OPERATION AND MAINTENANCE PROCEDURES - SYSTEMS TO ENSURE SAFETY MEASURES ARE IMPLEMENTED, OPERATED, AND MAINTAINED.

S. A. JAGGERS *

Procedures used to maintain the integrity of computer based batch chemical process control systems are described. The importance of software quality and software change control is identified; a change control protocol designed for software, hardware, plant, and process changes is presented.
Keywords: Change control, software, batch process control.

Introduction

During plant and control system design, various safety and operational requirements may be identified, for example by HAZOP studies, by experience from previous design, and in order to ensure compliance with statutory regulations. Experience of using computer process control system within The Boots Company suggests that safety features are rarely implemented as separate packages, but rather that they are all part of good design and control philosophy. Thus, the validation of safety features becomes part of the plant commissioning exercise.

To ensure that the integrity of such systems is maintained, particular attention must be given to change control procedures, in addition to effective breakdown and planned maintenance.

Many of the points to be raised in this paper, therefore, apply equally to safety features and to normal plant operation - essentially we have found that for the type of process we operate, if our plant is properly designed with respect to the materials and reactions to be handled, and adequately controlled, preferably using a unit operations approach, then separate safety systems are not generally required.

Safety factors originating within computer control system software and hardware only will be considered in this paper, although many of the points could be relevant when applied to the mechanical aspects of the plant.

* The Boots Company, Nottingham

The basis for a satisfactory system

The initial requirements should be identified, making use of as much as possible of the computer manufacturers standard facilities, such as alarm handling, and including a clear definition of the process needs. The critical control parameters, operating conditions, and alarm settings must be defined for each stage of the process; allowable variations and ranges must be identified.

The system should be tested to demonstrate that it satisfies the initial requirements. This would normally be incorporated in the plant commissioning programme, although some features may be tested before the plant is connected to the system. Remember that testing does not inject quality into a system, it merely confirms that what we decide to test works correctly. Any alterations to the system during commissioning must be properly recorded.

When the system is established, all modifications must be controlled, that is, they must be suitably authorised, properly carried out, and fully documented. Particular care should be taken to ensure that modifications do not degrade the function of the system.

Writing good quality software

It has become well established that careful software design will result in code which can more easily be tested and modified and is less likely to exhibit unexpected or undetected faults. Even though the design stage takes longer, the overall software effort over the life of the system will be greatly reduced.

We would suggest that the following points should be considered.

(a) Understand exactly what is required of a program before starting to write code. It always takes much longer to correct design errors than to avoid them in the first place, correcting errors may introduce other errors, and the time taken up in testing is increased.

(b) Divide programs up into subroutines or functional modules that can be tested in isolation. Maintain an easily accessible list of modules, so that subsequent users know what has been written. Think carefully about error handling within modules, and make every effort to detect when invalid data is being supplied to a module.

(c) If the system allows it, use remarks within the program to aid understanding. Put in the remarks while the program is being written, not afterwards.

(d) Be aware of the trade-off between understandable code and fast or memory-efficient code. It may be better to sacrifice execution speed or memory usage to make the program easier to understand, particularly if the program is likely to be modified later. Alterations are much more risky if the original working of the code is not clear.

(e) Limit the size of the software team. The larger the team the greater the communications difficulty, the harder it is to achieve consistency, and the more management is needed to keep track of progress. If the size of the project requires a large team, limit the number of people actually writing code.

Inspection and testing

The question of validation of software and hardware is under discussion and development, and is too large a subject to be dealt with in this paper. Our main concern is that there are guidelines and regulations in existence, but these are written in such a way that it is up to the user to define and justify the actual procedures he decides to adopt. We particularly need to be able to satisfy the Food and Drug Administration requirements, but there is some disagreement between the F. D. A. and industry over the applicability and interpretation of their guidelines.

Reference to our software validation record sheet (Appendix A) gives an indication of the types of testing we have found to be necessary.

We would emphasize the effectiveness of visual inspection of program code. There are many ways of writing programs which work, but to produce understandable and maintainable programs requires adherence to a common standard. Furthermore, it is far easier to intercept and correct errors before the physical testing stage. Ideally this visual checking should not be done by the same person who has written the program.

Testing and inspection should address two issues: -

(a) Does the program do what is wanted?

(b) Does it only do what is wanted, or are there undesirable side-effects?

The first issue is fairly easily dealt with. There are generally expressed concerns over the difficulty of testing programs with more than a few possible code routes, but in our experience, properly written process control code contains very few conditional branches, and is therefore easy to test statement by statement. This type of testing is normally done by the program writer, since we feel he is in the best position to know what tests to apply.

The second issue is potentially more difficult, and is where good design and careful visual inspection can prove its worth. As already mentioned, the risk of errors occurring is greatly reduced by highly modular code, and by adequate consideration being given to checking the validity of data within modules.

Whenever possible, initial testing is carried out on a spare, off-line, computer, using simulated plant measurements. Operation of the program can be confirmed using the same displays as are used for the on-line system, and unusual or limit-of-range input values can be used that would be difficult to produce on the real plant. (Much reference has been made, for example by the F.D.A., to testing at the limits - in practice we rarely find that this type of testing is appropriate).

Change control protocol

The philosophy of generally not using separate safety systems places great emphasis on the procedures used for change control, since in principle any change could affect the integrity of the normal control system, or the embedded safety system, or both. A balance must be established between the need to make alterations and improvements to the system within reasonable timescales, and the need to test and prove such changes as thoroughly as possible.

A system has recently been introduced to formalise the procedures used when changes are required (Appendix C). This protocol applies to all changes, whether to hardware, software, or the plant itself. A change is defined here as planned work which could in any way affect the product or the process chemistry, or the control documentation. (Unplanned changes, such as may arise as a result of breakdowns, are termed 'deviations' and are covered by a different procedure).

A change can in principle be originated by anybody, but must always be authorised by the plant manager, who also identifies the departments that need to know about the change. A change co-ordinator is then appointed, who follows the work as it progresses, and ensures that all supporting documents are collected together for archive.

Validation and testing requirements must be identified in advance, and the check sheet is used to provide a reminder of what validation criteria may need to be applied. (Appendix A).

To define further our procedures both for our own use in order to remind ourselves how we should be operating, and to assist in describing our operations to outside inspectors, we have produced the software change flowchart shown in Appendix B.

Protocol for unplanned changes

Deviations from predefined operating conditions may occur for a variety of reasons; we are most concerned with deviations that might affect the quality of the product, or our ability to confirm that it has been produced according to an agreed set of conditions.

The potential for deviation appears to come from two areas.

(a) Random breakdowns of plant equipment.

(b) Inability of the system to control within the required limits, which in turn is usually due to difficulties in measuring process parameters.

In some cases, it may not be possible to proceed until some corrective action has been taken. Usually, this will be carried out by the control room staff, using their normal facilities for limited operation of the plant outside the control sequence. Only rarely is it necessary for any temporary modifications to be made to the software to overcome such problems.

A potential deviation is reported on a 'Deviation Alert' form. This is then examined by the plant chemist, who completes a 'Deviation from standard operating procedure' form (Appendix D) to accompany the documentation for the affected batch. A review meeting may be held to decide if there was a significant affect on the product, and if so what action should be taken.

Selection of personnel

All development of, and change to software is done by a small team of specialists within Boots.

Personnel are selected by aptitude, and from a background appropriate to the system they support, (for example chemists or chemical engineers are generally preferred for our chemical plant systems), and are trained by making use of manufacturer's training courses and by on-the-job training. The ideal situation is for the personnel who developed the software to continue with its long-term support.

We have experimented with the use of part-time software support, and while this has been a useful approach, particularly during commissioning where full shift cover may be needed, care must be taken to ensure that part-time personnel have enough involvement to maintain their level of expertise. At least one full-time specialist is needed to deal with more complex problems and to co-ordinate activities.

Access Control

Having selected and trained suitable support staff, it is necessary to ensure that unauthorised personnel are not allowed to make alterations to the system. The process control systems at Boots do not have the means of restricting access to particular users; such passwords as are available are rudimentary and either cumbersome to change, or easily overridden.

Fortunately, we have not encountered any problems concerned with unauthorised access. We can only guess at the reasons for this, but factors could include:

(a) Our operating staff are already schooled in the idea that only specific groups of people carry out specialised jobs; in common with other areas, such as electricians, instrument engineers, pipefitters, there appears to be general agreement over who does what, and little need or desire for overlap.

(b) Unauthorised users see no personal gain in tampering with the system, and have a lot to lose if found out.

The control on access is, therefore, of a simple nature. The computer and its programming terminals are kept in a locked room, giving a clear physical location for 'programming' access.

Within the plant control room area, it is sometimes necessary to restrict some operations to certain people, such as shift foreman or product supervisors. We use a mixture of key locks and passwords for this, according to the facilities the system supports; no more than three levels of access have so far been required.

Equipment Location

All our computer systems are housed in control buildings, which are physically separate from the plant itself. The computers are installed in separate computer rooms adjacent to the control rooms. Air conditioning is used, primarily to give a comfortable working environment, since the environmental requirements for modern computers are not difficult to meet.

However, particularly with older equipment, there is evidence that a constant temperature, reasonably dust free, atmosphere will reduce maintenance and breakdowns. Many of our breakdowns have happened during, or shortly after, periods of unusually high temperature due to air conditioning faults.

Fortunately we do not suffer problems from atmospheric contamination, but it is well known that acidic vapours and some airborne dusts and powders can cause problems, particularly at the edge connectors of computer cards.

Equipment breakdowns

Fortunately the realibility of computer hardware has improved dramatically over the years, allowing virtually uninterrupted usage of our computer systems.

When a breakdown occurs, clearly it is necessary to identify the faulty part, replace it, and then confirm that the fault has been corrected. The faulty part must then be repaired or thrown away.

This sounds very simple; in reality there are many problems associated with fault-finding and correction.

Faults may be transient, perhaps occurring a few times a week. It is impractical to shut down a working plant to run diagnostic programs for long enough to identify the fault, so usually an educated guess is made on which module should be replaced. This may cure the problem, but possibly several attempts will be needed.

The situation is complicated by our experience that simply removing and replacing a suspect module, or maybe even switching the equipment off and on again, may cause a fault to disappear.

The result is that one is left with a suspect module, which may exhibit a fault. In most cases, the only option is to return this to the manufacturer for repair. Unfortunately it is not unusual for the manufacturer to find no fault with the module, leaving us the difficult decision of whether an expensive item with no apparent fault should be scrapped.

When a module is replaced, clearly it is necessary to confirm that the system continues to operate correctly. In our experience, the only way to do this is to run it and see what happens, which is not an entirely satisfactory situation.

All breakdown reports are recorded in a log book, to ensure that call-out personnel are aware of previous problems with the system.

Maintenance of computer hardware

Our experience has shown that the maxim "if it works, don't fix it" applies very well to computer equipment, and routine maintenance is kept at an absolute minimum.

This decision was made after an examination of system availability, which showed us that considerably more down-time was caused by routine maintenance than by breakdowns, and that major maintenance was often followed by a few breakdowns.

On our latest systems, routine maintenance is carried out at three monthly intervals. Usually this involves nothing more than checking of power supply voltages, replacement of dust filters, and alignment of disk drives; this is done with the computer (and the plant) running normally.

Maintenance of instrumentation

Plant sited instrumentation is, of course, situated in a much more inhospitable environment, and often contains moving parts which need occasional adjustment or calibration. Such equipment is checked at defined intervals, although it is often difficult to fit the maintenance schedule to the required plant operation cycle.
Keeping track of items due for maintenance has become a complex exercise, and we have introduced a computerised scheduling system. Good communications between plant and maintenance engineers is essential, to allow quick response to plant shutdowns.

Backup and recovery systems

Fortunately, computer system failures do not happen too frequently, but when they do the disruption can be great; it is important to be able to continue with normal operations as soon as possible after the fault is corrected.

Points of particular importance are:

(a) Every change to the software must be documented, so that it is possible to regain the latest status should it be necessary to reload using an out-of-date version. We do this by maintaining a log book containing brief details of all modifications, accompanied by detailed listings showing exactly what has been changed. The points at which system copies were made are also shown in the log.

(b) Several backup copies should be in existence; these should be rotated such that several previous versions are available in case a fault is found with the latest version. These must not all be stored in the same place.

(c) The backups should be clearly identified such that there is no danger of accidentally using the wrong one to reload the system.

(d) The method of regaining the correct plant status after a reload should be considered. We achieve this by writing critical plant status data from memory to disk at two-minute intervals, and including an option to refresh the memory from this backup data during the reload procedure.

(e) Procedures for backup and reload should be properly documentated.

Conclusions

Many of the perceived problems with computer control systems can be minimised by adequate attention to design of the process, the plant, the hardware, and the software.

Good initial design will help to ensure that on-going modifications do not degrade the system.

Procedures can be used to maintain the integrity of the system; operating staff must be committed to following the procedures.

Appendix A

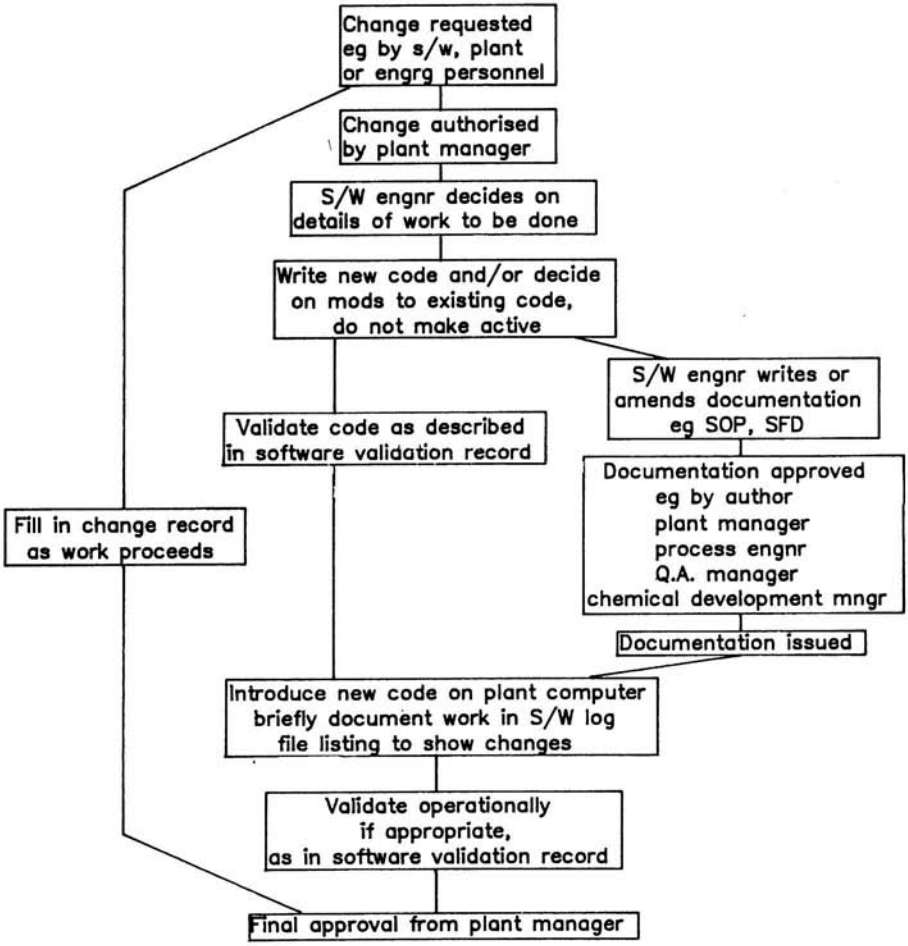
SOFTWARE VALIDATION RECORD

The level of validation required will depend on the complexity of the software involved, and on the anticipated effect of undetected faults. This list is intended to provide suggestions for validation checks; some or all of these checks may be appropriate, but other tests may also be required.

MODULE/VARIABLE NAMES			
TESTS APPLIED	tick if reqd	DATE	SIGNED
Visual inspection of code or variables			
Visual inspection of display or printout			
Check operation in normal range			
Check at range limits, use dummy inputs if reqd.			
Check alarm, fault, or error handling Introduce deliberate errors			
Check physical operation of plant I/O			
Check code against documentation			
Simulate operation on off-line computer			
Observe first run(s) on main plant computer			
Commission using water or dummy materials			
Commission using process materials			
Other (give details)			

Appendix B

SOFTWARE CHANGE PROCEDURE



Appendix C - Change Control Protocol

The following protocol covers all areas of change within the production related operations of The Boots Company Chemical Department (Boots Chemicals). All personnel are required to follow these procedures rigorously.

Any changes to the protocol may only be made with the authority of the Good Manufacturing Practice (G. M. P.) Committee.

Definitions

Change

Any planned work which, in any way, shape or form could affect either the products, intermediates, or control documentation. This excludes normal plant maintenance operations, (i. e. replacement of "like" with "like") or breakdowns where replacements are covered under deviations. Any uncertainties must be referred to the Q. A. Group.

Deviation

Any unplanned occurrences that cause production operations to be carried out in a way differing from normal defined practices or, where appropriate, outside previously defined parameters. This includes plant breakdowns which affect the batch as defined above.

Originator

A change can be originated by any person associated with a process or plant, although, in practice, most might be expected to originate from a small number of personnel.

Authorised By

Following origination, no further work can be carried out without authorisation of the change, by the Plant Manager or persons designated by him in writing. In the Plant Managers absence, the authority must be gained from the Group/Factory Manager.
In non-production areas, authorisation will be by the responsible Line Manager.

Authorisation List

Each Group/Site will provide a list of personnel authorised to sign Change Records together with their areas of authority.

Validation

All changes require validation at a level agreed by the personnel involved. A validation protocol must be agreed before work commences and tests carried out against this protocol.
The validation protocol and results must be included in the Change File as a photocopy or the original. References are not acceptable for this document.

Commissioning

During commissioning Change Records must continue to be issued when appropriate. However, it is accepted that the Change Record may not contain full details of all of the changes carried out, but may refer to the relevant commissioning log for details.
Equally, deviations must also be issued during commissioning but again a single Deviation Report may cover several deviations and may also refer to a commissioning log. It is, therefore, unlikely that more than one Deviation or Change Record should be issued for one batch.

Change Record

The records of work carried out for a particular change, made in five parts on the forms provided. The Master Copies are provided by the G. M. P. Supervisor.
The record is not numbered but becomes unique by use of batch numbers, dates and titles.

Change Reversion

When changes are implemented for a small number of batches following which reversion to the original procedure occurs, a Change Record must be generated to cover the initial change and lodged in the Batch File accordingly. On reversion to the original procedure a further Change Record must be generated, but does not need to be completed. It should simply refer to the original work and state that a revision to the original production procedures is occurring. This change revision record must also be included in the Batch Folder for the first batch concerned.

Change Documentation

All documents referred to in the Change Record as being required to completely document the work. These documents need not be in the Change File although this is recommended. Photocopies are acceptable.

Change File

A file containing the Change Record and all supporting documentation (or references) associated with it. The file is collated by the Change Co-ordinator and on completion, transferred to Q.A. archive where it is stored to be referenced by product, plant, date, title or batch number.

Change Co-ordinator

A person to be nominated by the authorisor after agreement with any other Function Manager if required. The Change Co-ordinator then effectively manages the change and must carry out the following functions:

1. Obtain nominees from other groups/departments involved in the change.

2. Arrange generation and submission of estimate (if required).

3. By use of project team, individuals etc. as appropriate for the change, ensure provision of materials services etc. after first providing a work schedule.

4. Progress work and collate documents.

5. Complete Change Record and arrange for photocopies to be supplied to other departments or individuals as required.

6. Collate all documents into Change File and archive.

It is obviously not always possible for the Change Co-ordinator to "oversee" other function work. His position is rather to ensure the work is progressed by regular liaison and to act as a channel for information, problems etc. In this context, it is unlikely that Change Co-ordinators without significant experience in their own particular functions, will be nominated for any project that is multi-discipline or complex. The nomination of a Change Co-ordinator does not remove the overall responsibility from the authorisors, or imply that any subsequent defects will be the "fault" of the Change Co-ordinator.

Flowchart - Change

1. Originator fills out Part 1 of Change Record and passes it to the Plant or Line Manager.

2. Manager agrees to progress change (or not).

   Manager defines change as minor or major. A major change requires Senior Manager approval.

3. Manager chooses Change Co-ordinator (which may be himself) on the basis of workload, expertise, availability, and commitment.

4. Manager (and Senior Managers, if appropriate) fill out Part 2 of Change Record, noting which departments or groups should be involved. (As the project progresses this group may be added to), and passes document to Change Co-ordinator.

Note 1: In the case of simple changes (e.g. a one line software change), use of the Originator as the Change Co-ordinator is recommended, such that the person carrying out the work may be the only other concerned.

Note 2: In the case of the Manager himself being the originator, a second person should be nominated as Change Co-ordinator.

5. The Change Co-ordinator then gathers together those involved and produces a Schedule of Work on Part 3 of the Change Record. Individual departments then carry out their normal functions to carry out the work.

   The Change Co-ordinator acts as:

   (i) Channel for information.
   (ii) Collator of documentation.
   (iii) Project progressor.

6. On completion of their section of work, the representatives from each department/group sign Part 3 of the Change Record.

7. The Change Co-ordinator (directly or by arrangement) writes or amends the S.O.P. as noted in the S.O.P. Operations Manual if required, noted on Part 4 of the Change Record, but does not yet make this document active.

8. The Change Co-ordinator completes Part 4 of the Change Record, outlining the details of the above points and then presents the full form to the Line Manager for authorisation.

9. The Line Manager signs off the work on Part 5 (or if necessary refers it back for more changes etc if not satisfied).

10. The Change Co-ordinator then activates or arranges to activate the new S. O. P. noting the batch number or date on the Change Record.

Note: Where a change is not specific to one product or one stage of a product such that it is not possible to identify a specific batch, then the date of implementation should be filled in.

11. All documents concerning the Change Record are collated/referenced by the Change Co-ordinator and the Change File completed. Part 5 of form is filled out.

12. If a batch number has been filled in a copy of the Change Record must be immediately supplied to the Plant Administrator for inclusion in the Batch Folder.

13. If no batch number has been filled in but the answer to Q. C. involvement on Page 2 was "yes", or the change involves processing operations, a copy of the Change Record must immediately be sent to Q. C. This will alert Q. C. to the change in order that they may monitor the product if required.

14. Change File is stored in archive.