innomech
Automation Solutions

# From Eureka! to FMECA:
# The benefits of risk-based analyses during validated system development

**Dr Peter Woods, Programme Manager, GB Innomech Ltd**
**Eur Eng David Beale, Technical Director, GB Innomech Ltd**

## Abstract

In this article, we discuss the value of a properly focussed analysis of engineering risk in the design of automated manufacture and test systems for pharmaceutical applications, and illustrate our case with real examples seen in the manufacture of medical devices and in the design of machines used in drug development.

## Introduction

In bringing new pharmaceutical products or medical devices to market, producers must adhere to rigorously documented procedures overseen by regulatory bodies, as embodied in for example ASTM E-2500 [1] and GAMP 5 [2], as well as maintaining a self-regulated quality system as in ISO 13485/ISO 9001.

Typically, producers are dependent on third parties to supply instruments and systems for manufacture. The producer must demonstrate that their production process, including these third-party elements, meets necessary standards often involving formal validation. Consequently, producers expect that any third-party systems must themselves be demonstrated to be built to purpose, compliant to the same methodologies mentioned above.

## The V Model

The heart of this process is the familiar “V” model which was first developed for software development and which came to symbolise the approach defined in the GAMP guidelines. The prime motivation for the V model and its associated documentation is the control of risk, which is our main area of concern in this article.

The V model is illustrated in figure 1. In this figure, the left hand arm of the diagram represents the succession of specification documents that starts with the user requirement specifications (the URS) against which a functional requirement specification (FRS) can be generated, and against which, in turn, a set of implementation specifications can be defined which embody how a specific solution will be engineered.

It is often the case that the automation provider takes responsibility for producing and maintaining these documents, even the URS, although of course these must be reviewed and agreed by both parties. At each level of the V there is a corresponding test specification on the right arm, so that as the elements of the solution are implemented and brought together it is possible to demonstrate that the intended functions are achieved and the user requirements are satisfied. This will include Installation Qualification (IQ), to demonstrate that the system as installed is complete, correctly configured, and has the right services supplied to it, and Operational Qualification (OQ) which determines that the installed system functions safely and to specification as a subsystem.

Please note part of this article was first published in “Pharmaceutical Technology Europe” in Sept 2009

An example of where care is required is where factors may vary from when they are qualified, such as ambient temperature. In tropical or semi-tropical locations, the indoor temperature can soar late in the day once the air conditioning switches off, allowing embedded computers for example to overheat, leading to sudden failure of the system in operation. The supplier is usually best placed to define the IQ and OQ test protocols working with the user, since these require a detailed knowledge of the system behaviour and service requirements, and indeed for a substantive system the supplier should supply a building and services specification to allow the site to be properly prepared ahead of installation. By contrast, the Performance Qualification (PQ) must be the responsibility of the user.

Where the third party element is a standard product, the purpose of the validation exercise is to confirm the design is an appropriate choice to meet the process needs, as well as to confirm the supplied version is installed and working as intended. In these instances, the documentation can also be standard.

For example the OQ test protocol might be a standard document for the product and the IQ might be a checklist generated from a generic template. The user may request copies of generic or type approval documentation in addition.

By contrast, automated systems must be designed for purpose and as a result each system is unique, often complex. In this case the project to supply the automated system must follow appropriate standards and generate all necessary documentation including system-specific specifications and test protocols. A supplier who is already familiar with these standards can add a great deal of value in helping to draw up these documents.

**FMECA**

Engineering companies are well acquainted with the process of a Failure Modes Effects and Criticality Analysis, or FMECA [3] to control risks in both the project itself and the system design. But although there are standardised techniques for quantifying and prioritising risks once identified, there is no guidebook that can tell anyone how to find every relevant risk factor in a particular process or project.

In fact, to be most effective, the analysis requires not only engineering judgement but also an ability to think laterally, to think of potential error conditions and how they might be alleviated. And it helps to be a free-thinking pessimist!

By contrast, the process of validation tends to be reductive in nature and the mindset of those involved can often be an expectation that the analysis will lead to the identification of additional functions and need for testing that is far from exciting to the engineering team developing the system. This dilemma brings to mind the tension between the need for formalised structure and the role of creativity [4].

**Earlier is Better**

For the automation provider, the additional level of documentation can be seen as a critical overhead to supply into this regulated market. It is not untypical to find much of the test and compliance effort being addressed late in the project, so that documentation might even lag behind the supply of the automated system itself, limiting when the system can be handed over for formal validation and productive use.

Whilst this approach allows all regulatory and quality goals to be met, such a retrospective analysis can miss the intended purpose of minimising risk through design, since even if valuable improvements are identified it is too late in the process to incorporate them in what is delivered.

Worse still, by focussing narrowly on confirming tight statements of functionality, the risk analysis and testing strategy does not encourage a consideration of how a system might fail in practice, which might have usefully informed the original design process.

For example, one function specified for an automated end-of-line test platform for a medical device was intended to ensure that two similar mechanical components in the device had not been exchanged in error during assembly, since the assembled device in this case appeared normal but would fail to operate effectively. Although the test function was feasible and the testing machine worked reliably, a better solution if recognised earlier through a wider examination of risk could have identified a design modification to one of the components to make it impossible for them to be confused during assembly.

Risk analysis should be conducted when the URS is first drawn up and be ongoing. Users may be aware of errors that can occur in an existing process which the URS can address. However some historic failure modes become less important or irrelevant in the automated version whereas new factors can become critical. At this stage, a risk analysis can help identify new issues, especially if the review includes people unfamiliar with the existing manual process.

The effective early use of the FMECA approach can be illustrated by the following example, again concerning a medical device. A spring force produced by the medical device, and critical to its operation, was the subject of a proposed static test system. In developing the test platform, the FMECA exercise revealed three additional potential failure modes in the assembly that would not be detected in a static test.

The test system developed into a machine that could perform a dynamic test program to confirm the absence of any of these failure modes. If the same information had instead come to light after the original test platform had been finalised, a substantial redesign exercise would have been required. And by that stage there is a huge inertia to be overcome in updating design documents, revisiting testing specifications, and deciding what retrospective retesting might be involved after implementing the change. At best, the change adds cost and potential delay to the supply of the test system. At worst, the launch of the device itself could have been severely delayed.

**Resolving risk**

As projects develop, known risk factors should be addressed and resolved. However, focussing only on the factors identified earlier can be another reductive exercise whereby the items in the FMECA are ticked off one by one, typically by identifying a test condition to be incorporated into one or other test protocol. It is important to realise that in the lifetime of a project, new risk factors might emerge at any time, and the nature of previously identified risks might change.

In the example considered above, where extra functionality is added to the scope of an end-of-line testing machine, it was realised at a project review that an earlier, sound, decision to effect a movement pneumatically could potentially lead to error in the measurement system now that additional test functions had been added. The actuator was replaced with a servo motor to eliminate the risk of that error, something that if not spotted may have led to incorrect results from the testing process, potentially compromising product safety.

Sometimes the Risk Analysis can throw up unexpected benefits. For example, in developing a design specification for a machine incorporating an expensive precision microbalance, it was clear from the user requirements specification that 1) the balance had to be easily removable by the user for independent use, and 2) for maintenance purposes, the maintenance operator required a way of seeing the raw balance output to check the device calibration.

Please note part of this article was first published in “Pharmaceutical Technology Europe” in Sept 2009

A straightforward conversion of these requirements would have yielded a perfectly adequate result. However, as part of analysing the operation of the device it was realised that adding a user function for simple weighing provided a way for a user to avoid needing to remove and replace the balance, could be implemented using a subset of the user interface already required, and eliminated the need for a special maintenance screen. The client was delighted to amend their URS to add this feature which, in retrospect, seems obvious, but which could have been overlooked by focussing on the letter of the specifications.

**Summary**

We hope this article has given some insight into the importance of an enlightened approach to the analysis and mitigation of risk in regard to automated production in regulated environments. In summary, we offer the following advice:

- When selecting a supplier, look for understanding of validation process – a supplier with the right experience and accreditation will make life easier for the organisation on the receiving end.
- Make sure the approach to documentation matches the needs of the project – will you end up having to rework a supplier's standard version into a specific qualification document or can the supplier provide this for you?
- Remember that both yourself and your automation providers should be using risk analysis tools to manage the project through its life, as well as simply a means of demonstrating that the necessary quality and regulatory standards have been met. We recommend the FMECA formalism for this purpose.
- Involve the supplier as early as possible so that the analysis can benefit from both application domain knowledge and engineering insight.
- Finally, consider to what extent you should be involved with the supplier's risk analysis process, for example, to review the plans for mitigating risk and ensuring there is a common understanding of the potential impact of failure modes. As discussed above this can potentially help both sides avoid problems early on and even spot ways to benefit both parties.

**References**


1 ASTM Standard E 2500 – 07, Standard guide for Specification, Design and Verification of Pharmaceutical and BioPharmaceutical Manufacturing Systems and Equipment

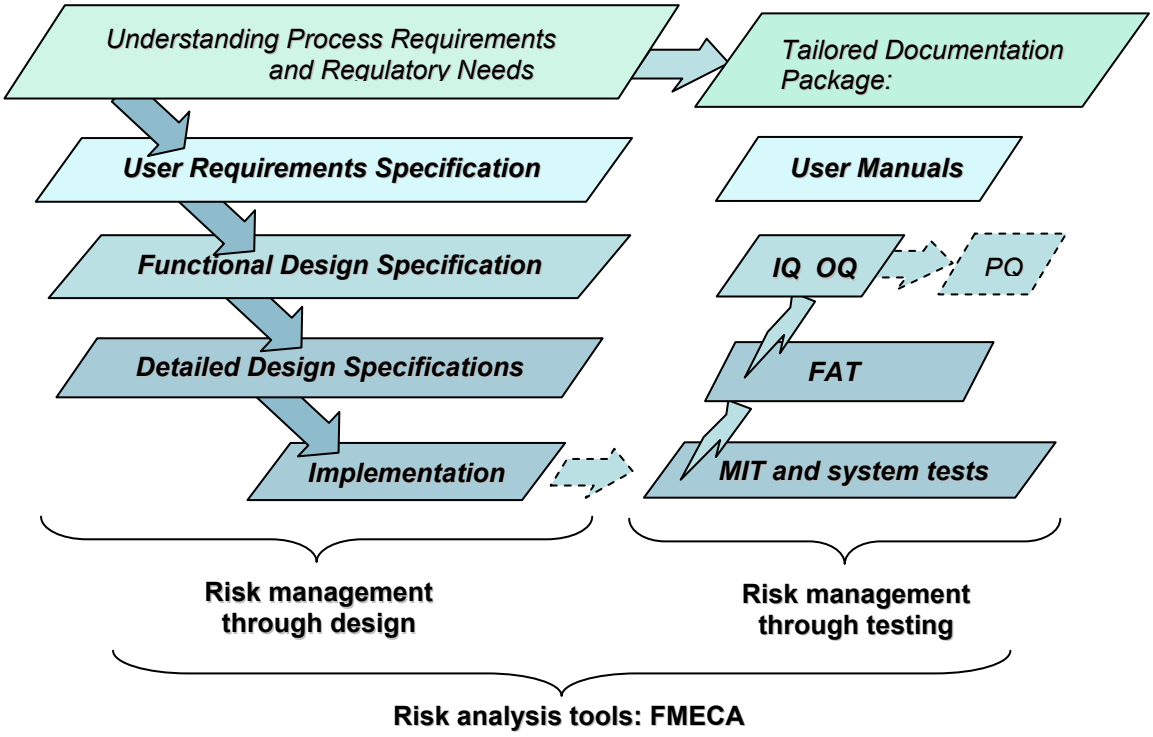
2 GAMP 5, International Society for Pharmaceutical Engineering, Tampa FL 2008

3 See for example http://www.weibull.com/basics/fmea.htm

4 Creativity Versus Structure: A Useful Tension. J S Brown and P Duguid, MIT Sloan Management Review, 15 October 2001.


Please note part of this article was first published in "Pharmaceutical Technology Europe" in Sept 2009

Figure 1




**ENDS**