Software Forensics Centre Technical Report TR 2002-01

At last a silver lining around the troubled NATS Air Traffic Control System.

May 2002

Ordered File from John Donaldson on NATS 1999 onwards in Chronological order as at 25th May 2002, with a few items and a theoretical framework from Robert Erskine.

Abstract

This is a working pamphlet initially written for sharing research data and offering interpretations about the troubled NATS air traffic control system, a classic computer runaway. The pamphlet begins with 26 papers down loaded from the internet since 1999 to get a profile of this system and its development history, ending in May 2002 with a five hour failure, and mass cancellation of flights. The pamphlet offers a tentative diagnosis of the system's development process, offers remedies to its problems as perceived, and offers a blueprint for a possible profitable future. This assumes investment and some innovative reforms to the system itself and more broadly the regulation regime of Britain intended to promote safety and viable IT project development.

Interpretations from Robert Erskine

Stabs at best practice IT Project Management

The literature on computer disaster is very extensive. For large projects 30% end up as 'runaways', see Robert Glass, (1998). On the face of it the NATS system being years late in delivery and £ millions over budget is probably a classic 'runaway', but with a tolerant owner, (HMG), and nowhere else to go, it did reach implementation in January 2002. As there has been no enquiry available in the public domain an explanation of its features of delivery late and over budget must be a matter of speculation. But what an analyst can do is sketch out a brief model of 'best practice IT management', and then review the evidence from the NATS material which is in the public domain to home in on few key areas of supposedly obvious mismatch with best practice. That should help us understand the particular dynamics of this important case study and perhaps offer a pathway for future management and development. The criteria used now of 'best practice' comes from focussed extracts from Erskine, Robert, (2002).

The strength of the *'Silver Bullet'* is that its base lies in the real analysis and diagnosis of many spectacular failures of IT delivery in the public sector and then the finding of a pattern which links that failure. This is simple in the extreme. It finds failure in the provider / client relationship, which is primarily a cultural one, as it is quite easy from experience of successful IT projects to define a 'best practice approach.'

A common weakness in 'runaways' is lack of expertise in the project owner role, the business champion, so that the provider gets only loose specifications, and becomes uncontrollable. The business project champion needs the clout to reconcile 'turf war' between competing owner stakeholders, for without that reconciliation the 'techies' in provider teams with have a field day at project owner expense!

The second vital role is a presence in the development team of a technical project champion, the one who is aware of the different technologies in hardware and software and capable of ensuring that the architecture which links the various interfaces has a consistency.

Next we need a few simple rules of development stemming from the original feasibility study. For a green light for funding an IT project should pass the following criteria:

(1) The project needs to establish NPV, based on project owner's expectation of benefit.

(2) The outputs of the project need to be clearly super-user friendly to employees, managers, maintenance staff.

(3) The project needs security, back-up, appropriate to threats of downtime or failure. (In a mission critical system where failure offers a life threatening scenario, this is a very demanding criteria).

The difficulty is to find an implementation process. But, Eureka, Italian Professor Ambriola of the University of Pisa, in 1997, running with a mandate from Premier Amato, sets up an INDEPENDENT AUTHORITY to monitor Public Sector IT contracts against milestones and quality assurance criteria. Projects have to be registered as a pre-condition of funding, so only well considered proposals get put forward. If significant variances are found during regular monitoring, they either have to be sorted out quickly, or the project is abandoned before consuming any more resources. The abort trigger comes as soon as there is no longer any NPV in the project. This is a brilliant mechanism, as there is a force of obligation to best practice which overcomes the cultural problem of the provider / client relationship. This is a model which is transferable to any public sector IT contract in the world. To use the model successfully the public sector department owning the IT contract needs to grow substantial competence in the 'project owner' role so that he / she has enough clout to resolve local' turf war' and give the provider a clear mandate for the IT system. If there is weakness in that mandate then the provider may disappear to some ivory tower and then fail at the point of implementation. Project owner and provider need to maintain continuous exchanges to keep the architecture of the project consistent.

Financial Implications of NATS

The NATS development project cost £623 million in development, so it was a particular target for government to recoup some of this money by a partial privatisation. Opponents of the sale have argued that safety may be compromised if the organisation is owned by a private shareholder or shareholders. Others argue that the NATS service is in desperate need of more investment, which a new owner would bring. Chancellor Brown, and Minister, Byers, went ahead in this partial privatisation expecting to recoup £500 million for the partial sale of NATS. In the deal completed in 2001 the Banks put together £1.46 billion of debt. They were Abbey National, Barclays Capital, Halifax Bank of Scotland and Bank of America. And the equity capital (£1.63 billion in total), was 49% government, 46% an Airline Group, and the remaining 5% taken up by NATS employees. The Airline Groups' motivation was primarily to have a lever over safety, rather than an expectation of profit. EasyJet soon was considering writing off its £7m investment in NATS when the industry had to grapple with a financial crisis owing to a downturn in air travel post September 11th. However, the Airline Group had substantial expectations as they made the investment commitment, and initially forecast that NATS would make a £60m profit in the year to the end of March 2002; in fact it made a loss of £80m in that period. It had been budgeting for 10 per cent growth in transatlantic traffic, but revenue is 11 per cent down on 2001, according to NATS officials. The company receives 44 per cent of its income from north Atlantic flights.

The original government inspired business plan proposed for NATS expected cuts in charges in real terms by 4% in 2003 and by 5% in both 2004 and 2005 and to raise a further £1 billion in development capital up till 2011, hiking the capacity of British Air Traffic Control from the current 2 million landings / year to 3 million.

But these financial aspirations for NATS soon went pear shaped. STEPHEN BYERS, the Transport Secretary, in February 2002 faced fresh criticisms of his performance after it emerged that the Government had agreed a £60 million emergency deal to protect the privatised air traffic control system from financial failure. One suspects that the Banks owning the £1.46 billion debt were prepared to put NATS into administration unless Government gave essential support.

Another interesting feature of the privatisation agreement was that NATS would not be liable for airline losses through air traffic control failures. On 17th May 2002 NATS was down for 5 hours and BA alone cancelled 64 flights. A rule of thumb calculation of costs would be 200 passengers @ £200 / ticket @ 64 flights, giving a grand total of £2.56 million losses in one day to the luckless BA! In the end it is the

passengers who absorb the shock in more expensive fares. This is rather an interesting manifestation of what the Tories call the 'Labour stealth taxes'!

Chancellor Brown's supposed cash cow at NATS with partial privatisation and a golden egg of £500 million looks a bit pear shaped 9 months on from his controversial deal. With the holders of debt holding a potential administration trump card which got an immediate £60 millions loan, and with operating profits turning into substantial losses, and cost of getting a dodgy computer system to work increasing, not decreasing, one wonders where the city gluttons for punishment investors are going to come from for the planned £1 billion investment by 2011. Perhaps, Chancellor Brown lives in some happy make believe world as far as NATS is concerned, where it would be a wonderful cash-cow reducing vital PSBR!

It looks that under 'best practice' there was no real attempt to use any project criteria of NPV from 1992, as it would have come to an early graveyard years ago! But as there has to be a system for air traffic control in Britain, it is understandable that the project was allowed to runaway. As the role of the air traffic controller is so well defined it should not have been difficult for the NATS' project owner to clear out the 'turf war' among owner stakeholders.

Safety aspects

Under the modern principles of Corporate Governance developed in recent years in Britain by heavyweights like Sir Aidrian Cadbury there should be a 'separation of powers' among corporate stakeholders. In the case of transport this clearly means a separation between ownership and safety regulation. If the relationship between company line management and the regulators is a 'crony' one then safety will be compromised. Only a few years ago the Alpha Pipa platform blew up and the relevant government department was heavily criticised in the ensuing enquiry for not having a corridor in the ministry between those responsible for development and those responsible for regulation. But in NATS no such corridor exists. CAA are the regulators and they own and manage NATS. A former Managing Director of NATS, Sir Roy McNulty, is now Chairman of CAA! In this file of cuttings there are several instances of comments made by the owners, CAA, about the high quality and reliability of the software of NATS. If they were independent they could not make such statements! On 23rd May controllers were reported as being so bold as to complain of safety implications when they were working with screens which were so fuzzy that they confused Glasgow with Cardiff, and also height data. But for a 'buddy' system of air traffic control colleagues, who could recognise the error there could have been a nasty accident. Yet CAA did not even acknowledge this serious complaint. In recent memory a rail crash was caused when a train went through a red signal, a signal that had clocked up no less than 5 recent previous incidents of SPAD, without being investigated and re-positioned. The result was severe loss of life. How close this fatal incident is to the one of fuzziness in the traffic controller's screen. How could the CAA be so wantonly soporific? Regulation should mean regulation, not complacency.

Criteria (2) and (3) above stemming from the feasibility study of best practice covering super-user friendliness and safety, look really pear shaped in this case study of NATS. Not much robustness if reliance has to be on a 'buddy system'; incredible, the reaction of CAA. They really do need to go back to 'school'!

Technical aspects of NATS development.

This data file reveals that the NATS system was developed with three different providers. In the period 1992 - 1994 IBM was the developer. The report suggests that those working on this project were new to Air Traffic Control systems, and were eventually replaced by provider two, Loral 1994 to 1996. But they too could not complete the project so made way for Lockheed Martin, 1996 - 2002, who are still going strong. The system was complicated and had to interface with various legacy systems. Lockheed Martin found an average of 15 errors / 1,000 lines of code, which seems to be a poor base of quality. Initially the Lockheed Martin packages worked well on a base of 30 workstations, but scaling up to 150 work stations was too much for a system with too many bugs not cleared.

There are still modifications in the process of being introduced in May 2002, after 450,000 hours of testing 2 million lines of code. Since the system went live in January 2002 here have been five breakdowns in Air Traffic Control systems all causing flight delays and cancellations; the five hours of May 18th prompted an airline spokesman to criticise the go live date of January, before proof of

reliability. It may be recalled that when London Ambulance went live on its planned date with 80 known bugs unresolved and no back-up facility, it lasted just four days before complete collapse!

More vulnerable was the role and operation of the 'technical project champion' for reconciliation of the different technologies. In NATS' system there were so many legacy systems from the 1970s for interfacing, it must have been a nightmare, and it looks as though the three providers could not provide the champion with the required expertise and clout for insisting on best practise.

However, there must be deep unease in May 2002 at the continuing interface with legacy systems on hardware of the 1970s, now long since out of production. That is really running on a wing and a prayer. To have indulged this link with such old legacy systems at the go live date in January 2002 is incredible. Today the top priority of getting stability into NATS must be to replace such old and seemingly unmaintainable legacy systems.

Office of Government Commerce

In February 2001 the OGC announced that it was biting the bullet of failed IT projects from the public sector and introducing a five step process for analysis and monitoring IT projects, and with a deployment of 300 experts, as project owners to get viability into projects, via 'A Gateway Review Process'. (This process is rather a watered down version of the Erskine 'Silver Bullet.') Of course, the NATS system had been developed from 1992, so none of that best practice approach had been applied. In hindsight it looks as though the 'project owner' role of NATS in direction of the three providers must have left a lot to be desired - otherwise why the slippage in 6 years to the delivery date and a development expenditure of a very substantial £630 million at the Swanwick Centre. The suspicion must be that much of the coding was not done to the best of industry standards, and this finds bugs difficult to find and eliminate, and enhancements difficult to bolt on. The expectation that running costs will reduce in the future is an optimistic scenario. More likely as enhancements bring more complexity costs will go up.

Tandem running for confidence

As breakdowns are horrendously expensive, and also life threatening, it would make good sense to duplicate the system in hardware and software. As modifications were introduced, old and new versions would run in tandem till the new version had properly bedded in. In the disaster recovery case study of Cathay Pacific, the second data centre in Kowloon went on-line when there was a fire in the main centre of Hong Kong, and for 15 days the auxiliary centre kept the airline in business. This duplication for NATS would be cheap weighed against costs of disruption or accident. I'm sorry, Chancellor Brown, but a few more £ millions of investment are essential for getting viability and confidence into NATS.

Reform of Regulation in Britain

Within the last year I have identified severe shortcomings in regulation and offered front bench spokesmen in Parliament a new mechanism to establish properly effective regulation. Above I was complaining about the 'crony' relationship between CAA and NATS, so that whistle-blowing over unreadable screens got no response; similarly at Potter's Bar the contractor who recognised 'dodgy points' found whistle-blowing to own line management got no response; nor did the Enron employees who whistle-blew to boss Lay that the partnership deals were flawed, get anywhere. When the Church of England Commissioners went on a spending spree with Commercial property deals a crony auditor, in this case establishment National Audit Office, indulged the failure of the Church Commissioners to consolidate the accounts of 37 property development subsidiaries with the Principal, and with this cover-up there was a £ 5 billion under performance over 10 years. This was an Enron look-alike from 10 years previously! The common mechanism for responding to these safety / financial disasters is a whistle-blowing system. I have recommended since 2000, (Erskine 2000), the setting up of a national INDEPENDENT AUTHORITY under supervision of a judge to become the antennae of whistle-blowers, for subsequent collection of abuse data with intervention down the chain to the relevant regulatory bodies. With that mechanism the abuse could not be forgotten and serious cases such as the points at Potter's Bar, the broken rails at Hatfield, or the confusing air traffic control screens at NATS would have to be investigated at once. With transparency and accountability forced on the regulatory community itself we could all expect to live in a safer Britain. The proposed new mechanism would also protect the whistle-

blower from subsequent discrimination at work. Now we need to follow the Cadbury principles of separation of powers in Corporate Governance and apply this to reform of regulation. As a first step in this reform CAA should surrender its present regulatory role over NATS to a new independent body with new staff , which would be dedicated to NATS. With two layers of independent regulation in place we ought to feel safe travelling by air. With this antennae in place the media would no longer be directly involved, to the comfort of the potential whistle-blower, whose job is currently protected by law, but possible discrimination in promotion is as yet unprotected.

A silver lining for NATS ?

There were CAA quotes in this set of readings that NATS was the most advanced Traffic Control system in the world. (I do find that rather optimistic)! However, if the quality assurance is really there it could be commercialised by being sold around the world under franchise or outright to make a pretty penny, but without best practice securely embedded, there would be no sale! In the airline industry Britain originally had two nationalised airlines, BEA and BOAC. Each had consumed 400 man / years of development of an airline booking system. On rationalisation as BA a further project consuming another 400 man / years of effort was expended to reconcile the demands of both long haul and short haul operation and after this 1,200 man / years of development the system became a 'profit centre' in its own right and was widely sold throughout the world.

Bibliography

Erskine, Robert, "*At last a Silver Bullet for IT systems*," Management Books 2002.

Erskine, Robert, *Erskine Agenda*, 2000, Management Books 2000.

Glass, Robert L., '*Software Runaways*', Prentice Hall, 1998.

Sources

[1] THE DAILY TELEGRAPH 1999. Air Traffic Services privatisation to raise £500m By Mary Fagan and Bill Jamieson

[2] THE DAILY TELEGRAPH 22 June 2000. Air traffic computer reliable, say managers By Paul Marston, Transport Correspondent (Filed: 22/06/2000)

[3] Computer Weekly CW360.com Tuesday 23 October 2001. Software "cracks" cast doubt over NATS launch date by Emma Nash

[4] Computer Weekly CW360.com 21st June 2001 NATS shops around for new air traffic control upgrade by Tony Collins (tony.collins@rbi.co.uk)

[5] THE DAILY TELEGRAPH 28 January 2002. Flight delays increase as air traffic centre opens. By Paul Marston (Filed: 28/01/2002)

[6] Fury at Byers bail out for air traffic, Jill Treanor, Patrick Wintour and Keith Harper Wednesday February 20, 2002 The Guardian

[7] THE DAILY TELEGRAPH `February 2002. Byers faces flak over cash for air traffic firm, By Benedict Brogan and Helen Dunne (Filed: 20/02/2002)

[8] Low Graphics Sunday, 24 February, 2002, 17:04 GMT Air traffic bail-out 'not gift'

[9] THE DAILY TELEGRAPH 28 March 2002 Second computer fault delays flights By Paul Marston, Transport Correspondent (Filed: 28/03/2002)

[10] FINANCIAL TIMES 3rd April 2002, NATS rescue package likely to be delayed by Kevin Done, Aerospace Correspondent. Published: April 3 2002 17:58

[11] CNN 10th April 2002 UK air traffic returns to normal. April 10, 2002 Posted: 1618 GMT

[12] Times April 10, 2002 Q&A: air traffic failure

[13] INDEPENDENT 11th April 2002. Computer crash adds to UK's air traffic woes NATS was already facing financial meltdown, now its system is creaking by Barrie Clement, Transport Editor 11 April 2002

[14] INDEPENDENT 11th April 2002. Flights in chaos as 'patched-up' air traffic computer crashes for the second time by Barrie Clement, Transport Editor. 11 April 2002

[15] THE GUARDIAN 10TH April 2002 EasyJet may write off stake in NATS by Andrew Clark on Wednesday April 10, 2002

[16] COMPUTER WEEKLY CW360. 10th April 2002 Air traffic delays as NATS systems fail again, by Cliff Saran

[17] THE DAILY TELEGRAPH 11 April 2002 Flight chaos as air traffic computer crashes again By Paul Marston, Transport Correspondent (Filed: 11/04/2002)

[18] THE TIMES May 18, 2002 Airports in chaos after computer breakdown by Emma Hartley

[19] THE GUARDIAN 18 May 02 Worst breakdown yet of air traffic computer causes flights chaos by Andrew Clark, Saturday May 18, 2002

[20] DAILY TELEGRAPH 18 May 2002. Air Travel Delays to Continue

[21] SkyNews 21 May 2002 Squeeze On Air Traffic Control

[22] The Telegraph 19 May02 NATS warns of more chaos unless charges are put up by Mary Fagan

[23] Times May 23, 2002 New computer glitch threatens air traffic safety By Ben Webster, Transport Correspondent

[24] NEW SCIENTIST - 23 May 02 (New Scientist.com news service) by Will Knight Unclear displays lead to air traffic controller errors

[25] DAILY TELEGRAPH 23 May 02 NATS call to lift air traffic fees rejected by Philip Aldrick

[26] Ananova 1 May 02 http://www.ananova.com/ UK and Irish air traffic controllers consider partnership