

TITLE:

A CASE STUDY FOR THE MODIFICATION OF A LEGACY PROCESS CONTROL SYSTEM AND THE CASE FOR DATA INTEGRITY WITHOUT "Part 11" COMPLIANCE

ABSTRACT:

It can be observed that the language of 21 CFR Part 11 expresses an underlying concern for the accuracy of clinical data that is maintained in a large system environment. The types of controls and documentation requirements laid out certainly focus more toward multi-user systems with highly critical data and network connectivity. The consequence of that valid concern is having that level of scrutiny placed upon older, often standalone, production based systems, where no individual data point is critical. The values simply do not change that rapidly and the data exists in a larger context of controls that reduces the risk of losing any individual reading, or even series of readings. (This is in marked contrast to changing a clinical subject form 'Dead' to 'Live.')

This presentation will describe a non-compliant system which still had controls, the consequences of organizational paranoia about Part 11 and the modifications made to improve compliance. The goal is to show how a system can be changed without significant consequence for data integrity while still remaining 'non-compliant' to the earlier full approach to Part 11.

PRESENTER:

John T. English, Senior Validation Specialist (Computer Systems)
Validation & Regulatory Compliance
Technip BioPharm, Inc.

TEXT:

Good afternoon. My name is John English and I am the Senior Validation Specialist for Computer Systems at TECHNIP BioPharm, Inc, headquartered in Liberty Corner, NJ. Technip BioPharm represents a collection of experience from both the US and our European colleagues in dealing with automated systems and compliance in a variety of environments. I would like to draw on that to present this case study which has been created to provide a discussion framework without focusing on any particular entity.

I first like to observe that 21 CFR Part 11 has a meta-expectation in its requirements. During my initial reading of the final rule, which was some almost exactly four score and seven months ago, it reminded me of a description for controls that would apply to what we used to call mainframe environments. For those of us trained in mainframe or minicomputer applications, tools that would control user and workstation transactions, chain events to their owners and provide security levels were built into the environments. These supported large-scale databases that were designed to hold discrete pieces of information that had separate consequences. This is entirely appropriate for financial and clinical trial environments. There an individual check or patient

record is a discrete and important reality. In the process world, we find ourselves dealing with streams of data which describe operations over time and verify functions within established parameters. While an alarm is a discrete event, it is the overall record which shows how far the system was out of control, when it returned and how that would have an effect on the quality of the product.

The focus of my presentation is to describe a process control system, complete with its faults. I would then like to describe the approach that was available to demonstrate overall data integrity in a system that did not have any reasonable hope of being compliant to 21 CFR Part 11 as formally stated. The system in question was a legacy system for two reasons. First, it was developed before Part 11 was an enforcement reality. Second, it was based upon code and technology that were previously in existence in the corporate environment. It truly inherited its capabilities from the past. The approach taken to the overall control was to develop a production control system with three segments.

Segment one was the system infrastructure. A workstation with an Intel processor was used as host for an MS windows O/S. That station provided instruction sets and data acquisition for a PLC which provided direct control of the production operations. Segment two was the application environment. There were three separate bespoke or custom applications. The process control used a standard RS Logix tool for the ladder logic that was loaded into the PLC. A second tool, also relatively standard, was used to code a graphic interface which also handled data acquisition, alarming and the download of instructions. In order to speed development, an additional program was coded in a higher level language to generate the instruction files. The intent was to allow validation of the instruction generator program as a separate and discrete task. The third segment was the overall organizational controls and procedure around the use of the system, initiation and documenting of batches and storing of records.

That is the simple overview. A set of instructions were generated by the first program. The instructions were verified by a piece of paperwork that was added to the batch record. The operators would then initiate the control program and the system would run on its own to completion. This was essentially a walk away system and, in a number of production runs, a lights out system as well. At the completion of a run, the paper batch record would be filled out and data files would be removed to prevent the system from exceeding memory. This is an oversimplified explanation, but one that I am sure has had a number of people here straining for certain missing words. Let me supply them.

SDLC – The control and data acquisition software was developed with a lot of good hall meetings. It was verified by engineering studies. And, no, you would not have found formal requirements. In the real world, that required remediation and the development of a design package to spell out what had been done.

SECURITY – This particular system emulated the famous 483 that included the phrase ‘The security for this system consisted of the ‘ON/OFF’ switch.’ The assumption was made that the site was secure, as was the building and the production area. The Windows® O/S was not one that had security and it had not been added.

PROCEDURE – Operators knew that the system should only be run as they were trained and to follow the steps in the SOPs. Paper records were printed and sheets were noted, but the electronic files were not formally covered.

DATA ARCHIVING – That was not a production duty and the local procedures did not cover it.

AUDIT TRAILS – Let’s agree that probably is something we should just move past. There were not any that were apparent.

How could this system be used in the current environment? There were no operator IDs, no passwords, no audit trails and no data archiving procedures. The answer was in practices that were not proceduralized and in paper records that were kept. This was not a typewriter system, by the way. The electronic records from the batches were used to review performance, improve process and answer product quality question upon occasion. Given all of that, where is the compliance with the basic goal of Part 11 – data integrity?

What was discovered was that on all of the production records were gathered on a routine basis by a particular member of the staff. While there was no procedure to document it, an employee gathered the records from each production system on a portable drive, verified the copy and then loaded those copies onto a secured folder on a departmental server. Upon review, every file for every run was present on that drive. Since the server itself was backed up, it served as functional archive and repository for the production records. The nature of the record design made the control of the records evident. The programmer who had developed the system elected to have the files named with a value generated from the time and date stamp at file creation, i.e. the beginning of the run. Linkage to the paper batch records was therefore, relatively straightforward. Each batch had a date and time for start. That provided the link to the paper. The end of the run provided a check against the time and date stamp on the file.

This would seem to be a rather thin methodology, but I would refer you a document that I believe gets too little attention. It is the FDA Investigation Operations Manual, Chapter 5 Establishment Inspection, and Subchapter 520 Evidence Development. The specific section 527 Records obtained gives practical direction to field personnel on gathering and protecting electronic records. That calls for time and date stamp, “if possible.” The reality is that in a controlled environment, where there are procedures in place, this is the best we have for now.

What this organization needed was a procedure to document and control the gathering of the electronic records of each production run. This procedure is perhaps the real focus of my

remarks. There was strong resistance to writing it. It was felt that ‘the FDA won’t like this system because it isn’t [fully] Part 11 compliant.’ The lack of the IDs, passwords and other controls were a real concern, but one that could not be addressed immediately. It would have required a sea change of technology and practice. There was also the belief that because the data wasn’t being copied to optical media that it couldn’t be acceptable. (This reflected the urban legend that the FDA only finds WORM drives acceptable.) All of these concerns for compliance are admirable, but it did not address the reality that they were gathering storing and retrieving their electronic records – with no way to actually address why the agency should trust any record they presented. (And, they were able to do so quite quickly, with a simple date sort and file copy.)

This system was lacking almost everything that one would expect in the fully rigorous interpretation of Part 11. What it did have was available data, under basic controls that could be checked for basic integrity if the users and the investigators would understand the structure. I am not suggesting that controls on systems should not be improved, what I am suggesting is the it is possible for basic IT controls to be placed on GMP data for production records which will give us the basic confidence that the data is trustworthy. The risk of change or falsification is something that the organization needs to address and that the agency can review. Until technology and practices improve, it is what we have. In the total picture this system would provide the investigator with what would be needed to do their jobs. (Even if neither they – nor I – would necessarily ‘like’ what we saw.)

In closing, my suggestion is that as the Agency reviews part 11, there needs to be some allowance for the fact that some data is expendable. Sections of a long set of production run data can be missing without adverse affect, e.g. a five or ten minute section in a run that may have been twelve hours long. The key will be why is it missing, how was it addressed and what decisions were made. The focus needs to be more on the data that addresses key decisions – such as deciding to sell a batch rather than burn it, rather than agonize over the ability to trace an individual temperature reading to its instrument and firmware from 5 years ago. (This is an exaggeration.) I believe that the validation package can address many of these individual flaws with a balanced picture. That does not mean we should not and will not improve our controls in the future. What I am suggesting is that in some areas and applications a reasonable level of assurance is actually ‘high’ enough to make a clear decision.

EOD