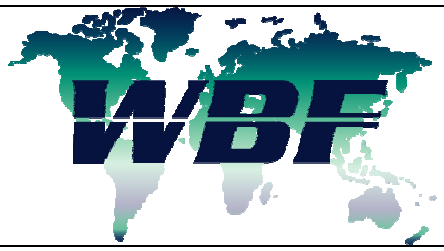
Presented at the
WBF
North American Conference
Atlanta, GA
March 5-8, 2006



195 Wekiva Springs Road, Suite 200
Longwood, FL 32779-2552
+1.407.774.5764
Fax: +1.407.774.6751
E-mail: info@wbf.org
www.wbf.org

Lean Computer Validation through a Risk Based Approach – Case story: SCADA upgrade project

Peter Werner Christensen
Quality professional
NNE A/S
Gladsaxevej 363
DK- 2860 Soeborg
Denmark
+45 3079 9600
+45 4444 3777
pwch@nne.dk

KEY WORDS

Lean validation, risk based approach, risk assessment

ABSTRACT

Lean Computer Validation through a Risk Based Approach – Case story: SCADA upgrade project

A substantial SCADA upgrade would earlier have caused full re-validation including update of basically all documentation and verification of a major part of the original functionality. This activity is costly and time consuming. This paper describes how to save up to 75% of the expected cost by applying Risk Assessment to the change of the system, so that risks are identified and eliminated, a feasible level of re-validation is defined and all existing validation reused to the degree possible.

Using a case story from a SCADA upgrade project the paper will describe how to structure the project and how to define the system model that is a necessary input to the Risk Assessment. It describes how to carry out a series of risk assessments and subsequently eliminate the unacceptable risks by changing key concepts or by adding controls and barriers. A very large number of possible test combinations were initially defined but a Risk Assessment Analysis reduced this to less than 10 situations to be tested. The result was a more controlled upgrade project, fewer necessary test protocols and considerable savings on expected time and cost.

Key aspects include:

- Relevant system model used
- The risk analysis influence on the validation planning
- Lessons learned

PAPER

Project background

In the spring of 2005 our client wanted to renew their SCADA system. The factory was built and initially validated in 1996/97 and all hardware in the SCADA system had the same age. During the intervening years all the software was continuously updated and the hardware was kept alive. The validation status was maintained using a strict change procedure.

It became more and more difficult to get the necessary spare parts and the operating system on the computers (Windows NT) was no longer supported by Microsoft. The up-time on the old equipment was no longer as good as it was initially.

The client was therefore forced to do take corrective action. A decision was made to change all hardware to the newest possible and to move to the latest versions of the operating system. The decision was made to move the servers from a Windows NT platform to a Windows 2003 platform and change the clients from Windows 98 to Windows XP. There was also a wish to migrate from an old SCADA version to a newer version.

The total SCADA upgrade was to be done with a focus on the entire plant being in a non-compliance situation for the shortest possible period of time. The goal was to be able to produce product while being in GMP compliance all the time, except for the small window necessary to make the physical change of equipment and

time subsequently needed to get the system validated and released for production again.

The layout of the factory consisted of several different cells, which in principle worked independently of each other, with the only communication through the overlying MES system. See Figure 1.

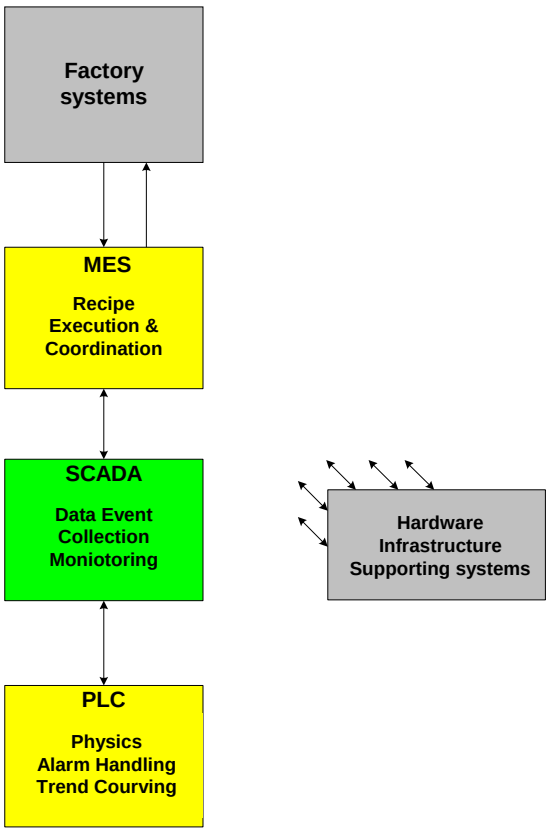


FIGURE 1

Figure 1 shows a schematic system architecture where SCADA only has interfaces upwards to MES and downwards to PLC systems. This is used as an important input to the Risk evaluation later in the project.

Validation challenge

The existing validation documentation was huge and contained in many binders. Furthermore many change requests supplemented the original validation. As usual, when the SCADA system was being updated large volumes of old validation documents and protocols had to be found, opened and updated. In the case

described here it would normally have been necessary to perform a full new revalidation as the change of the system would have direct impact on the product.

From the beginning of the project the client wanted to make the necessary re-validation as lean as possible. The whole system was already in full cGMP compliance and a detailed record of the systems performance was available. A key issue for the validation challenge was to cause the smallest possible interruption of the running production.

The upgrade project was not allowed to change any of the functions of the system and the application software was to remain unchanged. The supplier of the SCADA software had stated that existing application software from the old FIX 32 system could be reused without any changes on the new iFix with Desktop system.

Very early in the project it was decided to try to follow FDA's new Risk Based Approach strategy. This strategy helped us chose only the necessary efforts to put into the update project and only document what was really needed.

It was also decided that the upgrade of the individual servers should be made independently of each other so it could be planned into the natural slots for maintenance in the production.

FDA Risk Based Approach strategy as interpreted by us

Since the fall of 2002 FDA has worked on a new strategy, which was launched under the headline "A Risk Based Approach". In September 2004 FDA issued their new thoughts in the paper 'Pharmaceutical cGMPs for the 21st Century - A Risk-Based Approach'. Most recently in November 2005, the FDA consistently promotes this thinking in statements and conferences. These new FDA signals have opened up a whole new way of thinking about upgrades and new projects in the Pharmaceutical industry.

The validation process should not produce "Great Mountain of Paper" ("GMP") anymore but **the** proven evidence providing a high degree of assurance that a specific process will consistently produce a product meeting its pre-determined specifications and quality attributes as already stated by the FDA in 1987. As the FDA stated again in November 2005 we must all go back to establishing only the documents that really produce the stated evidence – and only this – and it must be based on scientific judgment.

One of the FDA's goals for this approach is to get more and cheaper medicine to the public and a better quality than it is today. FDA has seen that the Pharmaceutical Industry today exhibits a very high degree of variation in the medicine that it produces. It is also acknowledged that the industry has a low utilization rates and high scrap percentages during production. The FDA has stated that their old way of thinking may have prevented the industry from making the necessary changes.

FDA encourages the industry to make quality improvements and they are prepared to make it easier to do this. A means to do this is to implement a Risk Based Approach by defining the need for validation efforts. And this is what we did in this project.

We decided to perform the Risk Management according to the most used guidelines/standards in the industry today and we thus used the principles laid down in ISO 14971 and ICH Q9. These two documents provide good inspiration for the work.

Planning the project

Before the SCADA upgrade project could be started it was necessary to define an appropriate system model for the upgrade of the SCADA system in question. A team of experts was established to analyze what the upgrade would consist of.

The GAMP 4 software categories were used as guidance. These categories are defined briefly as follow:

Category	Software type	Validation approach
1	Operating Systems	Record version, check applications
2	Firmware	Record version, configuration and calibration. Verify requirements and test functionality
3	Standard Software Packages	Record version (and configuration of environment). Verify requirements. Consider auditing supplier.

4	Configurable Software Packages	Record version and configuration. Verify requirements. Validate any bespoke code. Audit supplier.
5	Bespoke Systems	Audit supplier and validate complete system

The SCADA system was then divided into individual software components which all were all evaluated against the GAMP4 software categories to identify the validation approach. It ended up with a System Model as shown in Figure 2. Focus was put on configuration, setup, drivers and supporting software. The hardware and operating system were also included.

The System Model is shown in Figure 2.

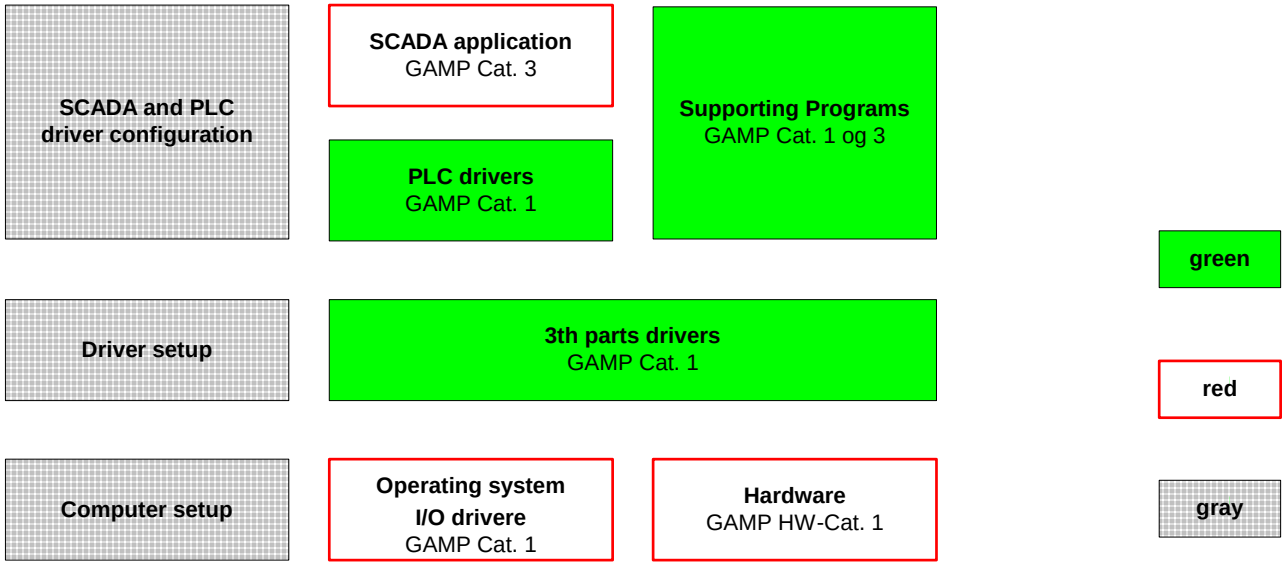


FIGURE 2

Figure 2 illustrates how the System Model is defined. The red colors show the known components which are to be upgraded. It was important to keep it very simple in order to be able to use this abstraction in the forthcoming work. To simplify the green and red "PLC drivers" and "SCADA application" the gray box with driver configuration was drawn out. The setup activities were also separated and illustrated as two gray setup boxes. The green boxes illustrate components that are being reused.

The SCADA system software itself was categorized as a GAMP software category 3 and the supporting programs were categorized as 1 to 3 depending on type. The

rest were all software category 1. The validation efforts of this software were used as an input to the Risk Assessment later on.

Basic Validation concept

It was decided to minimize the validation efforts to the lowest possible level and still be in full compliance with cGMP and leave the SCADA system in a new validated state after the upgrade. Therefore PC clones were used to the degree possible.

The idea of using cloned images of a PC is that when one PC is validated and the rest are just images of the first one – the validation efforts of the rest will only be to secure that the image is restored successfully without failure. The validation documentation for the rest of the group will therefore only be a test plan that shows that this situation is established.

To define the additional validation efforts it was decided to let the result of the Risk Assessment be the guidance for this challenge.

Risk Assessment and the validation planning

As mentioned earlier it was decided to use a risk method, which was inspired by ISO 14971. Therefore it was necessary first to define an ALARP distribution. The concept of ALARP is a key element of the ISO 14971 standard. ALARP means “As Low AS Reasonably Practicable” and is something, that should be agreed upon before starting a Risk Assessment.

Before the Risk Assessment was carried out it was decided that the User Requirement Specification (URS) for the SCADA upgrade project should form the basis for the analysis and that the Validation Plan should be directly affected by the result of the Risk Assessment.

A Risk Team was established. Members of this team consisted of a Facilitator who was an expert within the Risk Assessment work and a Quality expert who knew the procedures to follow. The rest of the team were experts in the specific systems.

The Risk Team agreed upon an ALARP scheme with logarithmic values and 3 levels for probability (p) and severity (s). It was used in the further analysis work. See Figure 3. Furthermore a three-level evaluation of the detection was used.

P_{harm}				
P3	1,00E-02	1,0000	10,0000	100,0000
P2	1,00E-03	0,1000	1,0000	10,0000
P1	1,00E-04	0,0100	0,1000	1,0000
P0	1,00E-05	0,0010	0,0100	0,1000
P	1,00E-06	0,0001	0,0010	0,0100
		1,00E+02	1,00E+03	1,00E+04
Severity		S1	S2	S3

FIGURE 3

Figure 3 shows the chosen ALARP scheme. As it is shown a logarithmic scale was used and only a simple band of ALARP is accepted. During the Risk evaluation it was decided that all yellow and red hazards should be mitigated.

The first task for the team was to go through a brainstorming session regarding possible hazards in relation to the coming upgrade project. The PHA (Preliminary Hazard Analysis) method was used for this purpose. It ended up with a list of hazards that needed to be grouped to continue the work. The time used for this first brainstorming meeting was fixed to only 2 hours. It is our experience that these kinds of meeting should not take longer, in order to make sure that they remain effective.

Step	Action	Result
1.	Perform a Preliminary Hazard Analysis, PHA (brainstorming)	List of possible hazards in relation to the upgrade project
2.	Definition of a suitable detail level for the analysis (use of System Model)	Three possible hazards and six root causes
3.	Creation of Excel worksheet	Overview of possible risk scenarios
4.	Calculation of Risk and evaluation Evaluation of possible mitigations for all yellow and red risk scenarios	Excel worksheet with calculation of all scenarios. Proposal for mitigations
5.	Review of the final analysis	Update of Excel sheet

Table 1

Summary of the Risk Assessment flow – step by step

After the first PHA we ended up with three possible hazards that could be introduced by the SCADA upgrade project. The three hazards were:

- Wrong data in the batch report
- Erroneous interface to the operator
- Wrong control of equipment

Things that could cause these hazards were also identified. This was limited to only six different causes (scenarios). It was errors regarding:

- the installation and configuration of the new operating system (Microsoft Windows)
- the installation of the new SCADA software
- the installation of the old supporting software
- the conversion of files

- the configuration of the software
- changed functionality of the new software

The Risk Estimation

After the identification of possible hazards and Root Causes for these we were to make an evaluation of the probability and the severity of the hazards for each of the components from the system model in Figure 2.

Severity	Wrong data in Batch report	Erroneous interface to the operator	Wrong control of equipment
High S3	The batch report contain critical errors - wrong and/ or missing data	Critical errors in the operator interface e.g. wrong and/or missing information on screen or operator can not send required acknowledges	System does not react or reacts incorrectly and feedback from equipment is wrong or missing
Medium S2	The batch report contain insignificant errors e.g. layout or wrong date/time format	Insignificant errors in the operator interface e.g. wrong format of date/time on screen	System reacts incorrectly or not as intended
Low S1	Of no significant importance or not relevant	Of no significant importance or not relevant	Of no significant importance or not relevant

Table 2

Definitions of Severities used in the Risk Assessment

For each of the analyzed situations the possible detection was evaluated. In many cases the system would not be able to run and therefore the detection was obvious as nothing would happen and thereby no risk would be possible.

Many other situations were more difficult and it was necessary for the experts in the Risk Team to make science-based decisions to secure a rational result. It was often a balance between the degree of detection and the related probability.

When this Risk Estimation was completed it was time to make the Risk Evaluation and find proper mitigation for non-acceptable Risk scenarios.

The Risk Evaluation

With the ALARP scheme in Figure 3 in place it ended as expected with a lot of green, yellow and red Risk scenarios. The Risk Team then started new working sessions of identifying acceptable mitigation for all yellow and red cases. This work led directly to the validation effort in the form of necessary IQ and OQ validation activities.

The process itself turned out to be very important as a lot of discussions were carried out during the evaluation. The gathered information was of great importance for the following validation planning. A Risk Report that contained guidance for the validation activities as well as a checklist for specific test items in the validation protocols concluded the Risk Assessment.

The whole effort of performing the Risk Assessment ended up with the use of only 33 hours in total. Often during the project we ran in to situations where we believed that we had to reconsider the Risk Assessment again but every time it turned out up that we had already dealt with all relevant and necessary decisions.

Preparing the documentation

During the preparation of the SCADA upgrade project Visual Source Safe from Microsoft was used to store and manage the necessary Configuration Items (CI). The actual configuration from the production system was used as reference input for the new upgraded configuration.

The supplier of the SCADA system had prepared a complete migration document that in detail explained how the upgrade from the old version to the new version could be done. This document was used as a key guidance for the upgrade project. A special IQ test was prepared to secure correct use of this guidance document.

The Risk Report concluded among other things that after successful upgrade, configuration and approved IQ offline test each SCADA cell should be tested with a reference batch online in Production environment. To get a qualified input to these tests, a meeting was set up with representation from the operators on each of the changed SCADA cells.

It turned out to be a very good investment as many interesting issues were raised during this process. Input from the operators in combination with the checklist from the Risk Report constituted this input to the relevant OQ protocols. In full agreement with the validation plan, this approach would then be sufficient and no other validation tests were conducted.

Key document

The key documents of the SCADA upgrade project were the URS, Risk Report and the Validation Plan. They all acted as the guidance for the project and were used again and again as reference documents.

Only **one** validation report was prepared for each kind of IQ and/or OQ activity – even though there were several cells with server and clients in the whole SCADA system. The reason for this decision was simple. The Risk Assessment had identified the necessary tests and then the conducted, completed, approved and reviewed test plans were sufficient to establish the documented evidence as stated by FDA.

The clients Change Request system was used during the implementation to keep track of the status and progress of the work. Following that system all of the work was carried out and all deviations were closed and approved, and a final validation report was written containing a summary of the entire SCADA upgrade project. Furthermore a new baseline was established and documented.

Lessons learned

In order to control the project and validation impact on the whole system it is very important to stick to the existing functionality and not to be tempted to make any changes during the project phase. It is crucial for the project's success that it is based on a validated platform with a well known performance because the upgrade project can then be considered as an incremental change.

The project showed us that it was very important to define a sustainable system model that could be used again and again during the many decisions that had to be made in preparing the IQ protocols and defining the necessary OQ tests. The system model was also necessary in settling several Risk evaluations in the analyzed Hazards scenarios.

During the Risk Assessment it was recognized that the discussion process itself was very important. It is also important to select the right team of experts to participate in the Risk process. A special focus must be made on the probability of human errors which must be considered at least one magnitude higher than an equivalent error made by machines.

When preparing the contents of the test batch which was used during the OQ activities it was important to involve the operators. They knew many important things about the system and the “intended use” which is a critical focus point by FDA. The OQ test was defined in a way so all critical items were included but at the same time in a way that it could be verified in practice.

The FDA statement of using science based methods should be used to the outmost in order to avoid duplicated works in the validation activities. Use of computer “images” to make copies of computers showed out to be a very good investment. It saved us for a lot of boring and repeating test. In addition there were lots of hours saved in preparing the computers for the different SCADA cells.

The amount of paper in this project was kept to a minimum and compared to a traditional way of performing an upgrade project it is estimated that there has been savings of approximately 75 % of the validation effort. It was also shown that the goal of a minimum disturbance for the production in form of wasted production hours was met. In one case changing the SCADA system in one cell including the final part of the validation activity took less than 4 hours.