WITN05970147

Live Trial Stressing *- A discussion paper*

Purpose

The purpose of this note is to introduce the concept of *"Live Trial Stressing"* of the Horizon service, though the deliberate introduction of sub-optimal or failure scenarios during the Live Trial, to gain maximum leverage and information from the Trial.

This activity would be focused on proving the service during a variety of situations that are likely to affect the overall service during its lifetime but that cannot be guaranteed to occur naturally[1] during the limited duration and scope of the Live Trial. The intention is therefore to improve the coverage and representativeness of the Live Trial, and hence to improve the quality of the decision on which authority for National Roll Out (NRO) would be made.

This activity is intended to de-risk the National Roll Out and should therefore be of benefit to both the Authorities and ICL Pathway, and can been seen as part of a series of on-going de-risking activities.

Background

The ICL Pathway NR2 *system* has been subject to extensive testing by ICL Pathway themselves, and also to testing as part of the wider environment through activities involving the Authorities such as DIT and End to End. The NR2 system is also subject to Model Office Testing, which is designed to prove the operation of the system against the operating procedures within a protected or simulated target environment.

However, the testing within E2E and MOT has been largely 'positive' in nature, generally testing the operation of the system under normal conditions, rather than testing its operation under stress - although some failures are considered, this is not the primary function of this phase. These test phases, although valuable in proving aspects of the system, are patently not representative of the number of outlets, type of staff or operating conditions which will be encountered in National Roll-Out or steady state.

The Live Trial is intended to allow the Authorities a period of time during which a small number of offices (300) can operate within a live environment, to provide evidence that the service is fit for rollout (and to manage any Acceptance events). Although it is likely that a number of *failures* or other *sub-optimal situations* will occur during the Trial period, it would be niaive to assume that this coverage would, if left to its own accord, be adequate to give assurance as to the likely operation across 20,000 offices over a number of years.

The Gap

The Live Trial is effectively the first time that the system will be run as part of the wider *service* - and of course it is this *service* which is the entity being contracted for by the Authorities. Although we may have some confidence in the operation of the *system*, for Horizon to be a success, it the correct operation of the overall *service* which counts.

[1] Or be monitored as occurring

WITN05970147

The point may be best demonstrated by example. There are certain "events" which are detected by the system and should be flagged to Pathway's operation staff. Whilst various stages of testing will have demonstrated that these events will be detected by the system, they have not shown that they will be correctly acted upon in live running, and that the service as a whole is capable to recovering from the specific types of failure. It should be noted that the activities are not confined to ICL Pathway and this "stressing" may well identify shortcomings outwith the ICL Pathway service, eg in the Authorities domains or in cross-domain areas.

It should be noted that the Horizon Programme has been unable to review ICL Pathway's application design, and in particular has not been able to gain full visibility of the performance of the system in abnormal (but real world) failure conditions. Live Trial Stressing can be seen as a means of filling this gap by gaining assurance that the overall service is indeed robust and capable of handling such natural failures. Such stressing would enable the Authorities to gain confidence in the service and ICL Pathway to "shake down" their internal procedures on a manageable number of outlets, before encountering a shortcoming with thousands of outlets live.

Stressing

It is therefore proposed that a certain amount of *controlled* stressing be applied to the Live Trial to ensure that the coverage of the service during this crucial period is adequate to provide a basis on which to authorise Rollout. This stressing would take the form of introducing non-optimal behaviour, representing potential real world events, into the service, to demonstrate that it can cope without loss of data, integrity, availability, security etc.

A number of scenarios are provided purely by example - this list is not intended to be in any way exhaustive or definitive:

- unplanned data centre failover - ensure that the cutover from one data centre to another can be handled within a satisfactory period of time and without loss of service. [This can be considered as proving of Business Continuity plans, but is considered as more representative than the "annual" DR tests which would normally be expected].
- loss of communications to outlets - ensure that the loss is detected and acted upon in a timely fashion. [This could be considered as proving System/Service Management]
- loss of LAN in an office - ensure that the loss is detected and acted upon in a timely fashion. [This could be considered as proving System/Service Management].
- loss of gateway terminal/non-gateway terminal in various states.[This could be considered as proving the System Management and Service organisation and the advice given by Helpdesks]
- loss of batch of cards [This could be considered as proving the relevant helpdesks and processes]
- unpicking a situation where the prescribed procedures have been ignored / wilfully flouted.
- …

Live Service vs Test Environment

WITN05970147

There will naturally be the debate between the introduction of "stress" into the actual live service, and the establishment of a separate, off-line, test environment for the purpose. Although there may be certain tests which may be best performed on a representative test environment, it is not seen as practical to test all of the service in such a sterile manner - in particular the human element is unlikely to be able to be made representative.

It is therefore inevitable that the stressing has to be applied to the live environment. Obviously, any such stressing needs to be performed in a very controlled manner, to avoid undue effect upon the live service - however, the intention would be to simulate only "real world" scenarios which would be expected to occur during live running, from which the service should be able to recover.

Stressing would need to be applied without providing undue warning to the ICL Pathway operational staff, to ensure that the response is representative, although it would advantageous to have the co-operation of ICL Pathway senior management with whom the schedule and timing of such activities could be agreed.

Stressing would only be introduced once the live service has stabilised and once the migration from Release 1c and to the two data centres has been completed. In addition to making this a fairer and more representative test of the service, it avoids the complexity of tracking faults in an unstable environment[2].

Not withstanding the above, it may be pragmatic to introduce pseudo outlets, to all system appearances a real outlet, but without real customers, where more aggressive scenarios may be run. The prospect of pseudo customers (especially in BA terms) is believed to be impractical from prior indications but the boundaries of what could be done need to be established.

Other considerations

There are a number of other aspects of Live Trial Stressing which need to be considered, including:

1. Use of real offices.
   A number of events are going to require access to "real post offices" to allow the simulation of events. This will require the identification of one or more willing and trusted sub-postmasters, who are prepared to be subject to a degree of disturbance and who will not abuse the activity. Any disturbance could be course be spread between a number of offices, to reduce the effect upon individuals - and targeting of those offices by ICL Pathway for 'special attention'.

2. Use of real customers.
   Some scenarios are likely to require the use of "customers", eg holders of benefit payments cards. A number of options exist, from the enrolment of volunteers (an extension of the live proving performed at go-live weekends, potentially using BA or POCL staff who are genuinely in receipt of benefit), to the creation of test beneficiaries *[A BA view on this would be appreciated - it is acknowledged that there may be sensitivity over use of "dummy NINOs" or payment of benefit to a dummy recipient, however it would considerably aid the ability to stress the service - both ICL Pathway handling, BA handling and reconciliation between POCL, BA and ICL Pathway].*

[2] As a consequence the stressing of the outlet migration to Horizon would not be covered.

WITN05970147

3. Management of clients and customers.
   The risk exists, of course, that this stressing could identify a weakness and cause some loss of data or other inconvenience to customers. This is an inevitable consequence of any Live proving activity, however will require careful management (itself a test of the Authorities ability to handle service failure). Any such temporary shortcoming is best exposed at the early stages of interaction with clients and customers where problems can be managed and where the small number of outlets and customers involved be carefully and actively monitored. It may be possible take certain actions to mitigate against potential failure in specific cases of stressing, to avoid impact on sub-postmasters and customers.

Conclusion

This paper has sought to introduce the concept of Live Trial Stressing of the ICL Pathway service, once stabilised, to ensure that it is representative of the service proposed for National Rollout. This has the consequence of de-risking the Rollout for both ICL Pathway, the Authorities and their clients and customers.

The paper is intended to promote debate and to gain agreement in principle to this activity. If the concept is accepted in principle, there will then be a considerable amount of work to be done to define the scope and nature of the stressing process, the ground rules under which it will be done, definition of scenarios etc., and finally to manage this activity.

Jeremy Folkes, 26th Jan 1999