Transactions on Information and Communications Technologies vol 8, © 1994 WIT Press, www.witpress.com, ISSN 1743-3517

Quality assurance dynamics required in mission critical systems

R. Erskine

Department of Management, Glasgow Caledonian University, Glasgow, G4 0BA, UK

Abstract

Although micro quality assurance methods for the quality and reliability of code within the computer program have improved much within the last 10 years, macro quality assurance methods for the computer project as a whole are still very poorly implemented. In this paper an analysis is done of the Inquiry Report into the London Ambulance Service, a mission critical system, which failed dramatically in November 1992, with a view to finding out whether it would be possible to generalise on some principles of good practice, which, if adopted, could have prevented such a disaster. The author offers a model of good practice project management led by a project champion and a team in which there is a disciplined separation of the functions of specification, validation, programming and operations management. The purpose of the model is to transfer confidently the ownership in a new system from designers to its users. The paper concentrates on the management dynamics of two particular stages of the design/implementation process - the feasibility study, and the 'go-live' decision. The paper claims that if the model were adopted there would be far fewer cases of computerised systems which were resourced for as much as £400 million but never implemented, such as Taurus, or implemented with very disappointing results for its patrons. The paper signposts a new method in design, the adoption of 'viability audits'. The inspiration for this model came from some successfully completed project management assignments done within an environment of many competing stakeholders, commonly found when computerising factory scheduling systems.

Introduction, micro, macro aspects

Enormous strides have been made in the last 10 years in getting quality assurance into the micro aspects of systems design. Code in a computer program is generally reliable, yet in large systems projects waste and disaster seem to be just as likely as they were 10 years ago. Some major projects were abandoned before implementation, such as Taurus, the planned Stock Exchange System for paperless trading. Others, such as the London Ambulance Service, a mission critical system, failed dramatically at the point of implementation. On 26th and 27th October the response time was so poor many 999 callers resorted to taxis to get to hospital. On November 4th the computer system failed totally. However, the case study literature is full of systems which never achieved the NPV expectations of their patrons and needed expensive and unexpected rewrites. For instance, in the autumn of 1990 LAS abandoned a previous attempt to computerise the ambulance dispatch system after being funded at the order of £7.5 million. The problem here is that quality assurance in computerisation projects fails primarily in the macro aspects of design and implementation and project control. This is a big field to discuss. To get a framework into a broad enough perspective it is necessary to assume that an information system is like a product with a life cycle starting at development, working through implementation, maintenance, maturity, and finishing at obsolescence. Computerising in a new field is very like backing a research and development project with all the inherent possibilities of expensive overrun. It should be easy to plan and cost for what is foreseeable, but the very nature of R & D style projects is that there is some risk and uncertainty, and if something does go wrong a lot of problem solving in the area of the immediate trouble will be needed, and assessment of the side effects, and there are generally no resources or time earmarked for this. Indeed if a contractor is a little too cautious in allowing for such contingencies, then the chances are that his tendering is higher than other less articulate operators, and he loses out in the bidding process. One always assumes goodwill among consultants or suppliers, but this is not always the case. A recall must be made to an unscrupulous computer manufacturer who supplied an unsuitable package to an engineering firm, who later got in a real mess in implementation, and had to spend large sums of consultancy money with the supplier to rescue them from the mess. The computer manufacturer was completely unrepentant, delighting in the making of a profit both with the original sale and the subsequent consultancy!

Aim of this paper

The purpose of this paper is to identify some of the norms of good practice from the literature about macro quality assurance, and discuss the problems of implementation. The case

study in prime focus will be the London Ambulance Service, chosen for the public's interest in this case, and the availability of an inquiry report, which was published by the South West Thames Regional Health Authority in February 1993. There is little doubt that if 'good practice' had been adopted throughout the project there would not have been a spectacular failure.

System ownership

A feature of good systems design, and a crucial one for a mission critical system, is that all the stakeholders need sufficient familiarity with the system and its dynamics and the business policies written into its design and commitment to its management and operation. It's not enough simply to hire an external software house and expect a sound solution to be developed from specifications and then implemented. Design and development in which ownership passes requires a significant positive activity of validation by the affected stakeholders. This in turn requires a structure of project management from which there is some role separation between those responsible for specification and those responsible for validation, and management of the project with a groundrule of 'working with validated specifications, no validation no progress to the next stage'! Educationalists from the polytechnic system will be painfully aware of validation, as this was the basis of rigour from which the CNAA approved curricula.

In the case of LAS the Inquiry Feb 1993 para 3116 "A Computer Aided Dispatch system for ambulances operating as it was intended in an absolutely objective and impartial way would always ensure the mobilisation of the optimum resources to any incident. This was perceived to overcome many of the working practices seen by management to be outmoded and not in the best interests of providing the best service to London. Unfortunately such practices could not so easily be eliminated and the CAD system would accommodate them only with difficulty and with a reduced level of efficiency. Management were misguided or naive in believing that computer systems could bring about such changes in human practices. Experience in many different environments proves that computer systems cannot influence change in this way. The introduction of a system which puts the operator into an operational 'strait-jacket' would potentially be doomed to failure."

For instance, ambulance crews reacted when they found themselves working to a rigid computer logic which always dispatches the nearest vehicle to an incident, gradually taking the crew further and further away from their home station into unfamiliar territory, and long drives home at the end of a shift. It is so easy to assume, as the designers did in this case, that there would be an improvement in performance to patients calling 999 if the nearest vehicle was always sent, but

one has to look more broadly at optomising activity between all patients and all crews. If the crews are alienated by the system then they have plenty of opportunities to sabotage the system itself, for instance, by failing to report their vehicle location or status or sabotaging the Datatrack communication equipment, or simply getting into a radio blackspot. It is understandable that crewmen trained to deal professionally with life threatening situations may find it irritating having to grapple with unfamiliar and complicated communications equipment, which they may not see as something directly assisting them in their operational jobs. To them 'big brother' was simply taking them into districts where they may not have known the structure of the one-way streets.

Owing to strained industrial relations between management and the ambulance crews for the two years before implementation this consultation with the crews as part of the validation process had been avoided.

Good practice suggests that as the computer analyst develops specifications then he or she looks to management to point him or her to the business user appointed representatives, who are completely familiar with the processes in the operating environment and have responsibility for validating the rules and policies. If they anticipate apathy or resistance to change and adoption of new policies then it is management's responsibility to initiate the necessary organisation development programme to generate the attitudes and skills to cope with the new environment of computerisation. Where the rules and policies of the system are of an evolutionary nature and likely to be fine tuned as a result of experience, then it is essential that the rules within the computer system are highly visible and easy to alter by request. This is one of the finest points in quality assurance.

The critical 'go-live' decision

Naturally, too the control room staff, and their supervisors would wish to feel comfortable in operating with a computer-assist under varying operating conditions in dispatching ambulances to patients. The 'go-live' decision for a large mission critical system is probably the most vital one there is. Some preconditions are obvious -

- the stakeholders should have ownership and be committed;
- the managers should be confident that they can control the new environment from evidence of trials;
- all the software and hardware should have been 'destructively' tested to ensure that it is robust;

- the system as a whole should have been subjected to systems testing.

This must be the most obvious of norms of good quality assurance. But in the LAS disaster the 'go-live' decision had been simply written like stone into the calender months before by the LAS director. He was desperate to redeem his promise to improve the performance in LAS through computerisation. Of course, working within time and budget are natural norms of good management, but a system involving the integration of many new technologies, is likely to have some unknowns about it. You cannot just come to the implementation date and press the button without taking account of the present viability and risk, particularly if failure or partial failure could lead to loss of life. Indeed, under good practice project management, there would be a regular reporting of the project status forward to the critical milestone dates, and if at any time these looked to be compromised, then project management would either rearrange resources or shift the dates forward; but please, no compromise on the basic parameters of quality assurance, or you are on a very slippery slope.

Under good practice one would expect a contingency plan to be ready on the go-live date so that there would be back-up in event of a failure of one of the file servers to the network. LAS had indeed a back-up facility, but it had not been tested and commissioned, and when the main system failed on 4th November the back-up system was not available. LAS were indeed criticised for not appointing a network manager some months before implementation to ensure that LAS themselves assumed ownership of the network. They could not expect to rely for ever on a software house for administering this vital operating function.

In the LAS disaster there was at least a reporting procedure of PIRs (Project Issue Reports); these were system modification requests. On the implementation date 81 remained outstanding from a total of 1,513. That very high volume of modification requests suggests a serious weakness in the quality of specification work done. Why did they not get the specification right first time? Why did they attempt to implement the system when many of the 81 outstanding PIRs contained crucial weaknesses of the system? The inquiry report also comments on the practice of the software house to put changes through 'on the fly' to please users, thus bypassing the PIR system. The validation process of this system had been seriously compromised.

Instability during testing

Inquiry Feb 1993 para 3098. "During the months the system was under test the system was never stable. Changes and enhancements were being made continually to the CAD software.

The Datatrack system was being similarly amended and enhanced. The Mobile Data Terminal system and Radio Interface system were also undergoing continuous changes. Thus there was never a time when the project team could stand back and commission a full systems test."

Good practice suggests that systems testing should be done from a stable base after the critical modifications have been fully processed.

A Step by Step Approach Advocated

Inquiry Feb 1993 para 5004 f) "Any new system should be introduced in a stepwise approach, with, where possible the steps giving maximum benefit introduced first".

Quality assurance processes should then surround the go-live date for each stage of the implementation, and no future stage should be attempted till the preceding stage has been found to be completely viable. In practice the LAS system had been implemented to some step by step outline plan but quality assurance processes were ignored at the milestones. LAS was simply an organisation which was not capable of learning and responding to its own feedback. This is a crucial weakness in many bureaucracies.

Selection of Software House

Even as late as June 1991 LAS had not assigned any full time staff to this project to oversee its design and co-ordination. They were entirely in the pockets of the software house. LAS were criticised in their choice of software house.

Inquiry Feb 1993 para 3066 "SO are a well established small software house ... However, in taking on the LAS project, which was far larger than anything they had previously handled, we believe that they rapidly found themselves in a situation where they became out of their depth".

Other sections of the inquiry report comment on the tendering process in which SO was appointed, mainly because of its lowest quotation. LAS were criticised for not identifying many gaps in the development, implementation, and training, which would have been evident from assessing the rival and more expensive tenders from more experienced software houses.

Procurement

Inquiry Feb 1993 para 3032 "We recommend that standing financial instructions should be extended to provide more qualitative guidance for future major IT procurements."

Inquiry Feb 1993 para 3042 "Throughout the procurement phase it was clear that LAS management had a proposed budget in mind, for the complete system of around £1,500,000. There does not appear to be any rational process by which this figure was established, although it is possible that it was based on misunderstanding the original Arthur Andersen estimate (which was for a packaged system and excluded the Automatic Vehicle Location system elements)."

Inquiry Feb 1993 para 3010 "In the autumn of 1990, the previous attempt to computerise the LAS Command and Control system was abandoned after load testing revealed that it would not cope with the level of demand. The funding of this system was of the order of £7.5 million."

Inquiry Feb 1993 para 3051 "Thus a contractor and an arguably unsuitably qualified systems manager (who knew that he was to be replaced and made redundant) were put in charge of procurement of an extremely complex and high risk computer system with no additional technical expertise available to them. This added to the high risk nature of the project. "

Good practice suggests that there needs to be some independent audit of the procurement items as a validation process, otherwise a supplier operates from a privileged position with a writ to write the specification to suit himself.

Original Project Authorisation

Now we need to discuss why so many computerised systems, both mission critical and others, fail to achieve implementation or perform well below the expectations of their patrons. Some business forces naturally make life difficult for the designer. In good practice it is often stated that there are naturally 11 main stages in a systems project, starting with the feasibility study and concluding with a post systems audit. (See Erskine 1991). And that naturally takes time, the cycle development time. An information system is normally positioned to achieve a specific purpose which adds value to an organisation, but oh dear, during that development period, the need may change. The organisation may be taken over or reorganised, or management may adopt a different set of objectives and strategies, so some re-positioning is required before the system is effective. There is obviously a need to design really fast to minimise the disruptive effect which re-positioning will have, without cutting corners in the design disciplines, so that quality assurance is not compromised. There are two compromises which are really bad news.

Two unacceptable compromises

The first is to avoid the first step and not have a feasibility study at all! A good feasibility study will require

data and commitment from two sources. Firstly, the users themselves need to identify the expected added value if they get the system. This requires some involvement through the user management structure down to those on the front line of the business, and is the basis for making people think about doing things differently, and brings them to discuss how the technology can be strategically positioned for their maximum benefit. Secondly, there will be the professional involvement of the providers of the system who will be expected to make judgements about time and cost of providing the system. If you put that data together you have the basis of an economic evaluation and a cashflow, and a calculation about NPV. Those who participate can then be made accountable for getting the added value later when the system is implemented. Establishing this link of accountability is the key to getting 'ownership' to move to the user. Unfortunately, for many organisations top management just assumes that the system is a 'good thing', and there is no accountability link through lower levels of management to reap the harvest if the system is introduced. If we have the involvement of those who have made predictions about expected added value then those same people can be looked to for commitment to the validation process, to ensure that the detail in the rules and policies of the system are practical. When we look at case studies a common observation is that it is obvious from early stages that there never would be a NPV from computerisation, yet top management still progressed the project.

Under good practice there should be three green lights looked for before positive authorisation is given. Firstly, the project under scrutiny should be technically feasible and a better solution than an alternative manual solution. Secondly, the project should have enough NPV from the economic evaluation that it has a priority against other projects which are competing for resources. In other words, the project is really worth doing. Lastly, line management, who are going to benefit from the project will need to assess in broad terms how much change will be involved in the organisation to develop and implement this system, and will need to be prepared to accept the pain of change involved in completing the project. This is a difficult assessment to make and line management might need some prompting from external sources to make a correct judgement. If the three green lights are all positive then we have a project which is likely to be viable. If any of the lights are amber or not flickering at all then the project is a high risk one. Notice, however, the limited role an external consultancy could play in the feasibility study, as it is the positive action of the users in this process which is the crucial part. If the external consultants attempt to do too much of what is the user's function you still have a high risk of rejection of the system later, and of course no natural base for the validation process. Who else but the users can take responsibility for the rules of business logic which are written into the computerised

system? The downside of all this is that the user organisation must bear the time and cost of the validation process. It just cannot be delegated outside. It does require considerable resourcing with able and representative people from within the user organisation. You will note above how LAS omitted to give sufficient resourcing to their project and this was partly blamed for the resulting failure.

The second unacceptable compromise is to fail to maintain role separation between analysts and programmers. If the separation is there then it is viable to work on the basis of documentation which is specification based. Without separation it is very tempting to postpone documentation till after implementation, but by that time the staff have probably been re-assigned and all we are left with is the program code which is unintelligible to users and probably even to other programmers and analysts. The excuse is that time pressures are so great that documentation is less important than results and can be done afterwards anyway! Beware of that one! If there is any staff movement during this development phase the partially completed work might have to start again from scratch. Anyway, systems relying on post documentation are generally very difficult to re-position, so the life span of the system is reduced rather than enhanced. The occupational role commonly seen in the industry of programmer / analyst is very open to abuse. The basic groundrule within any project team is that there is separation of the activities of specification, programming, and validation. That does not mean that a programmer may never do analysis work or vice versa, but that the one person should not do both activities in the same part of the project. We have already seen that the analyst has to have work validated by a user representative for viability.

Profile for successful project team

In complex projects one difficulty is that there are many user stakeholders, so validation is not done by an individual but by a group of users, some of whom may be in conflict with one another. That is very much the typical situation in the design of a factory scheduling system, where the computerised scheduling rules will need to take account of the customer waiting for goods, versus the factory manager wanting good plant and labour utilisation, versus the accountant, who wants the minimum stock levels for high profit. Validation in this environment will take the form of the analysts 'walking through' their specifications with the users with prototype design, till positive approval is given. At the head of any good project team will be a 'project champion', who has the communication skills and organisational powers to get the team to make good validation judgements, and the clout to ensure that internal resourcing is sound, and the control skills to ensure that role separation is maintained between specification, validation and

programming. Lastly for project viability we need sound management of the operations function. They will set up and maintain the networks, the scheduling and crewing the computer, making and testing the disaster recovery plan, ensuring security within the computer facility, and the adoption of password systems and back-up facilities. Figure 1 is a model illustrating the role of the Project Champion in this scheme of organisation.

Short cuts with packages (?)

Today it is fashionable to buy computerised packages, so that you do not need to have large teams doing original design. So how does the model for project management work in this environment? Unfortunately, the user validators still have to validate the package, otherwise it might be doing all the wrong things in the targeted environment and we would be left with the problems of passing ownership! So there is no short cut there of validator activity. Don't fall into the trap of avoiding the feasibility study just because there is a package on offer. Validators are likely, however, to be assisted in this task by analysts who have the communication skills to interpret the package specifications in 'walking through' procedures with the validators, but the three green light system is still just as relevant as with original design. If the package does not fit the environment, then some changes will need to be made to the environment, or some changes will need to be made to the package. The rules about role separation of team members vis as vis specification, validation and programming will apply to the package maintenance and change, just as they apply in original design. The 'project champion' will need to be just that bit more articulate in securing resources for the validation activity, which management might be tempted to overlook as being too costly. But, oh dear, industry is littered with examples of packages bought and never implemented, and suppliers who make profit both on package sale and the subsequent rescue from chaos! When will patrons ever get satisfaction from their investment in computerised systems?

Notes and observations on Taurus

In the final section of this paper a brief selection of quotations are reviewed from some recent articles covering the hopes and collapse of Taurus, one of the most ambitious computer projects ever undertaken in Britain.

Going late after 8 years

From Laurie 1992, "Despite the now legendary delays, the UK's paperless settlement system - transfer and automatic registration of uncertified stock - now seems on track for April 1993. John Watson, project director of the London Stock Exchange's Taurus scheme, takes most of the credit for the turnaround. He was able to take Taurus off the drawing board,

where it had been for 8 years, and persuade people that it really was going to happen. Although Watson is correct in regarding the first 8 years as a waste of time his own management of the project has been marred by over-optimism and lapses of judgement that have sent it sharply off-course. ... The 11 months Watson has allowed for testing will be the most critical period for the credibility of both Taurus and Watson."

Did Watson indeed have a profile of successful 'project champion' able to reconcile the requirements of the different stakeholders? Had a serious effort ever been made to expose the proposals to a process of validation?

Hopes and aims and risks of Taurus

From Dunham, May 1991, "The aims of Taurus (transfer and automated registration of uncertificated stock) are: 1. to make the UK's system for transfer of securities and their settlement fully competitive with other leading international stock markets, and 2. to reduce the costs of dealing both for institutions and private investors. Taurus is not just a settlement system; it will also enable investors to enjoy the cost and risk reductions associated with the book entry transfer of their market purchases and sales while remaining members of the company. This dramatic change will obviously have a major effect on investors, particularly when combined with the introduction of rolling 5-day settlement of bargains instead of the present method of settling one week after the end of each stock exchange account. There is some fear that Taurus could be used as an excuse to impose charges for services that are currently free, and there is concern about the potential problems of computer fraud."

This was a system aimed at reducing the costs of dealing! This was a system which would change the core role of its participants. No wonder it would be difficult to steer through a validation process without a very high profile project champion.

Collapse after £400 million

From Economist March 13th 1993, "Taurus is the paperless share-settlement system that the London Stock Exchange has been struggling for a decade to develop. It has suffered a series of delays and cost overruns, and on March 11th 1993, Peter Rawlins, chief executive of the stock exchange, recommended to the ruling board that the £400 million project be scrapped. Market participants had begun testing Taurus in January. Outside experts who reviewed the system during testing concluded that the project would take another couple of years, would take much more money to implement, and would even then be 2nd-rate. Rawlins, who had pushed ahead with Taurus in the face of others'

growing skepticism, has quit. The fault lies in a fundamental lack of consensus about what a modern stock exchange is for."

How could a computerised system possibly be developed for an institution and clients whose role and mode of operation was still evolving from the traumas of 'big bang'?

Bad news for chief executive

From Economist, March 20th 1993, "The London Stock Exchange scrapped Taurus, its planned share settlement system on March 11th, 1993. Taurus would have replaced the shuffling of 6 kinds of paper among 3 places over 2 weeks - which is how transactions in shares are settled in London - with a computerized system able to settle trades in 3 days. Its failure after 6 years of work and spending of perhaps £400 million led to the not entirely voluntary departure of the exchange's chief executive, Peter Rawlins. ... There are plenty of technical explanations for what went wrong, but the real failure was managerial, both at the exchange and among member firms."

Taurus simply was not the environment in which a 'project champion' could raise a standard and hope for success. There seems very little evidence of a feasibility study for Taurus with three green lights flashing for the authorisation decision. No wonder it was a very high risk venture.

Viability audits

Now, some generalisations. When a large project is managed through the project champion framework, i.e. with macro quality assurance uppermost, you could say the project is progressing through a 'window of viability' and its monitoring could be given the process label of a 'viability audit'. Alternatively the project is risky. When the project brings a requirement for the people to adapt to a new culture, then the organisation development activity for the people must precede the 'go-live' milestone. It is very risky to assume that the computer system itself can be the catalyst of change. It may equally generate attitudes of hostility and rejection. A profile of a successfully completed project is one with a long and useful life cycle giving continuous added value, and with a structure capable of re-positioning in light of experience and new priorities. For the computer industry to become productive and deliver, as a matter of course, implemented computerised systems it needs to confront the mega problem of macro quality assurance. The widespread introduction of 'viability audits' would be a giant step in that direction.

Avon Ambulance Service

(A summary from the Sunday Times, Jim Costello, 19th September 1993). "While the London Ambulance Service was having

its crisis Avon was quietly refining and developing a computer assisted dispatch system itself with its new trust status organisation. But their development approach was much more professional. Their software house, RDH, got fully involved with ambulance crews during the design so that crews could have uninterrupted meal breaks unless there were a super emergency. The computer system was tested in parallel for three months and after one month the ambulance staff wanted the new system. Rushton, Chief Executive, stated, 'Since the system went operational our performance audits have produced very positive results and a workforce which continually asks more from it'. "

Clearly, a lot more attention was paid to the process of validation at Avon than in LAS, and a greater thought paid to giving the operators better information for exercising their discretion, rather than having the computer system trying to take over.

Conclusion

This paper has discussed particular problems with mission critical systems, and more general macro problems of quality assurance and life cycle viability of computerised systems. A simple model, (Figure 1), is offered, based on experience and good practice from the literature, to strengthen the quality of project management and introduce a new type of monitoring, the viability audit.

BIBLIOGRAPHY

Dunham, Robin, 'Countdown to Taurus', *Accountancy (ACE) Vol: 107, Iss: 1173, May 1991 p:107.*

Costello, Jim, 'Software that can save lives', *The Sunday Times, p5 from Business Computing Section,* 19th September 1993.

Economist, (ECT),*'What is a stock exchange for?',* Vol:326, iss: 7802, March 13th 1993, p: (UK 119), anonymous

Economist, (ECT), *'Finance: When the bull turned',* Vol:326, Iss: 7803, March 20th, 1993, anonymous.

Erskine, Robert, *Business Management,* Prentice-Hall, 1991

Laurie, Samantha, 'He who rides a Tiger', *Banker (BKR) Vol 142 Iss 792, Feb 1992, p: 36 - 38*

Report of the Inquiry into the London Ambulance Service, February 1993, ISBN 0 905133 70 6, Commissioned by South West Thames Regional Health Authority, 40 Eastbourne Terrace, London W2 3QR

ACKNOWLEDGEMENT

The author would like gratefully to acknowledge the contribution to this paper from Dr. Helen White, PhD, for her assistance in gathering secondary data.

FIGURE 1

FRAMEWORK FOR MICRO QUALITY ASSURANCE

IN PROJECT MANAGEMENT