



# Irish Automation Seminar

---

## A Risk-Based Approach to Validation of Automated Plant Control Systems

Presented by: Nigel de Haas

QMS 2000 Lead Auditor  
Measurement & Control

 2005

# What is Validation?

Oxford Concise Dictionary

“sound, defensible, well-grounded and sufficient; executed with proper formalities”

O 9001 Quality Systems

“Validation is confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled”

-Based Approach to Validating Automation Systems 

# Why Should We Validate?

## Regulatory Requirement

- Specific requirement of IMB, FDA etc.
- Required by EPA for environmental control

## Safety Requirement

- To ensure safe operation under all conditions
- Required for compliance with IEC 61508 and 61508

## Good Engineering Practice

- To ensure that equipment will function correctly
- It makes good business sense

-Based Approach to Validating Automation Systems =====

## v Much Validation is Necessary?

Validation is about risk reduction to acceptable limits, in order to provide the confidence that the process will meet its specified requirements

order for risks to be reduced, they must be:

Formally identified and quantified

Subject to control measures that reduce them to the specified acceptable level

Tested to a level that is commensurate with the level of risk

is is risk-based validation

-Based Approach to Validating Automation Systems =====

## ◀ Assessment

assessment is the core of the system validation strategy - it takes place at three or more stages through the system life cycle

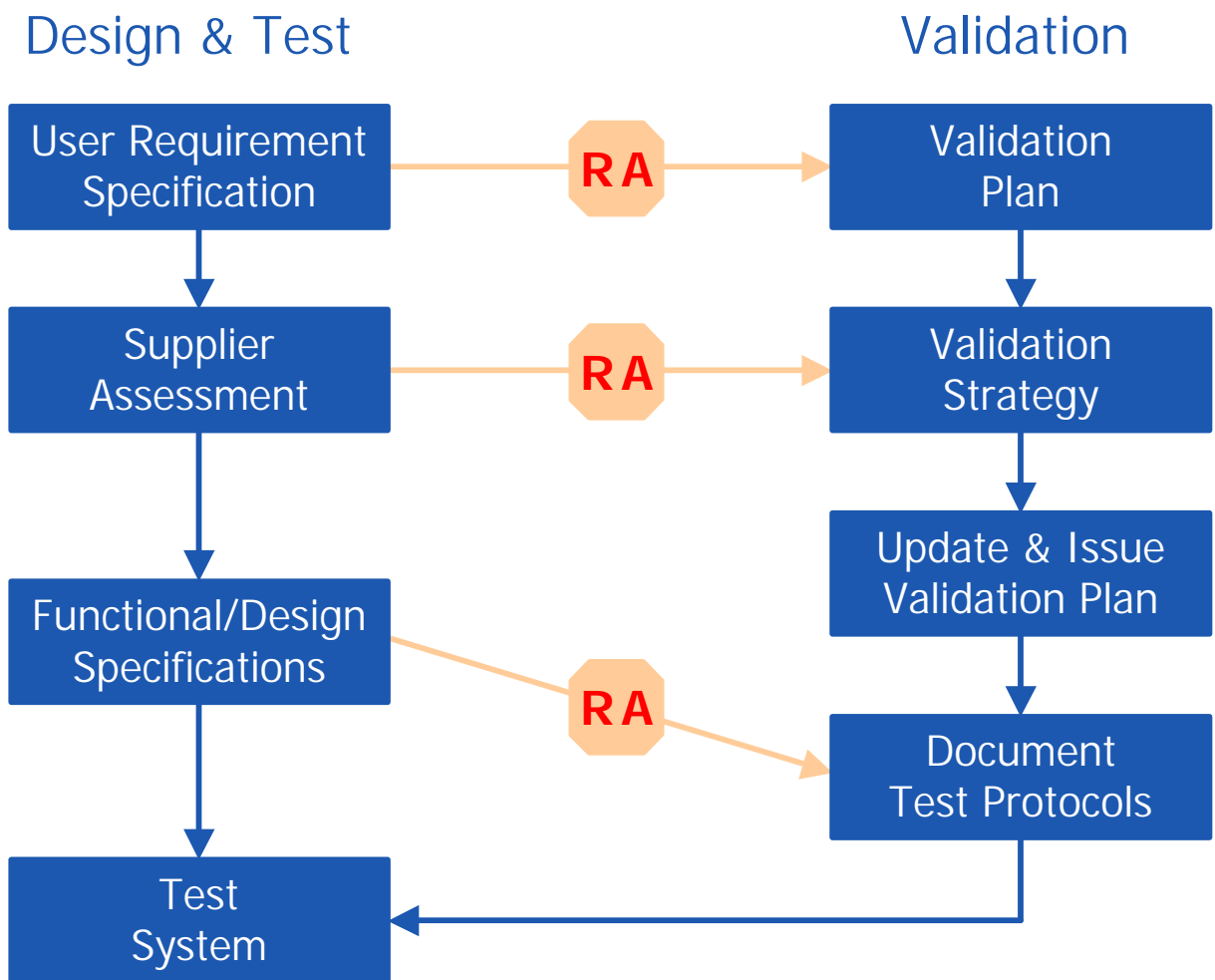
the criticality assessment carried out on the production of the user requirement specification

the validation strategy risk assessment that is carried out once the proposed system structure is known and the supplier has been assessed

the functional risk assessment (e.g., HAZOP, IEA etc.) of the documented design

-Based Approach to Validating Automation Systems =====

# Integrating Risk Assessment to Validation



-Based Approach to Validating Automation Systems

## ◀ Management Process

risk management process consists of five steps

1. determine system category

2. assess system impact

3. assess risks (proportional to impact)

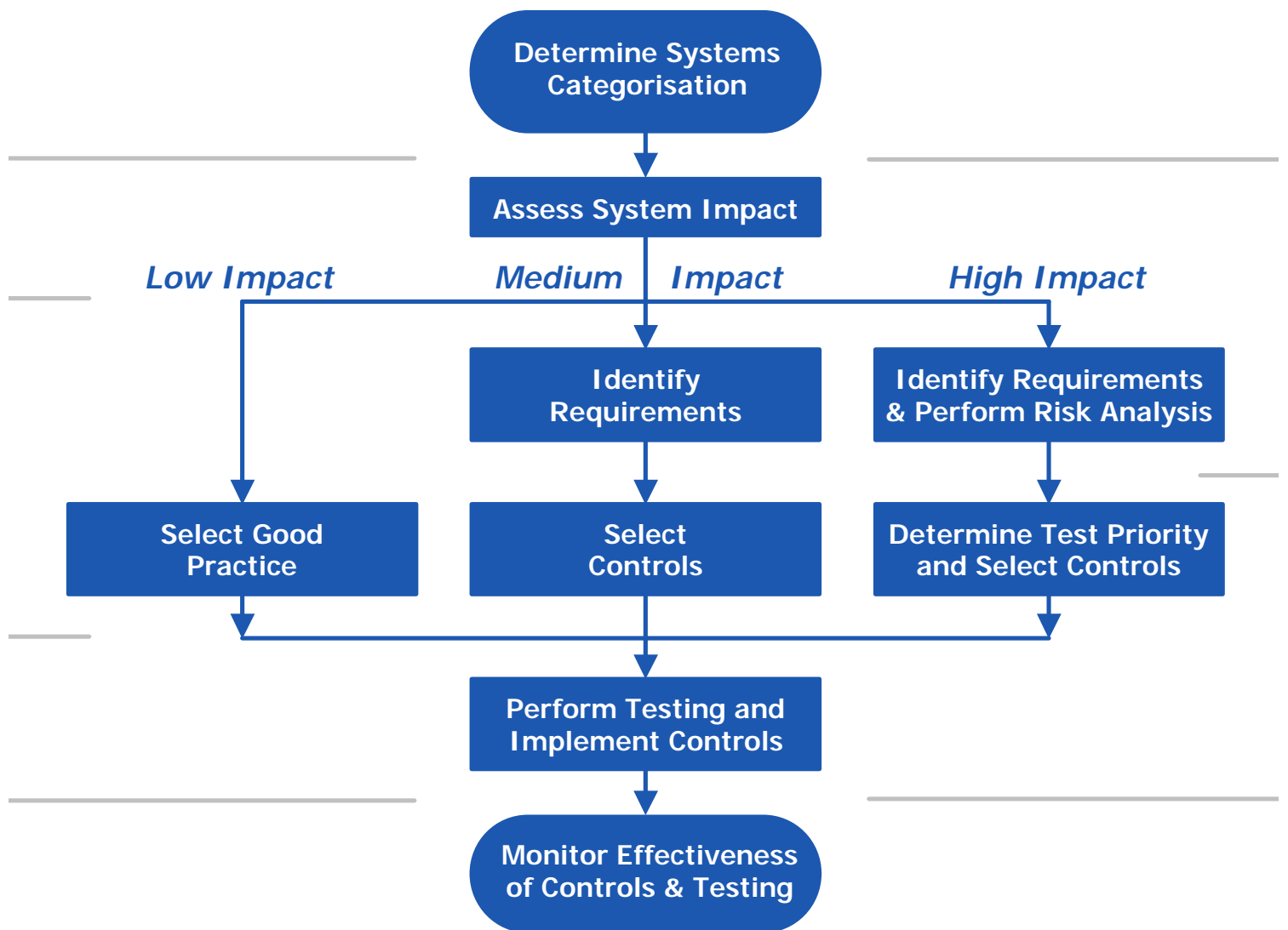
4. test and implement controls

5. monitor effectiveness of controls

⚡: Thorough cross-referencing is essential to ensure that no elements are lost between steps

-Based Approach to Validating Automation Systems =====

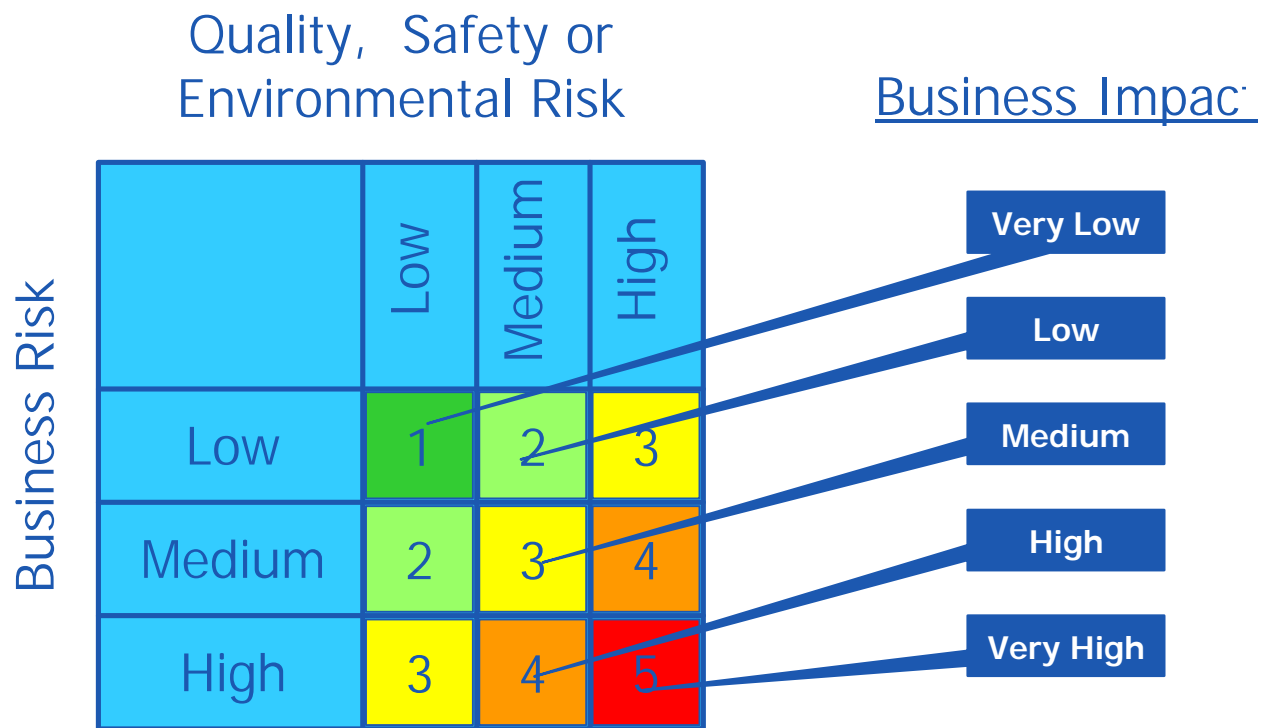
# 14971 Risk Management Process



-Based Approach to Validating Automation Systems

# Assessing the System Impact

to assess business impact from the severity of the process risk, and the quality, safety or environmental impact:



-Based Approach to Validating Automation Systems

# How to Select the Software Category

Category	Software Type	Validation Approach
	Operating System	Record version including service pack - the system will be indirectly challenged by functional testing
	Firmware	Record firmware version and configuration Calibrate instruments and verify operation
	Standard Package	Record version and configuration of environment Verify operation
	Configurable Package	Record version and configuration. Audit supplier if application is critical. Verify operation
	Bespoke Software	Audit supplier and validate complete system

Supplier- and Configuration-Based Approach to Validating Automation Systems

# Determining System Impact

How to determine the system impact based on the business impact and the software category:

Software Category

	1	2	3	4	5
1	1	1	1	2	2
2	1	1	2	2	2
3	1	2	2	2	3
4	2	2	2	3	3
5	2	2	3	3	3

System Impact

Low Impact

Medium Impact

High Impact

Business Impact

-Based Approach to Validating Automation Systems

# Extent of Validation

extent of risk assessment should be based on system impact

Low System Impact

These should be validated using good practice

Medium System Impact

Functional risk assessment of individual or group functionality required in addition to good practice

High System Impact

In addition to good practice, these systems should be subject to rigorous functional risk assessment

-Based Approach to Validating Automation Systems

# Validation Test Prioritisation

potential hazards to each individual or grouped functional requirement should be formally identified and analysed by a cross-functional team including the following, considering:

- the severity of the consequence

- the probability of an occurrence

- the likelihood of detection prior to harm occurring

Results should be recorded in a standard format and used for all risk assessments

-Based Approach to Validating Automation Systems =====

# Automation Test Priority

test priority is a composite of the system impact and the probability of detection - it is necessary to assess the risk classification from:

		Risk Likelihood			<u>Risk Classification</u>		
		Low	Medium	High			
System Impact	Low	1	1	2	Level 3		
	Medium	1	2	3	Level 2		
	High	2	3	3	Level 1		

-Based Approach to Validating Automation Systems

# Validation Test Priority

How to assess the validation test priority based on the risk classification and the probability of detection :

	Probability of Detection			
	Low	Medium	High	<u>Test Priority</u>
Risk Classification				High
	Level 1	H	H	Medium
	Level 2	H	M	Low
	Level 3	M	L	Low

-Based Approach to Validating Automation Systems

## Control Measures

control measures that are appropriate for reducing the risks to an acceptable level may consist of one or more of the following:

• adjusting (Validation test priority)

• modifying the process

• modifying the design

• applying technical controls

• applying procedural controls

# Questions?



D.H.Controls Ltd.

☎ +353 23 56896    ✉ [ndehaas@dhcontrols.ie](mailto:ndehaas@dhcontrols.ie)

-Based Approach to Validating Automation Systems 

---