Document Title:	HNG-X Branch Exception Handling Strategy- Agreed Assumptions and Constraints
Document Type:	*Strategy*
Release:	HNG-X
Abstract:	This document presents a summary of the agreed outcome of the analysis on Branch exception handling under HNG-X. It described the strategy with agreed assumptions and constraints, for addressing exception handling in the HNG-X solution.
Document Status:	APPROVED
Author & Dept:	Gareth Jenkins (version 1.1 onwards) Dave Johns (earlier versions)
Internal Distribution:	Distribution to Fujitsu staff as per section 0.3, document review list.
External Distribution:	Distribution to Post Office staff as per section 0.3, document review list.

Approval Authorities:

Name	Role	Signature	Date
Guy Wilkerson	Fujitsu Services Limited		
David Gray	Post Office Limited		

Note: See Post Office Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

@ Copyright Fujitsu Services Ltd 2006 to 2010

0 Document Control

0.1 Table of Contents

@ Copyright Fujitsu Services Ltd 2006 to 2010

@ Copyright Fujitsu Services Ltd 2006 to 2010

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	24/05/2006	First draft with formal document reference for formal review with Post Office as input to the HNG-X contract. It is based on an extract from the SIP working paper on HNG-X Branch Exception Handling. This version replaces previous informal working drafts.	
0.2	06/07/2006	Incorporates review comments. In addition to typographical changes and conversion to the new HNG-X template format, the following sections have been changed: Section 1.0 - clarified that earlier working document does not have contractual significance. Section 3.1 – details added on transaction volumes. Section 3.2 –clarifications on transient failures and counter PC operational throughout the failure. Section 3.3 – clarification that the time to diagnose permanent failures is similar to Horizon. Section 4.0 – clarified the scope of recoverable transactions. Section 4.1 – clarified state change in 3rd party systems. Section 4.2 – clarified when transactions can be cancelled. Section 3.1 – clarified impact on 3rd party systems. Section 4.2 – clarified when transactions can be cancelled. Section 5.1 – clarified why customer session are permitted to continue after a transient failure. Section 5.2.1 – clarified when Cancel option will appear. Section 5.3 – clarified counter PC failures within longer faults. Section 5.3.1 – clarified that Clerk can log at same or a different counter PC after failure. Section 5.3.2 – clarification on recovery process state and who can perform recovery. Section 5.4 – new section on other (non basket settlement) processes. Section 6.0 – wording changed throughout this section to “The HNG-X baseline assumption” and conventions used within the section. Section 6.2 – clarified that the implementation is assumed to be consistent for label printing across all current Postal Services products, and consideration for future flexibility. Section 6.3 – clarified that Postal Orders are treated as all other AP-ADC transactions, and consideration for ability to become recoverable. Section 6.4 – clarified that Clerk dialogue for card payment recovery will be defined during the design phase following detailed requirements definition. Section 6.5 – clarified indicators will be shown when the counter	

		detects a permanent fault in the connection to the data centre, and that the indicator, but will not give the status of individual service availability. Section 6.6 – clarified that decision on disabling of transactions when there is a permanent connection fault, will be made during the design phase following detailed requirements definition. Section 6.7 – clarified that other aspects of the system behaviour whilst offline will be investigated during the design phase. Section 6.8 – previous section removed (as duplicate of material in section 5.3.2). Section 6.8 – new section added on Recovery and Stock Unit balancing. Section 6.9 – new section added on ADC transactions Section 6.10 – new section added on Flexibility between Recoverable & Cancellable Section 7.0 – clarification on hardware faults and removal of duplicate line on average basket existence time. Section 7.4 – clarification that the failure volumes show Horizon and HNG at April 09 position.	
1.0	24/07/07	Submitted for Approval with the following change from version 0.2: Front sheet - Post Office Approval Authority changed to David Gray.	
1.1	27/07/2010	Changes to reflect the implementation. This involves the addition on a new Section 8. Distribution list updated to reflect the current people on the project. No other changes (other than typos) made to the rest of the document. Minor modifications from version 1.1a marked in Violet.	
1.2	22/10/2010	Updates in response to review comments. Changes from version 1.1 marked in red (with ~~strikeout~~ where appropriate) Note that version 1.1 was formally withdrawn following comments from Post Office Ltd.	
2.0	18-Nov-2010	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	Gareth Jenkins & PostOfficeAccountDocumentManagemen GRO
Mandatory Review	
Role	Name
Post Office	Ian Trundell (*)
HNG-X Programme	Alan D'Alvarez (*), Geoff Butts
HNG-X Architect	Amit Apte
HNG-X Infrastructure	Martin Brett
HNG-X Applications	Graham Allen

HNG-X Customer Services	Graham Welsh
Optional Review	
Role	Name
Post Office	Review list* as defined by Ian Trundell
HNG-X Infrastructure	Mark Jarosz
HNG-X Applications	Chris Bailey*
Fujitsu Operations	Ed Ashford
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
HNG-X Commercial	Guy Wilkerson
HNG-X Requirements	Dave Cooke
HNG-X Programme Manager	Mark Andrews
HNG-X Testing	Sheila Bamber
HNG-X Applications	Duncan MacDonald
HNG-X Infrastructure	Jason Clark
HNG-X Customer Services	Steve Parker (†)

(*) = Reviewers that returned comments

(†) = Reviewers that returned no comments

0.4 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
	0.3	03/03/2006	HNG-X Branch Exception Handling working paper	SIP working paper
ARC/SOL/ARC/0001			HNG-X Solution Architecture Outline	PVCS
Schedule B6.1			HNG-X Business Requirements	HNG-X contract

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

N.B. Printed versions of this document are not under change control.

0.5 Abbreviations

Abbreviation	Definition
SIP	Systems Integration Partnership

0.6 Glossary

Term	Definition

0.7 Changes Expected

Changes
None

0.8 Copyright

© Copyright Fujitsu Services Limited 2006 to 2010. All rights reserved. No part of this document may be reproduced, stored or transmitted in any form without the prior written permission of Fujitsu Services.

1 Objectives

To present a summary of the agreed outcome of the analysis on Branch exception handling under HNG-X and the strategy (with agreed assumptions and constraints) for addressing exception handling in the HNG-X solution.

It is intended to use this document as part of the HNG-X contract.

This is a summary document and does not cover all final details of the Branch Exceptions Handling process. This work was completed through the Exceptions Handling workshops. There is a separate working document available on the detailed analysis, which was produced as part of the SIP, including potential impact on Post Office procedures. However, any content within the working document that is not in the assumption and constraints within this CCD document has no significance within the HNG-X contract.

2 Scope

The scope is specifically to provide an overview, prior to contract, of the agreed assumptions and constraints on the Branch Exception Handling process. Further detailed aspects of the process will need to be agreed at a later point.

The assumptions and constraints within this document will be the agreed contractual position and subject to change control during the detailed design phase.

3 Approach/Overall Strategy

Analysis of the availability factors for HNG-X has identified the following categories of exceptions and the estimates of the impact of these exceptions.

- Counter peripheral failures
    - These are largely the same as Horizon, estimated at approximately 1 failure per counter per year.
- Counter PC failures
    - These are largely the same as Horizon, estimated at approximately 0.1 failure per counter position per year that could cause loss of data. Note that Power failure at the branch accounts for 80% of these cases.
- Transient failures (< 2 minutes) impacting online transactions
    - These are reduced for HNG-X (estimated at 6 per counter position per year) compared to Horizon (estimated at 11 per counter position per year).
- Transient failures (< 2 minutes) impacting settlement
    - This is a new exception category for HNG-X that does not apply to Horizon. The estimate is 15 incidents per counter position per year.
- Longer faults (> 2 minutes)
    - These are reduced for HNG-X to an estimated 0.2 per branch per year that impact trading – compared to 0.8 for Horizon, however the impact on HNG-X of these failures is different since HNG-X does not support offline trading.

The first two cases are so similar to Horizon, that they are not considered further within this paper.

Further details will be provided within the detailed sections below.

@ Copyright Fujitsu Services Ltd 2006 to 2010

3.1 Basis of estimates

The analysis work to derive these estimates and the assumptions from which they are derived is available as a separate spreadsheet. The figures are averages over the whole system and do not claim that they will be evenly distributed. For example, certain types of failure will have a larger impact, e.g. on the whole branch, or the whole network in the extreme case where a switch to DR is needed.

The estimates for the incidents and the assumptions behind them are provided as an appendix to this document. Whilst these are the best estimates available for such incidents, Fujitsu Services does not accept any liability for any consequences on Post Office if they turn out to be inaccurate.

The Transaction Volumes used in the estimates are based on January 2006, scaled to a full 12 months. Based on the calculations used in the estimate, changes in actual volumes would result in the following:

- Transient faults would rise in proportion with volume of online transaction.
- Longer term faults are static and independent of transaction volumes

The volumes of other (non basket settlement) processes such as reporting and other administration tasks are very small in proportion to transaction volumes and do not affect the calculations.

3.2 Transient failures

Transient errors are defined as errors within the HNG-X system that are resolved within 2 minutes.

The HNG-X system is designed so that there is no single point of failure, and mechanisms are in place to take over automatically from failing components. During this ‘failover’ process the network connection carrying the online interactions can fail leading to these transient errors. The majority of the failure cases will be resolved well within the 2 minute period, but this figure is chosen since it provides a realistic break point between the transient and (semi) permanent cases.

The counter PC is fully operational throughout the failure.

The impact of these transient failures depends on whether it occurs during an online transaction within a customer session, or at the end of session when the session data is committed to the Branch Database. These cases are treated separately within this paper.

3.3 Longer faults

These are defined as failures that cause outages of longer than 2 minutes for the connection between the counter system and the Data Centre. They can be local to the branch, or have wider impact, including complete loss of the data centre. Typically these failure types will impact all counter positions within a branch.

The counter PC is fully operational throughout the failure.

This category can be further split into failures that clear within a few minutes and those that do not. In the latter case, the system will at some stage detect that the connection with the Data Centre has been permanently lost and will display an appropriate indication on the counter PC. However, due to the nature of the network, it may take up to 20 minutes to diagnose the failure as permanent. This is similar to existing Horizon behaviour.

4 Recoverable and Cancellable transactions

Each transaction will either be recoverable or cancellable once the transaction is written to the session basket.

Some transactions such as Banking may be cancellable up to a certain point in the transaction sequence, and then become recoverable from that point onwards.

The scope of recoverable transactions is limited to sales transactions within a customer session. Cancellable transaction can be cancelled up to the point where the customer session has been settled and the session data has been committed to the data centre. All other transactions modes where a number of transactions are performed offline prior to session commitment are treated as cancellable transactions. This section gives some examples of each type of transaction, but is not intended to be a definitive list of all cases, however, where examples are provided they are definitive for that case.

4.1 Recoverable transactions

This category covers those transactions which communicate with a 3rd party system for authorisation as the transactions proceed. This results in a state change in the 3rd party system and can result in implicit transfer of funds between accounts based on the authorisation. The final outcome of the transaction must be reported, and potentially the transaction reversed with the 3rd party if the outcome is different to the authorisation.

Examples are Banking and ETU transactions.

4.2 Cancellable transactions

This category covers those transactions which can be removed from the session basket after the transaction has completed. They can either be cancelled by the Clerk as part of the customer session, or as a result of post error condition scenarios described later in this document.

Under HNG-X, the set of these transactions is extended to AP (including ADC) transactions. These transactions are not deemed complete until the end of the customer session when the receipts are printed.

Examples are stamp sales, Bureau, AP, AP-ADC.

[Note that Postal Orders are Cancellable rather than Recoverable transactions, even though they can attain an authorised state during the transaction. See section 6.3]

5 Analysis of exception categories

This section covers the exception cases excluding the counter peripheral and PC failure categories.

5.1 Transient failures impacting online transactions

For the purpose of the analysis work on exceptions, we have ignored failures within the 3rd party Client environment and the network interfaces to that Client from the Data Centre (since these are the same as Horizon).

A transient failure that occurs during an online interaction from the counter will result in a timeout at the counter. This will follow the same model as Horizon, e.g. Banking, PAF, DVLA.

Depending on the transaction, it may be possible to continue the transaction offline (e.g. PAF or DVLA). For other transaction types, e.g. Banking, a failure receipt will be printed and the transaction ends. The Clerk can retry the transaction (subject to manual procedures) – but this may involve the customer in further actions such as input of PIN.

These cases are very similar in operation to Horizon. Due to the improved network resilience within HNG-X, the estimated likelihood of failure is almost half that of Horizon.

Note that customer sessions are permitted to continue after transient failures since there is a likelihood that the problem will be recovered prior to either a subsequent on-line transaction or settlement of the customer session.

5.2 Transient failures impacting settlement

This is a new exception case for HNG-X, that does not apply to Horizon.

It is estimated that on average, there will be 15 incidents of this type per counter position per year. In multi-counter branches these failure cases will affect individual counter positions and will not necessarily impact all counter positions at the same time.

The settlement transaction sequence is described below.

5.2.1 Settlement transaction sequence

In general, the end of session transaction will be completed within 1 second.

The counter system will be designed to cover transient failures. It will do this by retrying the session settlement transaction a number of times:

1. The system will wait for a timeout period when writing the session data to the Branch Database. The timeout value will be set at around 30 seconds[1].
2. On timeout, the system will perform an automatic retry using the same timeout value.
3. On subsequent failure, the Clerk will be provided with the ability to "Retry" writing the session data. The system will perform the same two steps as described above, i.e. an initial attempt to write the session data followed by an automatic retry (if needed) – both with 30 second timeouts.
4. After failure of a Clerk initiated retry sequence (step 3), the Clerk manual Retry screen will be displayed again. This screen will also have a "Cancel" option. Use of the "Cancel" option will cause the system to follow the Cancelled Session process. See section 5.3.1. Use of the retry option will repeat step 3.

[1] The 30 second value is currently used for Horizon on-line transactions. The precise value for the Settlement timeout value will be defined during the design phase. The value chosen will balance the operational issues on longer timeouts against the probability that a re-attempt is likely to succeed during transient failure cases. The value will be configurable, but is likely to be the order of 30 seconds.

5. The impact of transient failures is to delay the settlement transaction. If the problem is cleared within 30 seconds, then the first (automatic) retry will enable the customer session to be completed. If the problem is cleared within 60 / 90 seconds, the manual retry from the Clerk (plus automatic system retry if needed) will also enable the customer session to be completed.

The system will clearly indicate that the Clerk needs to wait, and will manage the retry. The Clerk will be invited to retry after the first two failures, and can at that point abandon the session if the customer does not wish to proceed – but will be warned that there will be a forced logoff if that path is taken.

This is a new process for Branch staff, but the system will clearly lead the staff through the process.

5.3 Longer faults

This category covers faults which persist for longer than 2 minutes. Longer faults may result in one or more failures of online transactions before the longer fault becomes apparent at session settlement. However, for the purposes of this paper, this case will only be examined in the context of the settlement transaction.

The Settlement process will follow the model described in section 5.2.1. It will finally result in the Clerk taking the “Cancel” option. This will enter a recovery process that will be designed against the following high level assumptions:

1. The system will lead the Clerk through the failure sequence.
2. Recoverable transactions must be settled based on the basket data.
3. Cancellable transactions will be voided from the session basket.
4. The system will err in customer’s favour when outcome uncertain.

It is estimated that on average, there will be 0.2 incidents of this type per branch per year, but when it occurs, it is most likely to impact all counter positions within the branch.

The process to handle cancelled sessions is described in section 5.3.1. Throughout this failure mode, the counter PC is fully operational. The recovery process that will be followed subsequently is described in section 5.3.2.

The cancelled session process (section 5.3.1) does not apply when the counter PC fails before the session data is committed to the Branch Database. This can occur prior to attempting to settle the session, or during the session settlement transaction sequence and includes power loss as well as hard failure of the counter PC. In this case the recovery process sequence described in section 5.3.2 will apply when the counter PC is next used – potentially after hardware replacement. Note that the system automatically detects that an earlier session has failed based on data held centrally – not on the counter PC.

5.3.1 Cancelled sessions

At the point that the session is Cancelled by the Clerk, the outcome of the session within the Branch Database is uncertain. Whilst it is unlikely, it is possible that the session data has actually been committed.

1. The Counter system will at this point lead the Clerk through the exception process.
2. The system will indicate which transactions are recoverable and must be settled as per the basket details, and those transactions which will be cancelled by the system.
3. A revised basket total will be calculated.

4. The counter system will print a special “Recovery Receipt” that will be used later. This “receipt” will contain details of the session as finally settled, plus sections on recoverable and cancelled transactions.
5. The system will also record some details of this failure on the counter PC (e.g. presence of recovered or cancelled transactions), but will not store any transaction data on the counter PC disc.
6. The system will print any customer receipts that are needed, potentially including void receipts for cancelled transactions if required.
7. Finally, the Clerk will be logged off the system – even if the data centre system is not available.
8. The Clerk would be able to attempt to log on at either the same or a different counter position. Recovery of the failed session is described in section 5.3.2.

5.3.2 Recovery

Recovery will be counter position based – as for current Banking and APS recovery in Horizon. It will occur at the first successful logon by authorised branch staff to the counter position after failure.

It will proceed under the username of the currently logged on user (not necessarily the original user), but will be posted to the original Stock Unit. The recovery process cannot be deferred.

The outline of the recovery process is as follows:

1. On first logon to the failing counter, the system will detect that the last logon session did not close tidily. This will invoke the recovery process.
    - The system will automatically detect whether there are any transactions that need to be recovered.
    - In most cases, the counter PC will still be operational, and will contain some state data (but not transaction data) that can be used to simplify the recovery process.
    - In the case where a PC has been replaced or rebooted after the longer fault occurred, the system will detect this. It will ask the user whether a Recovery Receipt was produced prior to failure. If so, the recovery receipt will be used to obtain the equivalent state data – this will be encoded within a barcode on the receipt.
2. In either case, during the recovery process, the system may prompt the Clerk to respond on the outcome of the failing session based on information in the recovery receipt.
    - If the session data was not committed, the system will prompt for the outcome of any recoverable transactions.
    - If the session data had been committed, the system would reverse out the cancellable transactions, leaving the Branch Database in the state indicated to the Clerk at the point of failure.
3. During this process, the system may detect transactions which cannot be reversed.
    - For example, AP transaction cannot be reversed after EOD, since the original AP transaction data could already have been sent to the Client.
    - There may also be some transactions which cannot be reversed automatically – e.g. an AP Reversal.
    - These exceptions would need to be handled by manual processes, some of which are already in place.

The recovery process state will be maintained within the branch database. This ensures that the process cannot be avoided through abandonment and cannot be inadvertently done twice.

Note that outstanding recovery of a session on one counter position does not prevent the Clerk from logging on to a different counter position.

If / when the original Clerk logs on later at a different counter position – the system will detect that the previous session did not end cleanly and can provide suitable warning that recovery is needed, but the recovery process will need to be performed at the original counter position and cannot be initiated from another counter position. The Clerk will also be informed if the recovery process has already been completed by another user.

Only authorised branch staff logging on to the counter PC will cause the recovery process to be initiated. It will not be initiated by an engineer log on.

5.4 Other (non basket settlement) processes

This section covers other non basket settlement processes, such as reporting and other administration tasks.

In general, these follow the same model as online transactions, where the request can be retried later.

In cases where the request updated data within the branch database, the user would be able to view the results if in doubt prior to attempting the request, or would receive an error (e.g. duplicate user name) if the previous request had been committed.

Functions such as viewing messages would potentially re-display the status of a message as new, even though it had already been viewed

It is assumed that all the functions that are performed within this category can be retried if in doubt after a failure, and that the system will return an error if a duplicate arises. Details will be developed during the design phase following detailed requirements definition.

6 Related Points

These refer to lower levels of detail below the high level approach to exceptions described in this paper.

The list below, once agreed between Post Office and Fujitsu, will become the accepted position within the contract on these specific areas.

Conventions used within this section:

- The phrase “the HNG-X baseline assumption” means that the implementation described is assumed within the Target Price.
- The phrase “the decision will be made during the design phase” means that the feature described will be implemented within the Target Price according to the agreed method which will be decided during the design phase.
- The phrase “consideration will be given during the design phase” means that the design of the feature will be considered within the design phase, but does not necessarily imply that the feature can be implemented within HNG-X without additional cost, and if required would need to handled via the Change Control Procedure.

6.1 ETU

The HNG-X solution adopted the previous proposal from HNG to move ETU transactions into the session settlement transaction. This gives rise to significant complications in the exceptions cases that can arise, in particular when there is a card payment.

1. The HNG-X baseline assumption is that ETU transactions will revert to the Horizon model where the online authorisation is performed prior to settlement.

6.2 Mails labels

Postal Services transactions where labels are produced, cause significant operational problems if the transaction has to be cancelled, for example the label is highly likely to be already stuck on the mail item when the problem is detected at settlement.

There is a separate requirement to be able to write an audit record to prevent fraudulent printing of labels.

Post Office have indicated a strong preference that Postal Services transactions which result in a printed label, be classified as recoverable rather than cancellable. This means that the system must write recovery data with an audit record during the customer session.

1. The HNG-X baseline assumption is that mails labels can be implemented as either recoverable or cancellable transactions. The decision will be made during the design phase following detailed requirements definition. The HNG-X baseline assumption is that the implementation will be consistent for label printing across all current Postal Services products. Consideration will be given during the design phase to provide flexibility in this area, for example to vary recoverable / cancellable by Postal Service products.

6.3 Postal Orders

Postal Order transactions are AP-ADC transactions, and hence are cancellable transactions under the currently proposed model.

For the Sell to Customer case, the voucher / value is registered with the central system as an online transaction. The voucher is printed during the session, but will not be handed to the customer if the session cannot be committed. Whilst the inability to sell a voucher that has already been printed will be inconvenient to the customer, the customer will not be out of pocket.

The Buy from Customer case is different. There is an online transaction to confirm that the voucher is valid, and the voucher is implicitly marked as encashed as part of this online transaction. If the transaction were to be cancelled at this point, the voucher would need to be returned to the customer. However, this voucher would not be accepted as valid until the central record had been changed via the administration interface. This would require a manual process to be invoked.

An alternative is to make the Buy Postal Order transaction recoverable, with the recovery data written as part of the online transaction.

1. The HNG-X baseline assumption is that all AP-ADC transactions are cancellable transactions, which implies that Postal Orders are cancellable rather than recoverable transactions. Consideration will be given during the design phase on the potential ability to make the Buy Postal Order transaction recoverable, with the recovery data written as part of the online transaction.

6.4 Card payments

The card payment interface with Streamline is based on an explicit payment file record that is generated from the session settlement record. The customer receipt is part of the Session receipt.

In theory, card payment transactions could be cancelled at any point up to committing the session data and a void receipt printed. A reversal would be generated to remove the ring fence on the customer's funds. However, a zero value transaction would be recorded by the system.

In the case where the session cannot be committed, then it is possible that transactions will be cancelled that were being settled by card payment, e.g. stamps or DVLA licence. However, it is also possible that there is a recoverable postal services transaction in the session. It would therefore be difficult for the system to automatically recover the transaction, hence the Clerk would need to be prompted on the actual outcome of the session.

1. The HNG-X baseline assumption is that the Horizon model will be retained, where card payments are recoverable rather than cancellable transactions. The precise Clerk dialogue in the settlement failure and subsequent recovery process will be defined during the design phase following detailed requirements definition.

6.5 Indicators

There will be a single indicator provided as part of the HNG-X solution. It will be shown when the counter detects a permanent fault in the connection to the data centre. The indicator will not give the status of individual service availability – e.g. Banking.

Due to the nature of the network, the system will need to work through a number of cycles and retries before it can declare the connection permanently unavailable. It is important to prevent false alerting of failures in the process. However, this process could take up to 20 minutes to recognise a permanent network fault, though some types of fault may be quicker to diagnose. This is similar to the current Offline Indicator on Horizon.

The availability of the Backup network for HNG-X means that the likelihood of such failures is significantly less than with Horizon.

1. The HNG-X baseline assumption is that an equivalent indicator to the Horizon offline indicator will be provided for HNG-X.

6.6 Stopping further transactions when no connection

On Horizon, certain products are inhibited when the offline indicator is displayed. However, not all transactions with online components are disabled or check the indicator.

With the potential impact on session settlement when the system is offline, it may be advisable to prevent further transactions being attempted once the indicator is displayed. However, due to the potential 20 minute delay in setting the indicator, it might be seen as of little additional value since most sessions would have been completed by then and the Clerk logged off.

1. The HNG-X baseline assumption is that the decision will be made during the design phase following detailed requirements definition, on the disabling of transactions when the system detects that the connection has been lost.

6.7 Trading while offline

The HNG-X system does not support offline trading.

Post Office will be responsible for defining manual procedures to cover the case where all counter PCs in a branch are offline.

1. Other aspects of the system behaviour whilst offline will be investigated during the design phase, for example will the system prevent the user from attempting to log on whilst offline. The HNG-X baseline assumption is that there is no system support for offline trading. The decision will be made during the design phase following detailed requirements definition, on other aspects of the system behaviour whilst offline.

6.8 Recovery and Stock Unit balancing

There is the potential for the Stock Unit to be balanced at another counter position (by the same or a different Clerk) before the original failed session has been recovered. The current technical assumption is that the system will perform in the same way as Horizon, and there will be no interlock between the recovery process and Stock Unit balancing. Indeed in some cases, the system may not be aware that a failure has occurred on another PC. The volume of such failures indicates that any impact is likely to be low.

1. The HNG-X baseline assumption is that there will be no interlocks between recovery and Stock Unit balancing. The decision will be made during the design phase on the display during the balancing process of any additional advisory messages that recovery action might be outstanding.

6.9 ADC transactions

Potentially, there could be a some types of ADC transactions that need to be recoverable rather than cancellable once they have reached a specific stage within the transaction sequence, or have completed and been added to the basket. This would need to be under reference data control, potentially via a new ADC data type to record the recovery data within the data centre.

1. The HNG-X baseline assumption is that all AP-ADC transactions are cancellable transactions. Consideration will be given during the design phase on the provision of an additional ADC step to make an ADC transaction recoverable. This would be subject to overall HNG-X transaction volume constraints and could require different variants of the ADC sequence for Horizon and HNG-X to be managed by POL during the Branch Migration period.

6.10 Flexibility between Recoverable & Cancellable

Potentially, there may be a need over time to change individual transaction types between cancellable and recoverable, so that they are not fixed forever based on the initial HNG-X implementation. Any such changes would need to take account of the operational impact, e.g. longer transactions times.

1. The HNG-X baseline assumption is as described in this document above. Consideration will be given during the design phase on how flexibility could be provided to change individual transaction types between cancellable and recoverable. Individual changes would be implemented under change control and would be subject to overall HNG-X transaction volume constraints.

7 Appendix A – Assumption used in the estimates

This section contains estimates on the number of failures that will result in exceptions that need to be dealt with by branch staff.

The data is derived from the data used by Fujitsu Services for "SLT availability" calculations, which is separately available on request. This analysis is based on the best data available, but actual characteristics may vary.

The numbers are presented as the average number of events per counter position per year. Both Horizon and HNG-X estimates are provided to allow a comparison to be made. A number of different types of failures are looked at.

The assumptions made in the analysis are:

- Failures are spread evenly over the 24 hour day (since hardware faults can happen at any time including the middle of the night).
- Covers fixed branch analysis only - mobile branches are excluded
- All HNG-X branches have a backup network installed
- No Horizon branches have a backup network installed
- April 2009 MTBF projections for branch equipment failures
- A Gateway PC is used in Horizon Branches
- A Router used in HNG-X Branches
- Data Centre components fail once per year to their resilient partner
- Data Centre component failover time is 60 seconds (in practice likely to be between 30 seconds and 2 minutes).
- Third party failures (e.g. CAPO, EPAY, Streamline) are excluded from the numbers as no exceptions should be required.
- The average online transaction response time is 2 seconds
- The average basket online response time is 1 second
- The workload is spread evenly over the core day
-
- Average Basket Existence Time is 60 seconds (measured as first item on stack to basket settlement). In practice, this number is likely to be on the high side and therefore gives a pessimistic result.
- Horizon Online transaction failure rate is 0.1% (Jan06 data).
- HNG-X Online transaction failure rate is half that of Horizon due to use of SOAP rather than Riposte
- Average basket is 2.7 transactions (1.7 products + 1 settlement record)
- There are 34,000 counters in the estate
- Transaction Volumes are based on January 2006, scaled to a full 12 months.
- This results in the average counter transacting 11,000 online transactions and 28,000 basket settlements per year
- Long duration faults will only result in exception handling if they occur during the core day.

7.1 Peripheral Failures

The table below shows the estimated failures per counter position per year in April 2009 – the point at which the new application is expected to be fully rolled out.

Item	Horizon	HNG-X
Counter Printer	0.63	0.63
Bar Code Reader	0.05	0.05
PIN Pad	0.18	0.18
Keyboard (including card reader)	0.17	0.17
Total	**1.04**	**1.04**

7.2 Transient Faults

The table below shows the estimated average number of transactions per counter per year that are impacted by transient faults (of less than 2 minutes) where a retry should be successful. It is split into online transactions (e.g. banking, debit card, ETU, DVLA authorisations) and basket settlements.

Type	Item	Horizon	HNG-X
Online	Failover from primary to/from secondary network	n/a	0.2
	Central Components	0.4	0.5
	Transient Network Issues	11	5.5
	Total	**11**	**6.2**
Basket	Failover from primary to/from secondary network	n/a	0.2
	Central Components	n/a	0.4
	Transient Network Issues	n/a	14
	Total	**n/a**	**15**
Combined	**Online + Basket**	**11**	**21**

7.3 Longer Faults

The table below shows the estimated average faults per counter per year that will result in longer faults (more than 2 minutes) where the counter still has the data.

Item	Horizon	HNG-X
Complete loss of branch network	2.00	0.20
Router failure	n/a	0.04
Gateway PC failure	0.16	n/a
Significant Data Centre failure	0.50	0.50
Total	**2.66**	**0.74**

These faults will only result in exception handling if they occur during the working day (if the occur at night no transactions are in progress). Due to the time to detect such faults, it is assumed that faults during the day result in an impact. The table below shows the estimated number of such faults per counter position per year:

Item	Horizon	HNG-X
Complete loss of branch network	0.62	0.06
Router failure	n/a	0.01
Gateway PC failure	0.05	n/a
Significant Data Centre failure	0.16	0.16
Total	**0.83**	**0.23**

@ Copyright Fujitsu Services Ltd 2006 to 2010

7.4 Loss of Basket Transaction Data held in PC Memory

This is an estimate of where basket transaction data is held in the PC memory (e.g. before a basket is settled) and there is a failure that results in loss of that data.

The estimated number of failures per counter per year is shown below. These failure rates show the April 09 position for both Horizon and HNG-X.

Failure Type	Horizon	HNG-X
PC Failure	0.16	0.11
Screen Failure	0.10	0.10
Power Cut	1.62	1.62
Total	**1.89**	**1.83**

However only a small number of these will result in data being lost as most of the time, there is no basket in progress. The number of failures that result in a lost basket per counter per year is estimated as:

Failure Type	Horizon	HNG-X
PC Failure	0.009	0.006
Screen Failure	0.005	0.005
Power Cut	0.086	0.086
Total	**0.100**	**0.097**

8 Appendix B - Implementation Detail

Following the implementation of HNG-X a number of changes have been identified from the original Assumptions and Constraints described in this document. These are highlighted in this section referring back to the part of the document in which they are described.

1. Section 3: Other causes for failures have been identified and now need to be considered in this document. These are:

   a. Double Log Ons. This is where a User Logs on at a new terminal without Logging off at the original terminal. The system assumes that this is due to the original sessions having failed, but analysis of current behaviour indicates that this is often not the case.

   b. User reboots of a counter. It is difficult to ascertain exactly when or why this occurs, but it is believed that this is often due to a software error resulting in an apparent freeze of the counter application.

Any such freezes are due to defects which need to be investigated in their own right.

2. Section 3: Current experience indicates that the number of Transient Failures has not improved from Horizon. Also it should be noted that a Transient Failure is defined as one of 2 mins or less. There are some scenarios where if Users do not follow the process correctly they could be Logged Out as a result of a Transient Failure (see point 5 below).

3. Section 4.2: The statement at the end of the section about Postal Orders being cancellable is not correct. As a result of introducing MoneyGram into the HNG-X Contract it was realised that some AP-ADC transactions would need to be Recoverable and so a mechanism has been introduced to allow any AP-ADC script to make a transaction recoverable. Post Office Ltd has exploited this facility in the Postal Orders AP-ADC scripts.

4. Section 5.1: See point 2 above regarding Network Improvements.

5. Section 5.2.1 point 3: What has been implemented does not distinguish between the first manual retry and any subsequent manual retry. In all cases the User is given the option to Cancel as an alternative to Retrying. A consequence of this is that if the User does Cancel when first invited to Cancel or Retry, they could be logged out even if it is a Transient Failure.

6. Section 5.3.1 point 4: What has been implemented here is the production of 3 copies of a "Disconnected Session Receipt". This consists of an entry for every item that was originally in the basket. However any Cancellable Transactions are amended to show a value and quantity of zero (indicating that they have been cancelled).

7. Section 5.3.1 point 5: No details of the failure are stored on the counter PC. All that is held is the last successful Session Id to assist with the recovery process.

8. Section 5.3.2 point 1 3rd bullet: No bar code is produced. All that is required for recovery is a Recovery Code which can be easily keyed in if the counter has been replaced. (Where the counter has not been replaced, then this is held on the hard disk and so nothing needs to be keyed in by the User.)

9. Section 5.3.2 penultimate paragraph: Text for such messages are under Post Office Ltd's control. However it is understood that they are not currently as explicit as described here. This may be one of the reasons that the number of Double Log Ons (see point 0 above) is quite high.

10. Section 5.4: In order to protect the integrity of the Audit Trail, it is necessary to have the same behaviour as has been described for Settlement, whenever an auditable message is written to the Branch Database. In general, this means any interaction which will result in an update to BRDB other than where the update is purely to Recovery Data.

11. Section 6.2: It has been agreed that Mails Labels transactions would not be recoverable. However an Audit record is secured to the Data Centre before printing any mails label, thus providing an audit trail if the system is misused when processing mails labels
12. Section 6.3: As mentioned in point 3 above, a mechanism has been provided to make AP-ADC transactions recoverable. It is understood that Post Office Ltd have exploited this feature in their Postal Order transactions.
13. Section 6.4: Card Payment transactions are Recoverable. In addition, logic has been introduced to provide a whole or partial refund if some of the items covered by the card payment are cancelled as a result of a failure.
14. Section 6.5: Given the online nature of HNG-X and the time taken to decide that the communications network is permanently unavailable, it is assumed that the User would have been "forced to Log Out" as a result of a failure to settle a basket by the time the Network is considered to be permanently unavailable. This means that there is **no** indicator visible while the User is Logged On. However once the User has Logged off (either explicitly or as the result of a Forced Log Off due to repeated timeouts), there will be a visible indication as to whether the comms is considered to be available or not, thus enabling the User to see when it is reasonable to attempt to Log On again.
15. Section 6.6: As described in point 14 above, if the User is still Logged On, then the comms are assumed to be working. Therefore there is no concept of inhibiting transactions due to unavailability of comms.
16. Section 6.7: As part of the Log On functionality, an option is available to invoke a cut down version of the Engineering menu as an alternative to Logging On. This allows an Engineer to investigate problems such as comms connectivity issues without needing to access the Data Centre. Since such functionality is outside the control of Log On, this functionality is available to anybody who has physical access to the terminal.
17. Section 6.8: An interlock has been implemented such that a Stock Unit cannot be Balanced until any failed sessions belonging to Users who were attached to that Stock Unit at the time the sessions failed, have been recovered.
18. Section 6.9: As mentioned in point 3 above, a mechanism has been provided to make AP-ADC transactions recoverable.
19. Section 6.10: There is limited flexibility:
    a. All Transactions involving Online Banking, E-Top Up and Debit / Credit Card Payments become recoverable when the [R1] authorisation request is sent to the Data Centre
    b. All Reversal baskets (for both Existing and New Reversals) become recoverable immediately prior to the final settlement
    c. AP-ADC transactions become **may** become recoverable if specific commands are executed in the scripts. This therefore, is the only aspect of Recovery that is under the direct control of Post Office Ltd.
20. Section 7: It is now felt that the average existence time for a basket is likely to be more than 60 seconds. However this is not thought to be significant.

8.1 Recovery Targets

During the pilot and rollout of HNG-X, there has been extensive monitoring of the number of Recovery Log Ons that have taken place.

This shows the following:

1. Over 90% of Recovery Log Ons result in "No Recovery Required"
2. The number of baskets which do not result in Recovery being invoked at the next Log On is over 99.4%
3. Between 25% and 40% of Recovery Log Ons are due to the "Double Log On" issue based on a sample of data taken during July 2010 mid rollout
4. The rest are either due to two or more successive timeouts or a counter restart.

These figures will continue during Live operation and should be considered to be the ongoing target.