plans and the supplier quality plan).
Project – Specification	Supplier involvement in the detailed risk assessment steps will need to reflect the extent to which process and equipment knowledge resides with the supplier. For a control system that is packaged with process equipment and sold as a standard product, regulated company documentation sets may need to reference product life cycle documentation maintained by the supplier. Documentation deliverable lists should set out where copies of such documents are required by the regulated company and where their existence and quality is just confirmed as part of the supplier assessment process.
Project – Configuration and Coding	Depending on the degree to which the control system is embedded with the process hardware, coding standards and coding expertise may reside entirely with the supplier (or possibly a sub-supplier). In this case, the rigor of coding standards and code reviewing may need particular attention during supplier assessment. The degree to which the control system is part of a standard product will determine the split of configuration management activities between the supplier's product life cycle and the process control system life cycle.
Project – Verification	The degree to which the control system is part of a standard product will determine the split of verification activities between the supplier's product life cycle and the process control system life cycle (see example in Appendix E6). As with the specification activities, the validation planning process should set out where copies of validation results are required by the regulated company and where their existence and quality is just confirmed as part of the supplier assessment process.
Project – Reporting	Just as for the planning phase, care is needed in ensuring that reporting of all activities is covered between the regulated company validation reports and the supplier quality report.
Ongoing Operation	Where the control system is embedded with process equipment, a single support contract is likely to cover both. Where control systems are provided by a sub-supplier to the supplier, it is important to ensure that suitable support for ongoing operation is available.
Retirement	Where the control system is embedded with process equipment, it is likely that both will be retired together thus minimizing risk to the process. If the control system is to be replaced, process expertise from the original equipment supplier is likely to be needed.

3.4 Phased Delivery

Large process control systems are often delivered in phases – either horizontally (with I/O and control module layers followed by equipment modules, sequencing and batch control) or vertically (with one plant area followed by another). This process introduces additional interfaces that need to be considered at all times between the operational areas of the overall system and those under development.

There should be a clear understanding of what does and does not constitute a change during phased delivery. For example, the tuning of equipment or the timing of an interface by an SME during installation may not be subject to formal change control unless this impacts previously delivered elements or critical aspects. Responsibilities for managing changes across phases should be defined. Particular consideration should be given to the impact of changes on the phased delivery, such as the possible need for data migration.

Table 3.7: Example Risks Introduced by Phased Delivery

Element	Risk Scenario	Example Mitigation
Installation of second and subsequent phases	Second or subsequent phase identifies problem with an element that is already installed in a prior phase.	Change management strategy for how such changes will be back-tracked into existing elements. Documentation split and versioning needs to allow for such changes. Configuration management system needs to allow for such changes.
Installation of second and subsequent phases	Installation of new elements has negative impact on those already present.	Configuration management strategy may involve use of standard (or pre-tested) export/import methods to minimize impact on existing configurations. Verification strategy may involve making changes to a test environment and verifying the change process as well as the end result. Verification strategy may need to include significant elements of regression testing.

Table 3.8: Life Cycle Activities Affected by Phased Delivery

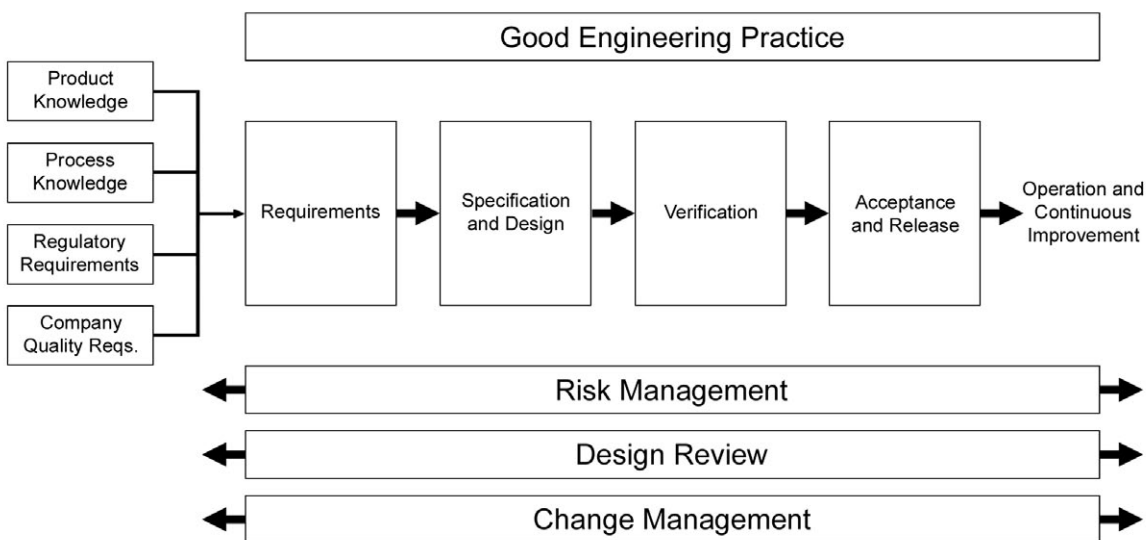
Life Cycle Phase	Items for Consideration
Concept	Early consideration needs to be given to how the installation will be phased.
Project – Planning	Planning will need to set out in detail how the phased delivery will be managed.
Project – Specification	Documentation structure and versioning needs to allow for changes if a second or subsequent phase identifies problem with an element that is already installed in a prior phase. Interfaces between phases will need special attention in the specification documents.
Project – Configuration and Coding	Configuration management system needs to allow for changes if a second or subsequent phase identifies problem with an element that is already installed in a prior phase. Configuration management strategy may need to involve use of standard (or pre-tested) export/import methods to minimize impact on existing configurations.
Project – Verification	Verification strategy may involve making changes to a test environment and verifying the change process as well as the end result. Verification strategy may need to include significant elements of regression testing.
Project – Reporting	Reporting strategy will need to address how handover of each phase will be managed.
Ongoing Operation	Care will be needed in determining: How handover of each phase will be managed. How changes will be managed during the period where part of the system is active and part still under development.
Retirement	There are no additional risks in retirement unless the retirement is also taking place in a phased fashion – in which case change control and the impact on interfaces between phases will need special attention in the retirement planning.

4 Process Control System Life Cycle Overview

Compliance with regulatory requirements and fitness for intended use may be achieved by adopting a life cycle approach following good practice as defined in this Guide.

A life cycle approach entails defining and performing activities in a systematic way from conception, understanding the requirements, through development, release, and operational use, to system retirement. Figure 4.1 shows a general specification, design, and verification process described in ASTM E2500-07 (Reference 17, Appendix 13).

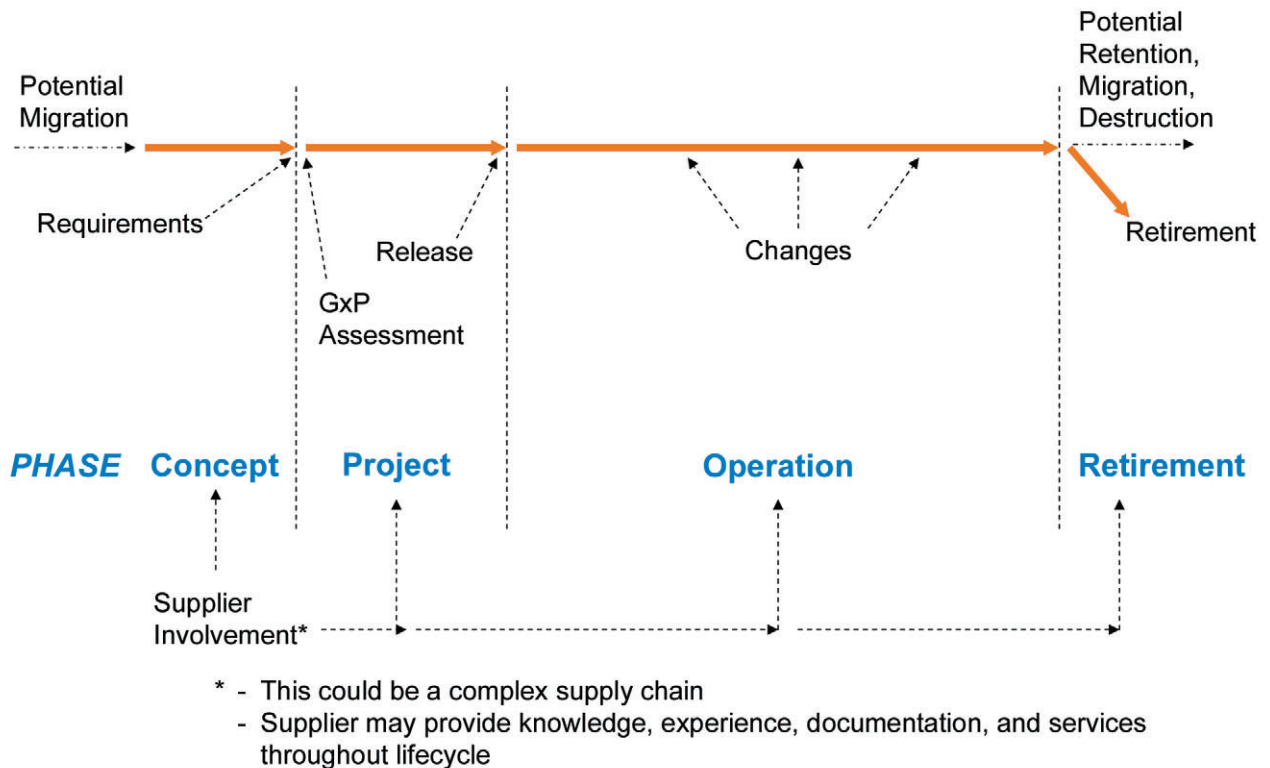
Figure 4.1: The Specification, Design, and Verification Process



Reprinted with permission from ASTM E2500-07 Standard Guide for Specification, Design, and Verification of Pharmaceutical and Biopharmaceutical Manufacturing Systems and Equipment, copyright ASTM International, 100 Barr Harbor Dr., West Conshohocken, PA 19428. A copy of the complete standard may be obtained from ASTM at www.astm.org.

For a specific process control system, the life cycle should encompass all activities from initial concept to retirement, as shown in the following figure.

Figure 4.2: GAMP 5 Life Cycle



During the concept phase, the regulated company is considering opportunities to automate one or more business processes based upon business need and benefits. Typically at this phase, initial requirements will be developed and potential solutions considered. From an initial understanding of scope, costs, and benefits, a decision is made on whether to proceed to the project phase. This phase is sometimes referred to as analysis.

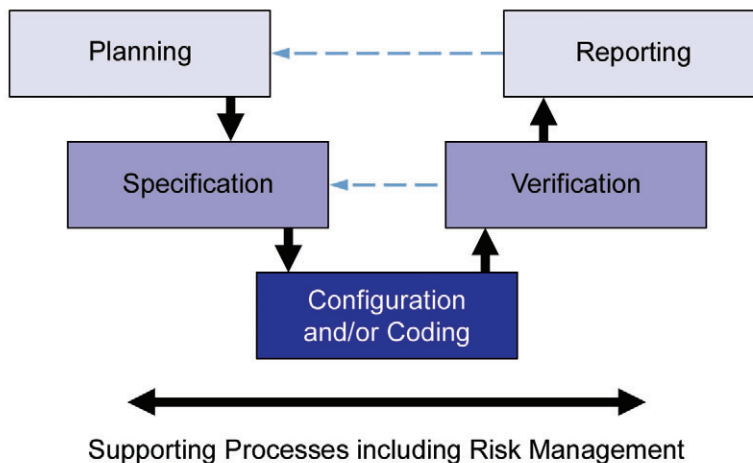
The project phase involves planning, supplier assessment and selection, various levels of specification, configuration (or coding for custom developments), and verification leading to acceptance and release for operation. Risk management is used as a tool to identify risks and to remove or reduce them to an acceptable level.

System operation is typically the longest phase and is managed by the use of defined, up to date, operational procedures applied by personnel who have appropriate training, education, and experience. An important consideration during operation of GxP regulated systems is maintaining control (including security), fitness for intended use, and compliance. The management of changes of different impact, scope, and complexity is a key activity during this phase.

The final phase is the ultimate retirement of the system. It involves decisions about data retention, migration, or destruction and the management of these processes.

Figure 4.3 shows a general approach for achieving computerized system compliance and fitness for intended use within the process control system life cycle.

Figure 4.3: Specification and Verification Approach



The application of this general approach within the life cycle will vary widely depending on the risk, complexity, and novelty of the system.

Note that the regulated company computer system life cycle fits alongside the life cycle of the process and process equipment. Where a computer system is regarded as one component of a wider manufacturing process or system, particularly in an integrated QbD environment, specific and separate computerized system validation may not be necessary. This environment requires both complete product and process understanding and that the critical process parameters can be accurately and reliably predicted and controlled over the design space. In such a case, the fitness for intended use of the computer system within the process may be adequately demonstrated by documented engineering or project activities together with subsequent Process Validation or continuous quality verification of the overall process or system. For automated manufacturing equipment, separate computer system validation should be avoided. Computer system specification and verification should be part of an integrated engineering approach to ensure compliance and fitness for intended use of the complete automated equipment.

4.1 Roles and Responsibilities

This section describes key roles and responsibilities when achieving compliance. Designated individuals should have sufficient experience and training to perform their respective roles. Specific activities may be delegated to appropriate nominated representatives.

Process Owner

The owner of the business process or processes being managed should be identified. The process owner is ultimately responsible for ensuring that the computerized system and its operation is in compliance and fit for intended use in accordance with applicable SOPs. The process owner also may be the system owner.

System Owner

The System Owner is responsible for the availability, and support and maintenance, of a system and for the security of the data residing on that system. The system owner is responsible for ensuring that the computerized system is supported and maintained in accordance with applicable SOPs. The system owner also may be the process owner.

Quality Unit

The term Quality Unit is used here as an encompassing term that includes many quality-related roles that are important to developing and managing regulated computerized systems. The manner in which a Quality Unit addresses the responsibilities noted below may vary based on the applicable regulations. The Quality Unit has a key role to play in successfully planning and managing the compliance and fitness for intended use of computerized systems, and provides an independent role in the:

- approval or audit of key documentation such as policies, procedures, acceptance criteria, plans, reports
- focus on quality critical aspects
- involvement of SMEs
- approval of changes that potentially affect patient safety, product quality, or data integrity
- audit processes and supporting documentary evidence to verify that compliance activities are effective

Subject Matter Expert

Qualified and experienced SMEs have a key role in performing reviews and assessments, and taking technical decisions, based on science-based process and product understanding, and sound engineering principles. Different SMEs may be involved with different activities, e.g., during specification and verification.

SMEs should take the lead role in the verification of the computerized system. Responsibilities include planning and defining verification strategies, defining acceptance criteria, selection of appropriate test methods, execution of verification tests, and reviewing results.

4.2 Process Control System Supplier Life Cycles

A typical regulated company application does not develop completely custom process control system components, but rather seeks to use standard software and hardware elements wherever possible.

These individual components also have their own life cycle, in this case controlled by the supplier. The life cycle for a system component (product from the supplier) encompasses all activities from initial concept to obsolescence.

During the product concept phase, the supplier company is considering opportunities to create and market a standard solution. Typically at this phase, initial requirements will be developed and potential solutions considered. From an initial understanding of scope, costs, and benefits, a decision is made on whether to proceed to the development phase.

The product development phase involves planning, specification, configuration and coding and verification leading to acceptance and release of the product.

This Guide does not constrain the choice of supplier development methods and models. Suppliers should use the most appropriate methods and models for their needs, which may include RAD or prototyping, or other techniques.

During the lifetime of the product, releases to introduce new functionality or to correct defects each have their own mini-life cycle. A product release also may prompt an upgrade to existing systems and therefore have impact on the regulated company system life cycle.

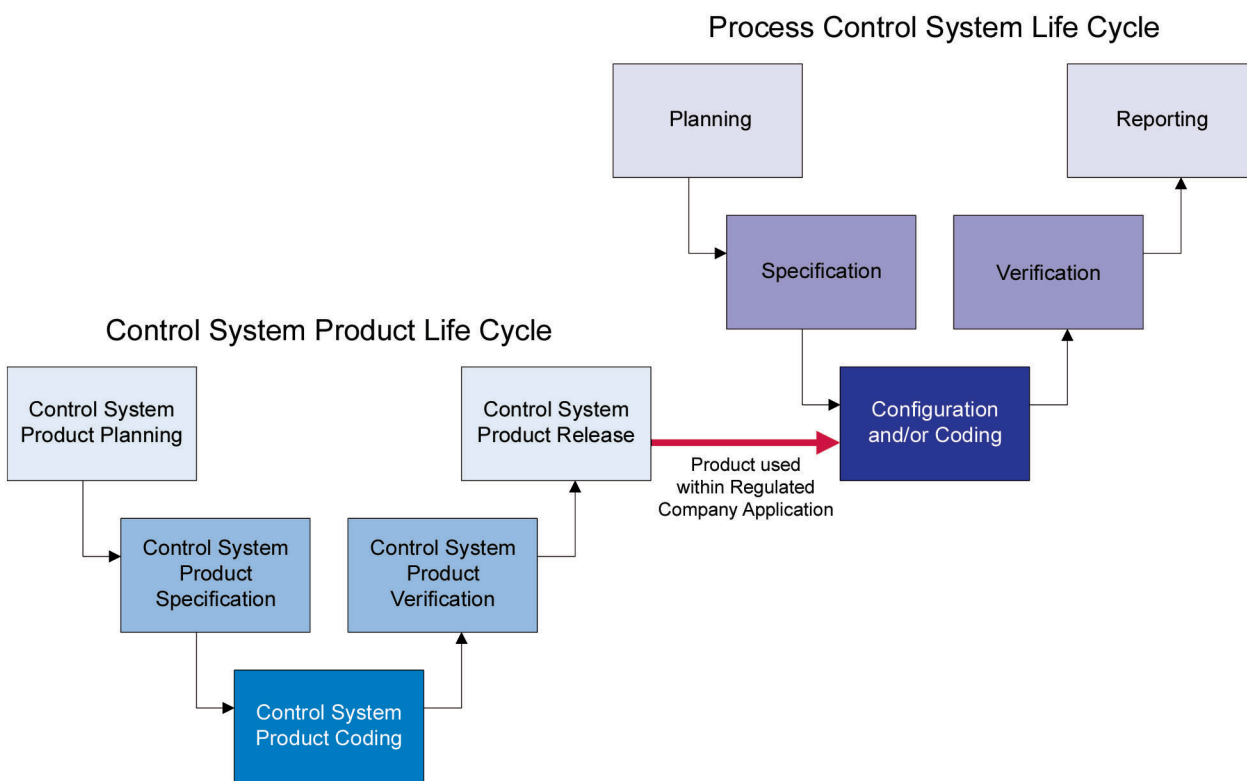
The final phase of product obsolescence involves decisions about support for the installed base and potential migration paths to newer product

4.3 Leveraging Supplier Effort

The overall life cycle approach for the process control system needs to take into account the range of components and suppliers used and seek to minimize duplication of activities within the life cycles applied by each party.

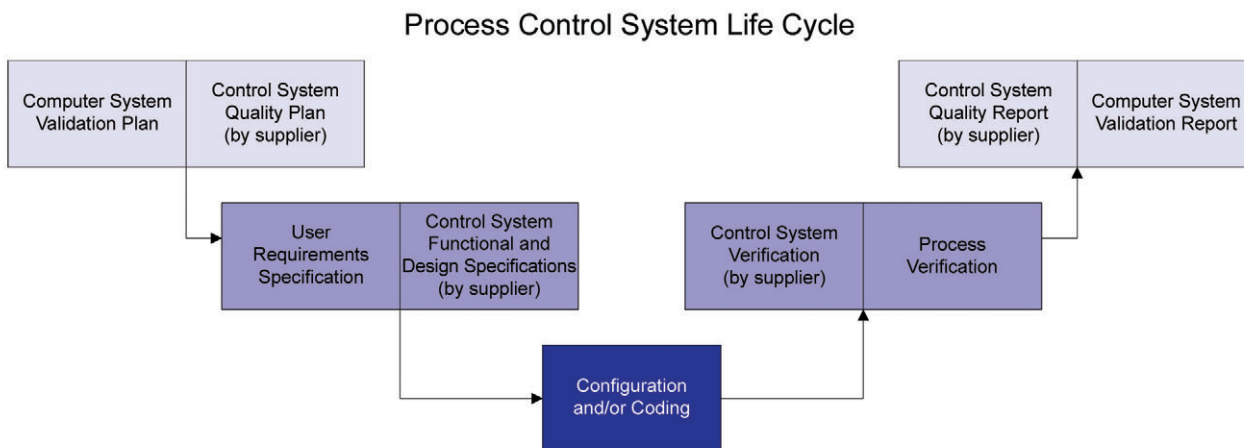
Although all software (including standard packages and instrument firmware) will originally have been developed as custom code by a supplier, where that supplier has been suitably assessed, the regulated company may benefit by leveraging activities already carried out as part of the product development life cycle. This can reduce the activities required as part of the regulated company system life cycle. The categorization process described in Section 4.4 of this Guide can help ensure that supplier activities are appropriately leveraged.

Figure 4.4: Leveraging Work already done in the Supplier's Product Life Cycle



A regulated company also can seek to benefit from supplier activities carried out within the system life cycle, e.g., by leveraging supplier documentation produced during the life cycle as illustrated in Figure 4.5.

Figure 4.5: Leveraging Supplier Work during the System Life Cycle



4.4 Leveraging Supplier Effort for Different Types of Control Systems

The main differences between the life cycles of packaged and non packaged control systems result from the extent to which knowledge of the process and process equipment reside with the supplier and the regulated organization.

For a system where the process controls are not packaged with the process equipment, the regulated company and supplier activities need to interleave to allow transfer of knowledge about the required control strategy for the process and equipment from the regulated company to the control system supplier.

Figure 4.6 shows example life cycle activities for a custom coded system (e.g., a large DCS system) where controls are not packaged with the process equipment.

Figure 4.6: Example Life Cycle Activities: Custom Coded System – Not Packaged

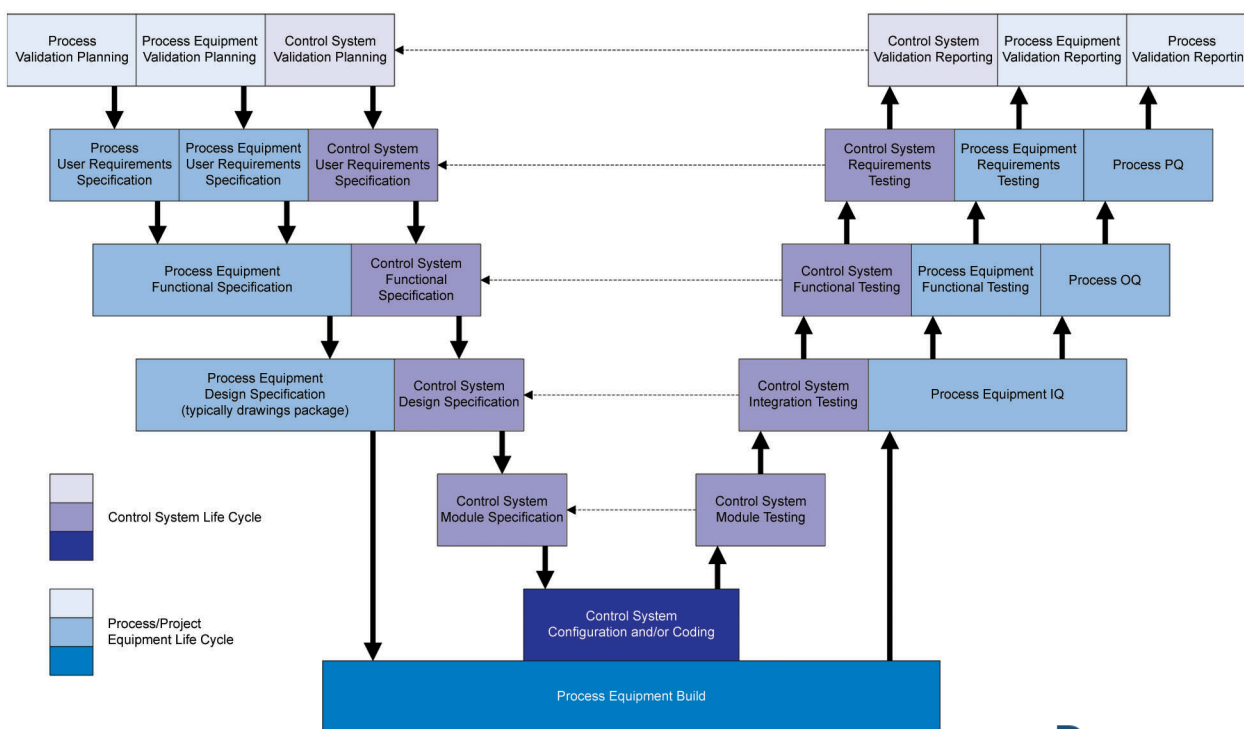
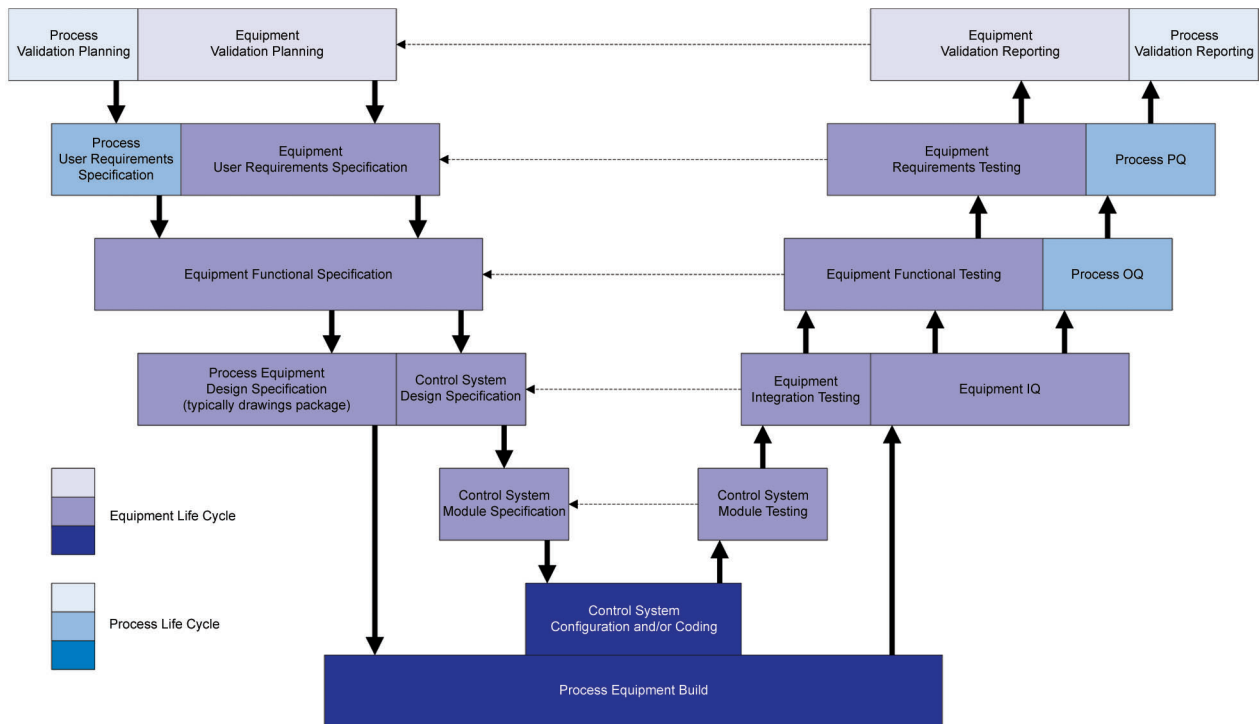


Figure 4.7 shows example life cycle activities for a custom coded system (e.g., a one-off piece of equipment) where controls are packaged with the process equipment.

Figure 4.7: Example Life Cycle Activities: Custom Coded System – Packaged With Process Equipment



Categorization of software and hardware can assist in scaling life cycle activities appropriately.

The examples given are illustrative only, and are intended to be neither prescriptive nor exhaustive.

For further guidance on categorizing software elements within a system, see Appendix E1.

Figure 4.8: Illustrative Examples of Software Categories

Category	Description	Range of Applications	Typical Examples
5 Custom Software	Software custom designed and coded to suit the business process.	Complex application, coding language requires consideration of program level decisions/timing/looping as well as process level decisions/timing/looping. Increasing complexity of code	VB or C++ Application
		Simple application, coding language needs programmer to define only process decisions/timing. Control of scanning inputs, performing actions, looping, etc. is by the underlying system.	DCS or SCADA Scripting
4 Configured Software	Software (often very complex) which can be configured by the user to meet the specific needs of the user's business process. Software code is not altered.	Library functions selected, parameterized, and connected with branches and decisions. Increasing complexity of configuration	IEC61131-3 IL or ST Application
		Library functions selected, parameterized, and connected in linear fashion.	IEC61131-3 LD or SFC Application
3 Non-Configured Software	Runtime parameters may be entered and stored but the software cannot be configured to suit the business process.	Standard item needs a large parameter file loading before it will work. Increasing complexity of parameterization	IEC61131-3 FBD Application
		Standard item with no parameterization (works 'out of the box').	DCS/SCADA Databases
1 Infrastructure Software	Software used to manage the operating environment. Layered software upon which applications are built.	Refer to GAMP 5 and the GAMP Good Practice Guide: IT Infrastructure Control and Compliance for further details	DCS/SCADA Mimics (standard icons)
			Electronic Chart Recorder
			PID Controller
			Smart Transmitter
			Version Control Tools
			Programming Languages
			Underlying Operating System

Figure 4.9: Illustrative Examples of Hardware Categories

Category	Description	Range of Applications	Typical Examples
2 Custom Built Hardware Components	Bespoke software components designed specifically for the application.	↑ Complex bespoke item – typically defined by a large set of drawings and/or a design specification. Increasing complexity of functionality Simple bespoke item – typically defined by a single drawing.	Safety Shutdown Relay System Control Cubicle Control Loop
1 Standard Hardware Components	Standard hardware components bought 'off the shelf' using a standard order code from the supplier and covered by manufacturer's specification details.	↑ Complex standard item – typically requires many elements specifying within order code. Increasing complexity of functionality Simple standard item – single element order code	PLC Control System I/O Module PT100 Temperature Sensor

Examples have been chosen which might be part of the process control system itself. For packaged systems where validation of process, process hardware, and control system are being performed together, a similar approach may be needed for the process equipment.

5 Quality Risk Management

Section 2 of this Guide introduced the concept of quality risk management as part of the life cycle approach. This section gives more detail on this topic.

This section is primarily aimed at a life cycle approach to new systems, and does not imply that formal risk assessments are required for all existing systems. The extent of risk management required for existing systems, including the need for formal risk assessments, should be considered as part of periodic review and when changes are required to the existing system.

Organizations may have established risk management processes, including the use of methods such as those listed in GAMP 5 Appendix M3 (Reference 15, Appendix 13). While this Guide describes one suggested approach, it does not intend or imply that these methods should be discarded, rather that they continue to be used, as appropriate, within the context of an overall quality risk management framework consistent with ICH Q9, and taking into account ICH Q8 (R2) and Q10 (References 2, 1, and 3, Appendix 13).

Further examples of application of quality risk management approaches are given in Appendix E3.

5.1 ICH Q10 Pharmaceutical Quality System

ICH Harmonised Tripartite Guideline Q10 (Reference 3, Appendix 13) describes a model for an effective quality management system for the pharmaceutical industry.

Within this model, quality risk management is seen as one of the enablers for successful implementation.

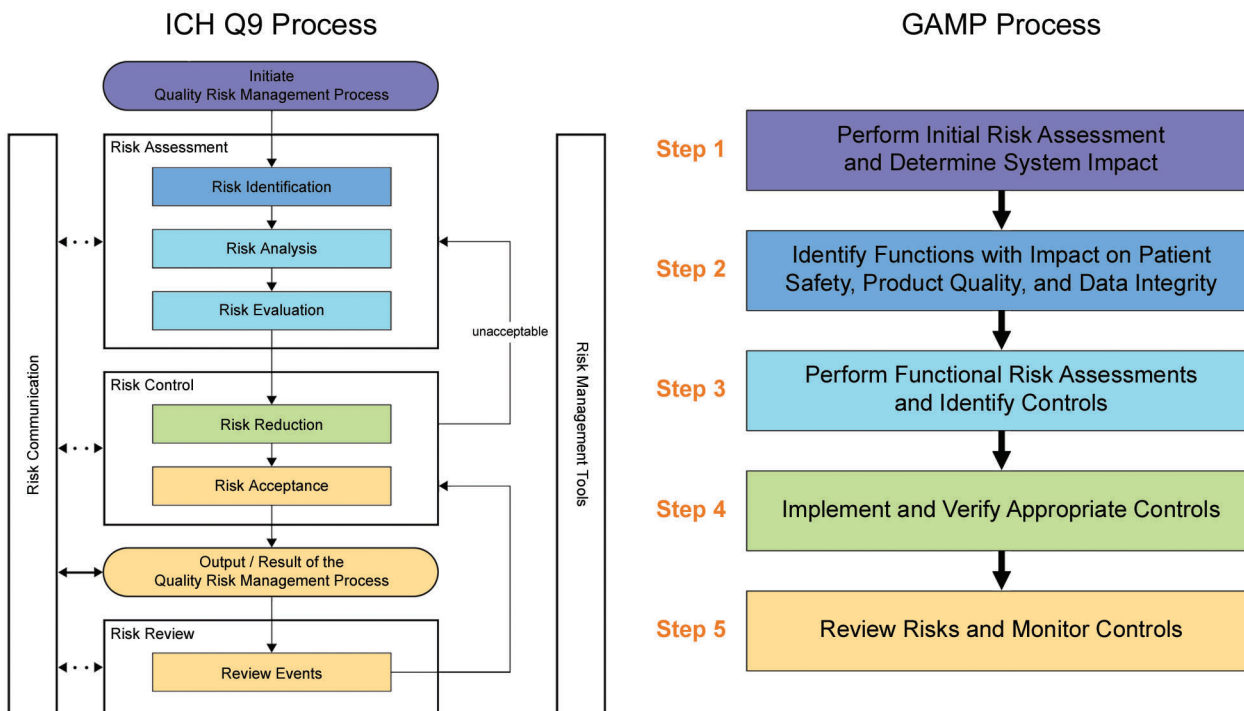
5.2 ICH Q9 Quality Risk Management

ICH Harmonised Tripartite Guideline Q9 (Reference 2, Appendix 13) describes a systematic approach to quality risk management intended for general application within the pharmaceutical industry. It defines two primary principles of quality risk management:

- The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the protection of the patient
- The level of effort, formality, and documentation of the quality risk management process should be commensurate with the level of risk.

Figure 5.1 shows how this Guide applies the general principles of ICH Q9 to describe a five-step process for risk management as an integral part of achieving and maintaining system compliance.

Figure 5.1: Application of ICH Q9



Step 1 – Perform Initial Risk Assessment and Determine System Impact (based on an understanding of product and process understanding).

Step 2 – Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity.

Step 3 – Perform Functional Risk Assessments and Identify Controls (considering possible hazards, and how the potential harm arising from these hazards may be controlled).

Step 4 – Implement and Verify Appropriate Controls (to ensure that they have been successfully implemented and traced to the relevant identified risks).

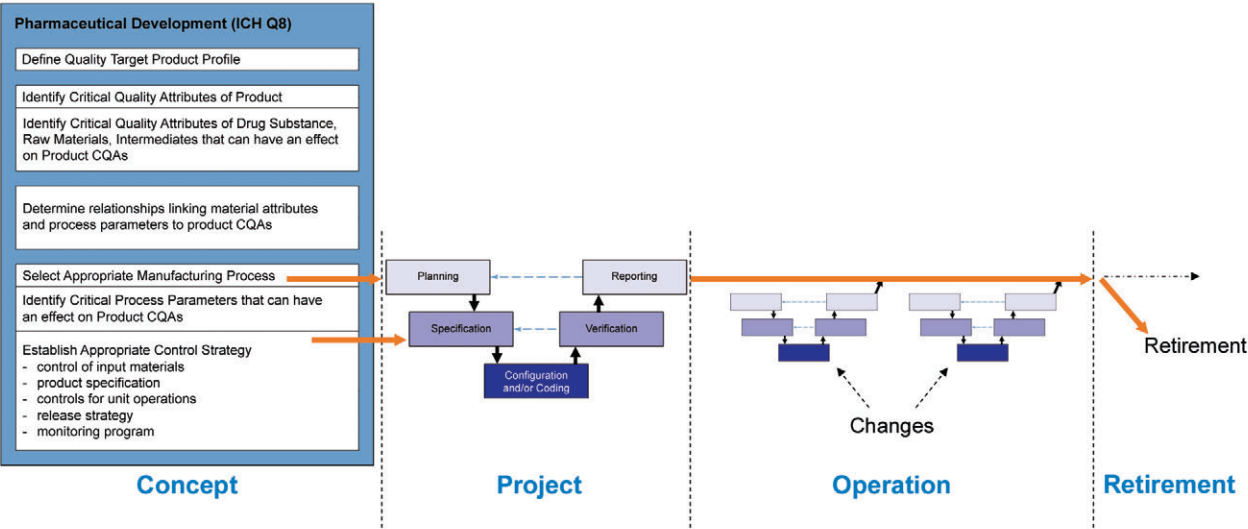
Step 5 – Review Risks and Monitor Controls (to confirm that residual risks are acceptable and verify that controls are still effective)

5.3 ICH Q8 Pharmaceutical Development

For process control systems, there are a physical process and equipment being controlled in real time. As a result, process control systems could be controlling parameters or attributes which can have a high impact on product quality. Therefore, it is important that output from the pharmaceutical development process (in terms of the process and product understanding underlying the proposed control strategy) feed through into process control system risk management. It is also important that the focus is not solely on equipment capability, but takes into account aspects introduced by computerization, such as electronic data, record storage, and security.

Figure 5.2 shows how the process control system life cycle links to the pharmaceutical development process as described in ICH Harmonised Tripartite Guideline Q8 (R2) (Reference 1, Appendix 13).

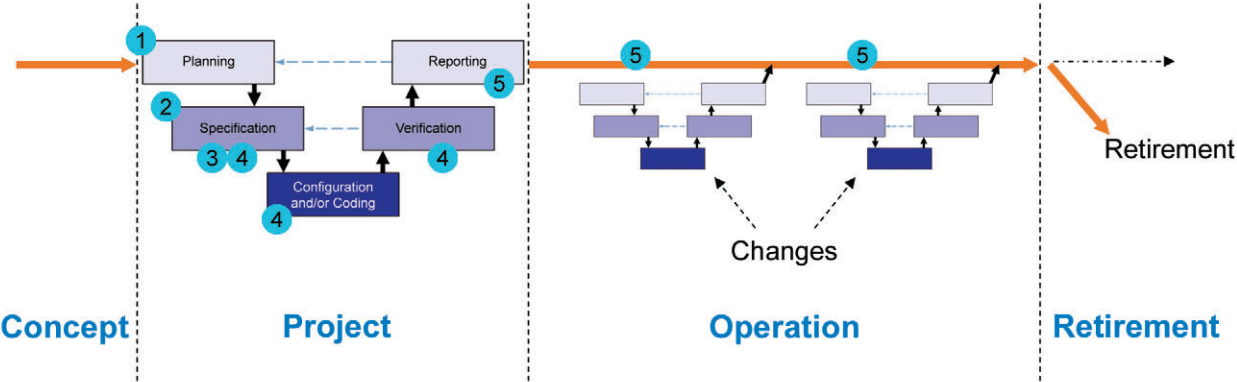
Figure 5.2: Relationship of ICH Q8 to the System Life Cycle



5.4 Risk Management in the Life Cycle

For a process control system, risk management activities are typically performed throughout the life cycle.

Figure 5.3: Typical Risk Management Activities within the Life Cycle



The risk management steps introduced in Section 5.2 can be performed at various points during the life cycle. The following table shows typical inputs and outputs at each step.

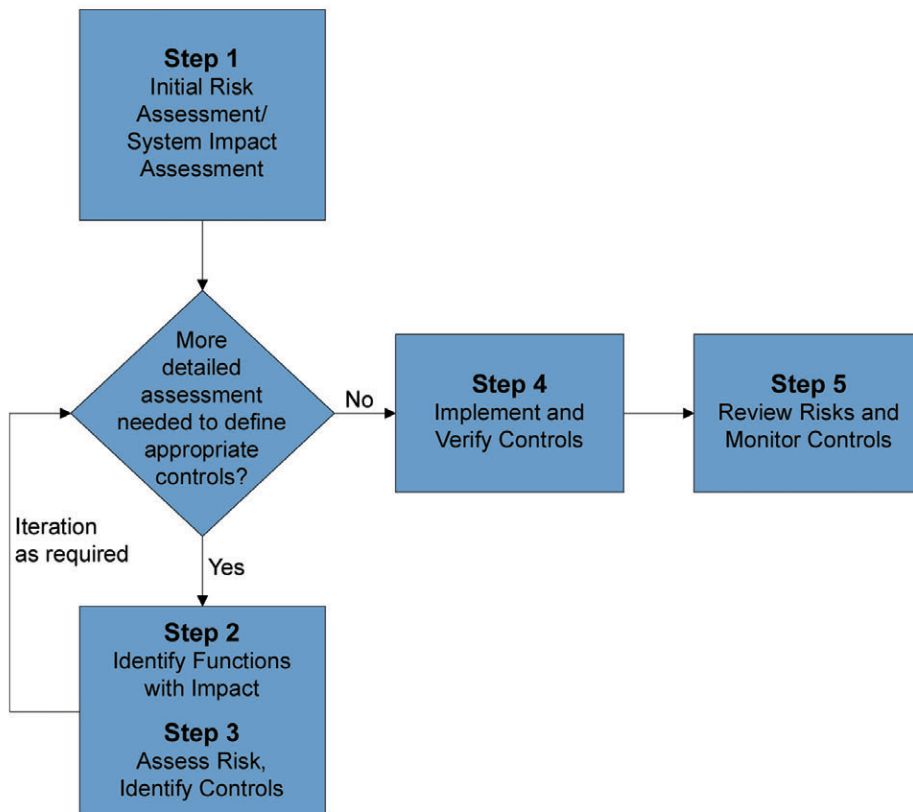
Table 5.1: Typical Inputs and Outputs at Each Risk Management Step

Step	Quality Risk Management Activity	Inputs	Output
S 1	<i>Perform Initial Risk Assessment and Determine System Impact</i>	Proposed manufacturing process and information about critical parameters from pharmaceutical development process	High level system GxP status and impact assessment Planning for appropriate scaling of risk management and project activities
S 2	<i>Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity</i>	Proposed control strategy from pharmaceutical development process	Risk scenarios and potential impact associated with each function
S 3	<i>Perform Functional Risk Assessments and Identify Controls</i>	Design specifications of appropriate level to allow assessment of risk likelihood/probability of detection	Functions assessed for overall risk Necessary controls identified
S 4	<i>Implement and Verify Appropriate Controls</i>	Controls identified by risk assessment	Necessary controls implemented Risk-based scaling during specification, implementation, and test planning
S 5	<i>Review Risks and Monitor Controls</i>	Risk assessment Test results and other evidence of controls Performance review during ongoing operation Data migration/retention requirements	Acceptance of residual risks or iteration to implement additional controls Risk-based decisions during planning of operational activities Risk-based decisions during change control (may require Steps 2, 3, 4 to be revisited) Risk-based decisions when planning system retirement.

5.5 Scalability of Risk Management

At each of risk management steps 1, 2, 3, the decision may be taken to scale the remaining assessment steps based on the output of the current step. This results in a cascading process as follows:

Figure 5.4: Iterative Risk Assessment Process



So, for a complex, higher impact process control system, the iterations might produce the following outputs:

- initial risk assessment
- impact assessment based on functions listed in URS (allowing definition of appropriate controls for some lower impact functions)
- functional risk assessment based on information in Functional Specification including level of customization and complexity of the proposed solution
- possible further iterations of more detailed functional risk assessment for higher risk functions only; based on information in Design or Configurations Specifications

For a simpler, lower impact system the iterations might produce the following outputs:

- initial risk assessment
- impact assessment based on functions listed in URS (allowing definition of appropriate controls for the whole system)

5.6 Step 1 – Initial Assessment and Determination of System Impact

At this stage, little detail may be known about the process hardware or the control system. Furthermore, there may be multiple process control systems supporting a business process. However, it is necessary to be aware of the Quality Target Product Profile (QTPP), proposed manufacturing process, Critical Quality Attributes (CQAs), and Critical Process Parameters (CPPs) from the pharmaceutical development process.

Some types of business processes have a higher impact on product quality than others, and system risk assessment should take into account the processes that the system supports. Systems that support critical processes include those that:

1. generate, manipulate, or control data supporting regulatory safety and efficacy submission
2. **control critical parameters and data in preclinical, clinical, development, or manufacturing**
3. **control or provide data or information for product release**
4. **control data or information required in case of product recall**
5. control adverse event or complaint recording or reporting
6. support pharmacovigilance

Those highlighted in **bold** above are more likely to be applicable to process control systems:

The system impact assessment is based on the potential of the control system to affect product quality, patient safety, or regulated data and records. It should ideally correlate to the CPPs and/or CQAs associated with the business process. A system cannot have a higher impact than the process it supports.

The output of this step is used to assist with:

- scaling of the system life cycle
- scaling of the risk management activities
- judgment of whether the system is GxP regulated

5.7 Step 2 – Identify Functions with Impact

This step involves identifying functions with impact on patient safety, product quality, and data integrity.

At this stage, little may still be known about the system hardware or software design. However, there should be access to the User Requirement Specification defining those functions from the control strategy that is applicable to the specific system.

For each function within the User Requirement Specification, risk scenarios are identified and the impact assessment is based on the potential of that function to affect product quality. A process control system function inherits its impact from the process (e.g., “What is the worst thing that could happen if this function was not carried out correctly?”) and not vice-versa. An example is shown in Table 5.2.

Table 5.2: Example Impact of a Process Control System Function

Function	Risk Scenario	Worst case harm	Impact Rating
Dispensing of reagent onto test strip	Reagent volume wrong	Test strip returns erroneous result	High

Sometimes, a function may support multiple CQAs (e.g., an interface allowing several pieces of data to be transferred between systems). In this case, its impact rating should reflect the highest impact of any of the supported CQAs.

This step provides greater clarity on the extent, rigor, and focus of any further risk management activities. It also helps with establishing the appropriate level of subsequent specification and verification activities required, including for those functions identified as not having GxP impact.

The list of impact ratings forms the starting point for risk assessment in Step 3.

5.8 Step 3 – Perform Functional Risk Assessments and Identify Controls

This step involves performing functional risk assessments and identifying the controls required to reduce risks to an acceptable level.

At this stage, there should be access to system design specifications at an appropriate level to allow necessary controls to be identified (note that the process may be iterative with an initial assessment against the Functional Specification highlighting that a further, more detailed, assessment against the detailed design specifications is required for certain higher impact functions). It may be possible to identify suitable controls without further detailed analysis.

If it is necessary to perform a detailed assessment, a risk assessment process should be applied. This should be based on identifying possible scenarios and hazards associated with the function then combining impact, likelihood, and probability of detection to generate overall risk priority levels and identify appropriate controls. If a HAZOP has been performed on the process, some functions may be Safety Integrity Level (SIL) rated, and this higher integrity should be taken into account during the risk assessment. Understanding how a failure may propagate or cascade to and from integrated systems and equipment may need to be considered. For further information on general risk assessment tools, see ICH Q9 Annex I: Risk Management Methods and Tools (Reference 2, Appendix 13).

- **Impact** for a hazard/scenario is identified as in step 2 (What is the worst case result of this scenario?).
- **Likelihood** for a hazard/scenario may involve a combination of process knowledge (How often does this type of process problem arise?) and system knowledge (How often does this type of hardware/software/manual control fail?).
- **Probability of Detection** for a hazard/scenario may involve a combination of process knowledge (Will this definitely be detected by some independent downstream check?) and system knowledge (How reliable is this type of hardware/software/manual fault detection?).

When assessing risk for process control systems, there will be some scenarios where the potential harm results from a process problem (which the control system function is intended to mitigate) and some where it results directly from a system problem. Sometimes, a function is introduced in order to mitigate the risk of failure of another function.

This should be considered in advance when drawing up guidelines for assessing likelihood and probability of detection and the team performing the risk assessment should be clear over whether they are assessing the process alone (treating the system as providing new controls to mitigate the identified risks) or the process **plus** system (treating the system as an existing control). Table 5.3 shows an example of the same scenario assessed both ways.

Table 5.3: Example Functional Risk Assessment

Scenario	Existing Controls (assessing “process” alone)	Impact	Likelihood	Probability of Detection	Risk Priority	Proposed Solution Required	Impact	Revised Likelihood	Revised Probability of Detection	Revised Risk Priority
Blocked dispensing nozzle results in insufficient reagent dispensed	None	H	H	L	H	Additional automated inspection step to check liquid level in well on test strip Functional testing of inspection step	H	H	H	M

Scenario	Existing Controls (assessing “process + system” together)	Impact	Likelihood	Probability of Detection	Risk Priority	Additional Controls Required	Impact	Revised Likelihood	Revised Probability of Detection	Revised Risk Priority
Blocked dispensing nozzle results in insufficient reagent dispensed	Inspection step automatically checks liquid level in well on test strip	H	H	M	H	Functional testing of inspection step	H	H	H	M

The output of this step is a list of required controls which may include:

- modification of process design or system design
- application of external procedures
- increasing the detail or formality of specifications
- increasing the number and level of detail of design reviews
- increasing the extent or rigor of verification activities

5.9 Step 4 – Implement and Verify Appropriate Controls

Appropriate controls should be implemented based on the assessment output from Step 3.

Table 5.4: Example Controls

Example of Type of Control	Typical Method of Implementation for a Process Control System
Modification of process design or system design	Functional specification re-issued with changes Risk assessment updated to reflect new design
Application of external procedures	Check as part of handover that additional SOPs put in place by regulated organization
Increasing the detail or formality of specifications	Scalability of documentation package (e.g., low risk system detailed design might be combined into the functional specification)
Increasing the number and level of detail of design reviews	Tends to follow the detail/formality of specifications Might also include additional subject matter experts in the review
Increasing the extent or rigor of verification activities	Scalability of verification activities (e.g., low risk element may need only functional level testing whereas high risk also requires structural testing)

The controls are required to be verified in order to confirm that the implementation has been successful. Verification planning should include for traceability back to the risk assessment output to demonstrate that all required controls have been appropriately verified.

Process and/or equipment verification activities also will be required. Furthermore, it may only be possible to verify certain controls in association with the physical process and equipment. Combining verification activities for the control system with these can make significant efficiency gains, but this needs to be considered at the planning stage of the verification activities.

5.10 Step 5 – Review Risks and Monitor Controls

Reviewing of risks during the project life cycle normally includes the following (non exhaustive list) for a process control system:

1. Design Reviews:
 - whether the design includes all elements identified as part of risk mitigation
 - whether any assumptions about the system design (e.g., the software categorization) are still valid
2. Post Execution Reviews of Verification:
 - whether the verification included all elements identified as part of risk mitigation
 - whether any changes made during system development and testing have been appropriately fed back into the risk management process

3. Risk Assessment as part of system release:

- whether all procedural controls are now in place
- whether all necessary design and test reviews have taken place
- whether any known faults, pending changes, or workarounds have been appropriately fed back into the risk management process

During ongoing operation, review of the risks will be triggered from:

4. Corrective Action/ Preventive Action (CAPA):

- Are previously agreed controls still effective?
- Are any previously unrecognized hazards present?
- Is any estimated risk associated with a hazard no longer acceptable?

5. Change Management System

- Will any new hazards be introduced by the change?
- Will any previously identified hazards no longer be applicable?
- Will the estimated risk associated with a hazard be affected by the change?
- Will the change affect any control previously put in place?

6. Process Performance and Product Quality Monitoring

- How robust is the process control system?
- How variable is the process control?
- Is the original risk assessment invalidated, e.g., following changes to applicable regulations or change of system use.

On system retirement, risks associated with retention or migration of data will need to be considered.