WITN11070106

Document Title:	HNG-X Counter Architecture
Document Reference:	ARC/APP/ARC/0003
Release:	HNG-X
Abstract:	This document focuses on the hardware and software components that constitute the HNG-X Post Office Counter, and the interactions between them. This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager.
Document Status:	APPROVED
Author & Dept:	Andy Thomas, HNG-X Architecture Team
External Distribution:	
Security Risk Assessment Confirmed	YES, security risks have been assessed, see section 0.9 for details.

Approval Authorities:

Name	Role	Signature	Date
David Court	Programme Manager		
Amit Apte	Chief Technology Officer		

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

Documents are uncontrolled if printed or distributed electronically. Please refer to the Document Library or to Document Management for the current status of a document.

WITN11070106

0 Document Control

0.1 Table of Contents

WITN11070106

WITN11070106

0.2 Figures and Tables

WITN11070106

0.3 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	28-Oct-2006	Initial Version	
0.2	07-Nov-2006	Draft for preliminary review.	
0.3	23-Nov-2006	Draft for review.	
0.4	31-Jan-2007	Updated to reflect comments.	
1.0	31-Jan-2007	Released for approval.	
1.1	27-Nov-2007	New revision to satisfy End-to-End Group Review process.	
1.2	02-Jan-2008	Changes arising from End-to-End Group Review.	
1.3	09-Apr-2008	Updated to reflect comments. Updated reviewers / approvers from current reviewer matrix.	
1.4	15-Apr-2008	This document has been revised by RMGA Document Management on behalf of the Acceptance Manager to contain notes which have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. This text must not be changed without authority from the FS Acceptance Manager. These changes will not require full review using the RMGA Document Control Process, as agreed between Acceptance Manager and Programme Management. Added at V1.4 - Footnote 1 added to section 2.3 which comprises text that has been identified to POL as evidence to support Acceptance by Document review (DR) for Requirement ARC-432. Added at V1.4 - Footnote 2 added to section 7.6 which comprises text that has been identified to POL as evidence to support Acceptance by Document review (DR) for Requirement ARC-437.	
1.5	29-May-2008	Added description of Utimaco VPN to architecture. De-scoped migration to Windows XP. Updated branch router related content. Added migration changes to display settings. Updated SSL related packages. Added PHU 2.0 mobile counter to architecture. Removed the use of print service devices for connection of the back office printer.	CP4549 CP4472 CP4523, CP4543 N/A CP4622 CP4405 TBA
1.6	24-Jul-2008	Footnotes added by RMGA Document Control at V1.4 (above) removed and a table containing the same information inserted as Section 0.5 Acceptance by Document Review. Added to table in Section 0.5 Acceptance by Document Review section 2.5.2.6 which comprises text that has been identified to POL as evidence to support Acceptance by Document review (DR) for Requirement ARC-430. Updated to reflect V1.5 review comments.	
~~2.0~~	~~23-Sep-2008~~	~~Released for approval.~~	

WITN11070106

2.1	28-Oct-2008	• Version 2.0 withdrawn and version 2.1 introduced with 'Changes Expected' and design notes as a result of feedback following the request for approval. • Fixed document numbering errors.	
2.2	25-Nov-2008	• Updates to Spares Strategy (3.2); the document referenced (DES/INF/HLD/0001) has not yet been formally reviewed, but will contain this content. • Updated 2.5.2.11 to reflect the fact that legacy devices will not be disabled, merely unused and not present on new spares. • Added to table in Section 0.5 Acceptance by Document Review section 7.2 which comprises text that has been indentified to POL as evidence to support Acceptance by Document Review (DR) for requirement SEC-3308. • Added Appendix A, containing UML Model. • Added reference to CNIM LLD.	
2.3	01-Dec-2008	Additional line in table in 0.5 for SEC-3243 / SEC-3308 / 6.6 / Encryption.	
2.4	11-Feb-2009	• Changed touch screen resolution from 32-bit to 16-bit. • Removed Steve Godson from reviewer list at his request. • Split SSH server & Cygwin tools into separate products. • Added section *Manageability – Remote Support*. • Added NetworkQoS component to architecture. • Added use of SDELETE to securely delete data during migration.	HNG-X CP 0312 (4831)
2.5	23-Feb-2009	• Minor changes following review.	
3.0	16-Jun-2009	• Document Approved	
3.1	5th Aug 2011	• Document reviewed/updated after Release 5.0	
4.0	19-Aug-2011	Version for approval	

WITN11070106

0.4 Review Details

Review Comments by :	
Review Comments to :	
Role	**Name**
Solution Design / Development	Tariq Arain
Infrastructure Design	Alex Kemp
Head of Service Introduction	Role unfilled
CISO	Ian Howard
Information Governance	Bill Membery
Capacity & Configuration Manager	Mark Brosnan
Optional Review	
Role	**Name**
Security & Risk Team	CSPOA.Security GRO
Architect	Jason Clark
Network Architect	Mark Jarosz
Test Design	Sheila Bamber
Service Network	Andrew Hemingway
Head of Service Management	Tony Atkinson
LST Manager	Mark Ascott
SV&I Manager	Chris Maving
POL Test Manager	James Brett (POL, JTT)
VI & TE Manager	Not applicable
Testing Manager	Debbie Richardson
SSC	Steve Parker
Business Continuity	Adam Parker
Head of Service Support	Sarah Bull
Infrastructure Delivery Manager	Martin Brett
Integration Team Manager	Vijesh Pandya
Programme Manager	David Court
Integrity Testing	Not applicable
Operational Security	Donna Munro
Core Division	Ed Ashford
Core Division	Andrew Gibson
CTO	Amit Apte
Lead Architect Systems / Estate Management	Ian Bowen
POL Design Authority	Ian Trundell (POL, via RMGA Document Management)
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	**Name**
Acceptance Manager	David Cooke

WITN11070106

0.5 Acceptance by Document Review

The sections in this document that have been identified to POL as comprising evidence to support Acceptance by Document review (DR) are listed below for the relevant Requirements:

POL NFR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
ARC-430	ARC-481	2.5.2.6	Report Printer (PH500.05)
ARC-432	ARC-482	2.3	Node Description
ARC-437	ARC-484	7.6	Network Failure
SEC-3114	SEC-3272	6.3	Security: Windows Hardening
SEC-3118	SEC-3273	9.17.4	Migration: HNG-X Application Pilot and Rollout: Post-Installation
SEC-3199	SEC-3295	6	Security
SEC-3211	SEC-3299	2.5.3.1.2	Windows NT 4.0 Lockdown (PS500.32)
SEC-3211	SEC-3299	6	Security
SEC-3228	SEC-3228	6	Security
SEC-3228	SEC-3228	6.3	Security: Windows Hardening
SEC-3243	SEC-3308	7.2	Counter Hardware Failure
SEC-3243	SEC-3308	6.7	Encryption

0.6 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	1.0	13-JUN-06	Fujitsu Services RMGA HNG-X Document Template	Dimensions
ARC/GEN/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Architecture Document Template	Dimensions
PGM/DCM/ION/0001	44.0	12-FEB-09	HNG-X Document Reviewer & Approver Role Matrix	Dimensions
ARC/APP/ARC/0001			HNG-X Reference Data Architecture	Dimensions
ARC/APP/ARC/0009			HNG-X Counter Business Applications Architecture	Dimensions
ARC/GEN/REP/0001			HNG-X Glossary	Dimensions
ARC/MIG/STG/0001			HNG-X Migration Strategy	Dimensions
ARC/NET/ARC/0001			HNG-X Network Architecture	Dimensions
ARC/NET/ARC/0003			HNG-X Branch Router Topic Architecture	Dimensions
ARC/PER/ARC/0001			HNG-X System Qualities Architecture	Dimensions
ARC/PPS/ARC/0001			HNG-X Platforms and Storage Architecture	Dimensions
ARC/SEC/ARC/0003			HNG-X Security Architecture	Dimensions
ARC/SOL/ARC/0001			HNG-X Solution Architecture Outline	Dimensions
ARC/SVC/ARC/0001			HNG-X Support Services Architecture	Dimensions
ARC/SYM/ARC/0001			HNG-X System and Estate Management	Dimensions

WITN11070106

			Architecture	
ARC/SOL/ARC/0005			HNG-X Counter Training Offices Architecture	Dimensions
REQ/CUS/STG/0002	1.0		HNG-X Branch Exception Handling Strategy-Agreed Assumptions and Constraints	Dimensions
TST/GEN/STG/0004			HNG-X Testing Strategy	Dimensions
DES/MIG/HLD/0001			HNG-X Migration High Level Design for Branches	Dimensions
DES/APP/HLD/0057			HNG-X Counter Infrastructure: Service And Process Control High Level Design	Dimensions
DES/PPS/PPD/0016			HNG-X Counter Physical Platform Design	Dimensions
DES/PPS/PPD/0127			HNG-X Mobile Counter Physical Platform Design	Dimensions
AS/DPR/031	1.0	10-OCT-06	Counter Printer Replacement Design Proposal	PVCS
AS/DPR/032			Counter Printer Speed Change Proposal	PVCS
BP/DES/003	9.2	28-FEB-06	Counter Hardware Design Specification	PVCS
SD/DES/236	2.0	10-AUG-04	Counter Physical Platform Design	PVCS
SD/SPE/016			Horizon OPS Menu Hierarchy	PVCS
CP4259			Epson Counter Printer Rollout	
CP4260			Epson Firmware & Logo Download Support	
CP4266			Printer Replacement Programme	
CP4273			Counter Printer Com Port Speed Change	
CP4305			PCI Compliance	
CP4405 (HNG-X CP0022)			Migration of PHU1.5 Portable Counter to HNG-X	
CP4472 (HNG-X CP0041)			XP Counter Descoping *(CP CLOSED)*	
CP4523 (HNG-X CP0077)			Definition of Branch Router Migration Strategy	
CP4543 (HNG-X CP0094)			Branch Router Topic Architecture	
CP4549 (HNG-X CP0098)			Retention of Utimaco VPN - Development and Operational Impacts	
CP4622 (HNG-X CP0156)			PPD Changes for Key management	
CP4831 (HNG-X CP0312)			Provide QoS data from counter though CasQoS extension instead of CNIM	
DES/NET/HLD/0013			HNG-X Time Synchronisation High Level Design	Dimensions
DES/APP/HLD/0096			HNG-X Training System High Level Design	Dimensions
DES/APP/HLD/0057			HNG-X Counter Infrastructure Service & Process Control High Level Design	Dimensions
DES/SYM/HLD/0012			SDAM Horizon Support High Level Design	Dimensions

WITN11070106

ARC/SYM/DPR/0002			HNG-X Estate Management Component Delta Changes	Dimensions
ARC/SOL/ARC/0005			HNG-X Counter Training Offices Architecture	Dimensions
DES/SYM/HLD/0017			Remote Support High Level Design	Dimensions
DES/SYM/HLD/0038			Counter AutoConfig High Level Design	Dimensions
DES/SYM/HLD/0035			HNG-X End To End Software Release & Delivery	Dimensions
IMP/GEN/SPE/0001			TS650P (Pilum Hybrid) Hardware Specification	Dimensions
DES/MIG/HLD/0005			Estate Management Migration High Level Design	Dimensions
DES/MIG/HLD/0006			VPN on HNG-X NT High Level Design	Dimensions
DES/SYM/HLD/0002			MON – Supporting Agents	Dimensions
DES/SYM/HLD/0007			SYSMAN-HYDRA Support High Level Design	Dimensions
DES/INF/HLD/0001			Spares Strategy For Horizon And HNG-X Migration	Dimensions
DES/APP/HLD/0125			HNG-X NetworkQoS High Level Design	Dimensions
DEV/APP/LLD/0084			CNIM Low Level Design	Dimensions

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

0.7 Abbreviations

Abbreviation	Definition
ADSL	Asymmetric Digital Subscriber Line
BIOS	Basic Input / Output System
CA	Certificate Authority
CAS	Counter Application Scheduler
CNIM	Counter Network Information Manager
COTS	Commercial Off The Shelf
CTO	Counter Training Office
DOLT	DN: TODO
DMZ	Demilitarized Zone
GB	Gigabyte
GNU	GNU's Not Unix
HNG-X	Horizon Next Generation – Plan X
IBM	International Business Machines
ID	Identity
ISDN	Integrated Services Digital Network
J2EE	Java 2 Platform, Enterprise Edition
JVM	Java Virtual Machine

WITN11070106

LAN	Local Area Network
MCG	Multi Counter Gateway
NST	Network Service Type
OBC	Operational Business Change
PC	Personal Computer
PHU	Portable Hardware Unit
PIN	Personal Identification Number
POLO	Postmaster Logon
POS	Point of Sale
RAM	Random Access Memory
QoS	Quality of Service
SAM	Security Accounts Manager
SAS	Secure Access Server
SCO	Single Counter Office
SOLT	DN: TODO
SRS	System Requirements Specification
SSH	Secure Shell
SSL	Secure Sockets Layer
TEC	Tivoli Enterprise Console
TLG	An bitmap image format
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
XML	Extensible Mark-up Language

0.8 Glossary

See also HNG-X Glossary (ARC/GEN/REP/0001).

Term	Definition
Counter Id	Each counter in the branch is assigned a unique identifier, the Counter Id. The former Horizon gateway counter will always have the lowest Counter Id.
GNU	GNU is an open source implementation of Unix. Many commonly used tools such as patch, diff, zip, unzip, etc may be obtained with a GNU licence, allowing these tools to be used and distributed without the need to purchase licences.
VSAT	Very Small Aperture Terminal's offer two way satellite communications between a ground station and geostationary satellites.

0.9 Changes Expected

WITN11070106

Changes
If approved, Change Proposals regarding the introduction of new hardware for branch counters will require this document be updated. If approved, Change Proposals regarding the migration from Windows NT 4.0 Workstation to an alternative operating system will require this document to be updated.

0.10 Security Risk Assessment

No identified security risks.

WITN11070106

1 Introduction

1.1 Overview

This document defines the infrastructure architecture for the Post Office counter in the HNG-X solution.

This section of the document explains the background to the HNG-X programme, the document context and scope. The notation is also explained, and key assumptions are identified.

1.2 Background

Post Office Ltd operates in both the retail and financial services industries. The main channel to market for Post Office is a network of approximately 14,000 branches with volumes of up to 28 million customers per week. In addition, Post Office has been expanding the use of the Internet and Call Centres as part of a comprehensive multi-channel strategy.

The objective of the HNG-X programme is to develop a system with structural and operational characteristics that substantially reduce ongoing support and maintenance costs with respect to the current Horizon system.

The overall requirement is that the business capabilities offered by the current system (Horizon) are preserved in the new system (HNG-X). However, a limited number of business capabilities will be revised based on a joint optimisation of business requirements and system properties.

The analysis of the serviceability profile for Horizon has highlighted data management as one of the most significant drivers for cost. The storage of transactional data within counters causes the need for security mechanisms that impact both the structural complexity and the operational performance of the counter applications. In addition, the presence of sensitive data on the counter increases the time, complexity, and ultimately the cost of maintenance procedures.

The HNG-X solution is based on a Business Application that supports a centralised model for data storage. The counters retain operational data (e.g. Reference Data) and business logic, but transactional information is stored directly in the Data Centre.

The counter side of the new applications is based principally on Java technology. The counter hardware is reused from Horizon with the initial migration deploying the new application on the existing Windows NT 4.0 operating system.

Where it has been feasible to reuse components from the existing Horizon counter, these have been carried forward into HNG-X, and these will be indicated in the section of this document entitled Physical View (section 2.5).

Following completion of the HNG-X Release 1 migration, a subsequent operating system upgrade to Windows XP or another operating system may be undertaken.

1.3 Context

Three types of HNG-X architecture document exist:

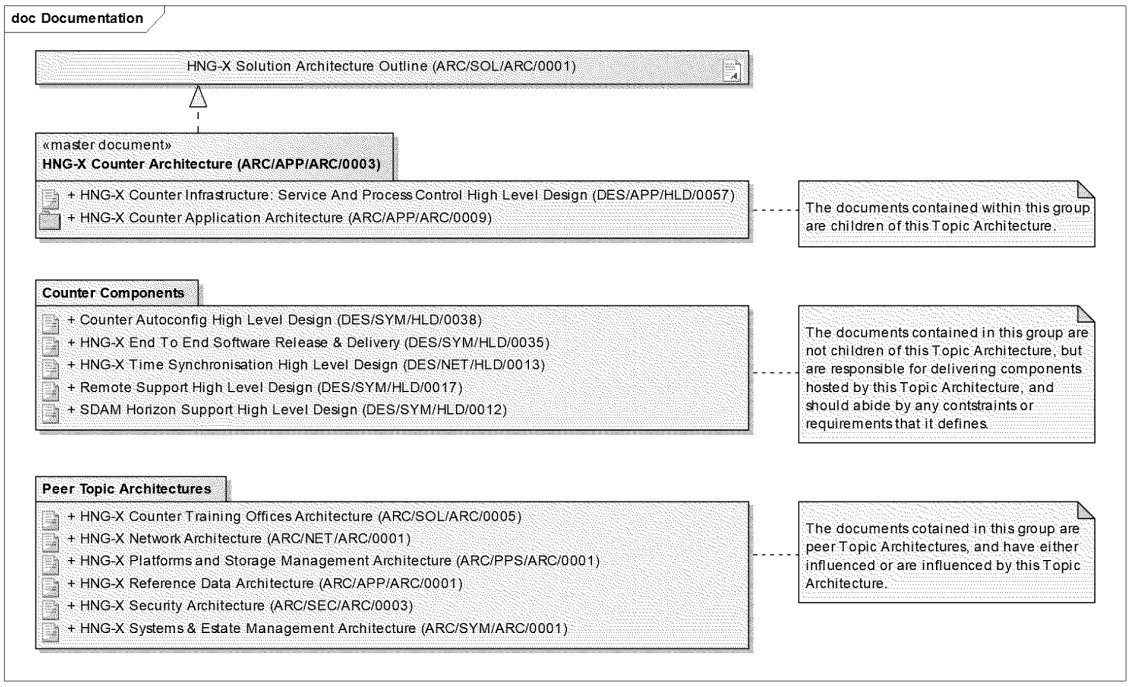
- The **Overall Solution Architecture** is the top-level description of the HNGX solution, identifying the individual Topic Architectures.
- A **Topic Architecture** is the first level of decomposition of the Overall Solution Architecture. Topic Architectures include Applications, Platforms, Networking, System Management, Security, System Management, Recovery and Resilience.

WITN11070106

- Where a Topic Architecture is complex, then a further decomposition into individual **Component Architectures** may be required. For example the System Management topic architecture could constitute Software Distribution, Monitoring, Remote Access and Diagnosis and Time Synchronisation component architectures. Component Architectures identify the scope for their associated High Level Designs.

This document is the overall **Topic Architecture** for the **HNG-X Counter**, and is derived from the outline architecture described in *HNG-X Solution Architecture Outline (ARC/SOL/ARC/0001)*, and will be used as input into the subsequent High Level Designs.

This document is closely associated with the document *HNG-X Counter Business Applications Architecture (ARC/APP/ARC/0009)* which describes the architecture for business applications running on the counter.



1.4 Scope

This document describes the various types of Branch Counter and any hardware peripherals directly attached to the counter.

The final migration of the counter to Windows XP is out of scope in Release 1 of HNG-X.

The Branch Router, all network attached devices in the branch (eg. network hubs, switches, etc), and all other nodes in the architecture are out of scope for this document.

PHU 1.0 and “luggable” counters (DOLT & SOLT) are being phased out prior to the introduction of HNG-X, and being replaced with the PHU 1.5 mobile counter. Under the HNG-X programme, the PHU 1.5 mobile counter will be migrated to the PHU 2.0 mobile counter. This document describes the target architecture, and hence descriptions of the PHU 1.0 and PHU 1.5 are out of scope. The migration activities associated with the introduction of the PHU 2.0 are covered in section 9, Migration.

WITN11070106

The requirements appertaining to counters used in Counter Training Offices is out of the scope of this document. For further information, see the *HNG-X Counter Training Offices Architecture (ARC/SOL/ARC/0005)*.

WITN11070106

2 Architecture Description

2.1 Overview

This section briefly describes the HNG-X Counter node, and then decomposes it into its constituent components.

This decomposition occurs at two levels of abstraction:

1. *Logical* – Where components are discussed in terms of their functionality only.
2. *Physical* – Where components are discussed in terms of the technology used to realise them.

2.2 Notation

Throughout this section, the following notation is used to uniquely identify components:

- "LH*NNN.nn*" for instances of **L**ogical **H**ardware component *nn* associated with platforms with ID "*NNN*".
- "LS*NNN.nn*" for instances of **L**ogical **S**oftware component *nn* on platforms with ID "*NNN*".
- "LD*NNN.nn*" for instances of **L**ogical **D**ata component *nn* on platforms with ID "*NNN*".
- "PH*NNN.nn*" for instances of **P**hysical **H**ardware component *nn* associated with platforms with ID "*NNN*".
- "PS*NNN.nn*" for instances of **P**hysical **S**oftware component *nn* on platforms with ID "*NNN*".
- "PD*NNN.nn*" for instances of **P**hysical **D**ata component *nn* on platforms with ID "*NNN*".

EW500 and NW500 are unique identifiers for the Windows NT and Windows XP-based counters respectively.

2.3 Node Description

The overwhelming majority of Post Office branch staff will need to interact with just one machine in order to perform all of their business transactions. This machine is called the HNG-X "Counter".

It can be deployed in two form factors, suitable for different working environments:

- "Fixed" – This is the most common form factor and the best option wherever there is a permanent Post Office serving location.
- "Portable" – Approximately 500 counters will be portable, so that they can be packed away to be transported to and from temporary serving locations, or locations where physical security is insufficient for them to be left unattended for long periods.

The HNG-X Counter machine is conceptually similar to that of today's Horizon system, but numerous technical changes are necessary for it to operate within the new architecture. These include:

- In contrast to Horizon's proprietary architecture, the HNG-X application architecture is based on a rich Java-client accessing a J2EE web application server via web services.
- All normal business transactions under HNG-X demand connectivity between the branch and the live Data Centre.
- The Horizon concept of "Gateway" and "Slave" Counters does not exist in HNG-X. All HNG-X Counters are created equal, although one "Primary Counter" in each branch may be the

WITN11070106

preferred platform for the installation of peripherals or dynamically-assigned roles not shared by the others.

- With the introduction of the HNG-X Branch Router, Counters will not need to be sensitive to the type(s) of Wide Area Network (WAN) connection available at their branch. Instead, all Counters will route all network traffic over a Local Area Network to the Branch Router, without any special knowledge of the WAN connections or protocols that lie beyond it.
- Branches will no longer be restricted to a maximum of 30 counters, with the limit being raised to 99.

2.4 Logical View

The Logical View depicts the logical components of the Counter, but at a higher level of abstraction than that of the subsequent Physical Views.

2.4.1 Summary Diagram

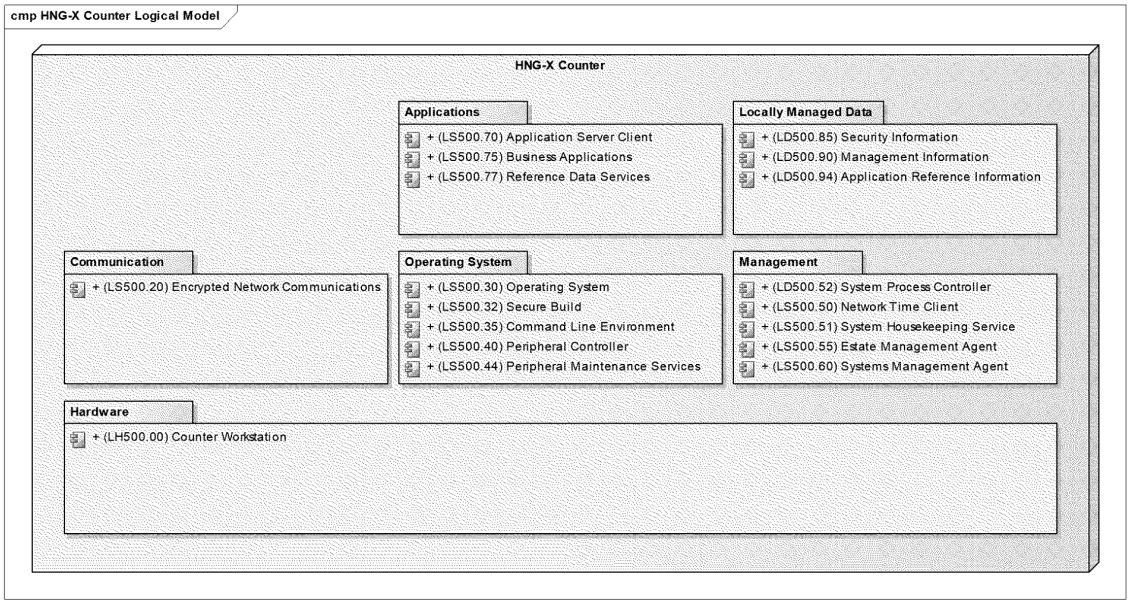


Figure 1 – Logical View of the Counter

2.4.2 Logical Hardware Components

2.4.2.1 Counter Workstation (LH500.00)

The HNG-X Counter node comprises a single logical hardware component called the "Counter Workstation", and this component is the conduit for all IT interaction between Post Office staff and the HNG-X IT system.

It provides functionality to support a range of Point of Sale transactions, including sale of goods, banking, automated bill payments, mobile phone e-Top Ups, PIN pad payments, receipt printing, postal weighing and currency exchange.

WITN11070106

The Counter Workstation operates in three distinct environments, and provides the same functionality in each:

1. At a fixed, physically-secure counter positions in a Post Office branch;
2. In a mobile capacity, with a fixed installation within a vehicle;
3. In a fully portable capacity, roaming with Post Office staff between Post Office and non-Post Office serving locations.

From a logical perspective, no distinction is made between a fixed position and portable counters.

The counter must be able to operate in both live & training environments (CTOs) without requiring a separate build.

For further information on the training environment, refer to the *HNG-X Counter Training Offices Architecture (ARC/SOL/ARC/0005)* and the *HNG-X Training System High Level Design (DES/APP/HLD/0096)*.

2.4.3 Logical Software Components

2.4.3.1 Operating System

2.4.3.1.1 Operating System (LS500.30)

The HNG-X Counter runs an Operating System, to provide a graphical user interface, network connectivity, support for Point of Sale peripherals, and system and data security appropriate to the counter.

2.4.3.1.2 Secure Build (LS500.32)

Working in conjunction with the Operating System, the Secure Build is a suite of configuration settings which combine to reduce the risk of unauthorised access to the counter, and best support the detection and diagnosis of potential security issues.

The optimal settings will closely reflect the selected version and edition of the operating system. They will also support the Post Office usability and security requirements, for example preventing Post Office clerks having direct access to applications and functions other than HNG-X.

2.4.3.1.3 Command Line Environment (LS500.35)

The command line environment is used solely by 3rd Line Support to access resources on the counter such as evidence files, etc.

2.4.3.1.4 Network Security Manager (LS500.34)

This component is used to ensure that counters only communicate with pre-approved network addresses, using only pre-approved network protocols.

2.4.3.1.5 Peripheral Controller (LS500.40)

Most of the counter peripherals do not have operating system device drivers. On Horizon, a Peripheral Controller component was used to control device access, but this component will not be available in HNG-X.

WITN11070106

Under HNG-X, the Peripheral Controller represents the provision of low level drivers to access the underlying peripheral hardware.

2.4.3.1.6 Peripheral Maintenance Services (LS500.44)

It is anticipated that some counter peripherals will need to be maintained with elements of the application reference data, to support business applications and their transactions. This logical software component is used to maintain that data on the peripherals.

2.4.3.2 Communications

2.4.3.2.1 Encrypted Network Communications (LS500.20)

The Encrypted Network Communications component ensures that all network connections used to transmit business transaction data are securely encrypted, to prevent data being read or written to whilst in transit between the counter and its Data Centre servers.

2.4.3.3 Management

2.4.3.3.1 Network Time Client (LS500.50)

The Network Time Client component keeps the Counter Workstation's system clock synchronised with an authoritative time source, to within an agreed tolerance. Other machines in the estate are synchronised similarly, such that:

- An accurate time and date can be reliably recorded against database transactions and on printed reports and receipts, in support of audit and reconciliation activities
- The times of events across the distributed IT system can be reliably compared during problem diagnosis.

2.4.3.3.2 System Process Controller (LS500.52)

The System Process Controller is responsible for providing the necessary "glueware" to allow other logical components to co-ordinate activities, and is responsible for the provision of the user environment, and activation of the application components.

2.4.3.3.3 Estate Management Agent (LS500.55)

This component takes direction from the central Estate Management systems to perform local actions in support of counter build, implementation and maintenance activities.

Such activities are sometimes driven by major IT change projects, but more usually by routine Operational Business Change requests for the deployment of new counters or peripherals, or for counters or branches to be re-purposed.

Because of its role in managing the Counter Workstation, this component needs a high-level of access to the other co-hosted hardware, software and data components.

2.4.3.3.4 Systems Management Agent (LS500.60)

The Systems Management Agent is the logical set of processes that liaise with the central Systems Management services.

WITN11070106

Amongst its duties are the following:

- Reporting of system events to the central Event Management service
- Monitoring system performance and capacity thresholds, and raising events where required
- Supporting incoming connections for shell sessions from support staff performing problem diagnosis
- Receiving distributed software and data from central software distribution systems, using it to perform local software installation and data maintenance.
- Invoking scheduled jobs which run locally on the counter
- Communicating inventory and versioning information back to central inventory systems.
- Deleting temporary files.
- Deleting expired evidence files.
- Emptying caches.
- Rotating log files.
- Performing customised health-checks on critical processes.

Because of its role in managing the Counter Workstation, this component needs a high-level of access to other co-hosted hardware, software and data components.

2.4.3.3.5 System Housekeeping Service (LS500.51)

This component runs periodically or on-demand to perform a set of specific housekeeping activities on the local counter. It manages system housekeeping and log rotation. Its precise set of responsibilities includes:

- Updating peripheral device firmware / data
- Daily reset of passwords for service accounts
- Activation of VPN key changes

Individual applications may implement their own housekeeping routines, but these are out of the scope of the scope of this component, and are invoked under application control.

2.4.3.4 Applications

2.4.3.4.1 Application Server Client (LS500.70)

The Application Server Client is a set of locally-installed libraries, static data and executable files which are installed on the client to allow it to run the Business Applications via the Branch Access Layer, but which are not provided by the client operating system.

Amongst other things, this component provides the execution environment, the user interface libraries for use by the Business Applications, and allows file-based data to be represented as a data object in memory.

Unlike the Business Applications, the Application Server Client is insensitive to the Post Office's specific set of business rules and objects, and is more closely related to the Branch Access Layer.

WITN11070106

2.4.3.4.2 Business Applications (LS500.75)

The Business Applications component is the sum of the business logic, workflow and supporting services which are run locally on the counter and provides the "desktop environment" seen by the user.

2.4.3.4.3 Reference Data Services (LS500.77)

The Reference Data Services component maintains any reference data copies which are present on the counter's local hard disk drive.

2.4.4 Logical Data Components

2.4.4.1 Locally Managed Data

2.4.4.1.1 Security Information (LD500.85)

Post Office staff will not authenticate with the Operating System itself, instead they will authenticate using credentials stored in the Branch Database, accessed via the Branch Access Layer servers.

Unlike Post Office staff, IT support staff will occasionally need to access Counter components other than the Business Applications. It is not appropriate to store credentials for these users in the Branch Database, so they will need credential data to be stored locally on each counter.

2.4.4.1.2 Management Information (LD500.90)

Various data associated with Systems and Estate Management will be required on HNG-X Counters. These data will include counter-specific and branch-specific identity data used by Systems Management and Estate Management components.

2.4.4.1.3 Application Reference Information (LS500.94)

This data component provides the Business Applications with locally-accessible copies of relatively-static, relatively-insensitive business reference data. Some of these data will need to be copied to peripheral devices to support business transactions which use those devices.

2.5 Physical View

The Physical View depicts the physical components of the Counter, and maps each logical component to the physical component(s) used to realise it.

Initially the HNG-X Counter will use the Windows NT 4.0 Workstation platform inherited from Horizon.

The information found in this section is summarised in the Physical Platform Design documents for the NT *(DES/PPS/PPD/0016)* & XP *(DES/PPS/PPD/0017)* variants of the HNG-X Counter.

WITN11070106

2.5.1 Summary Diagrams

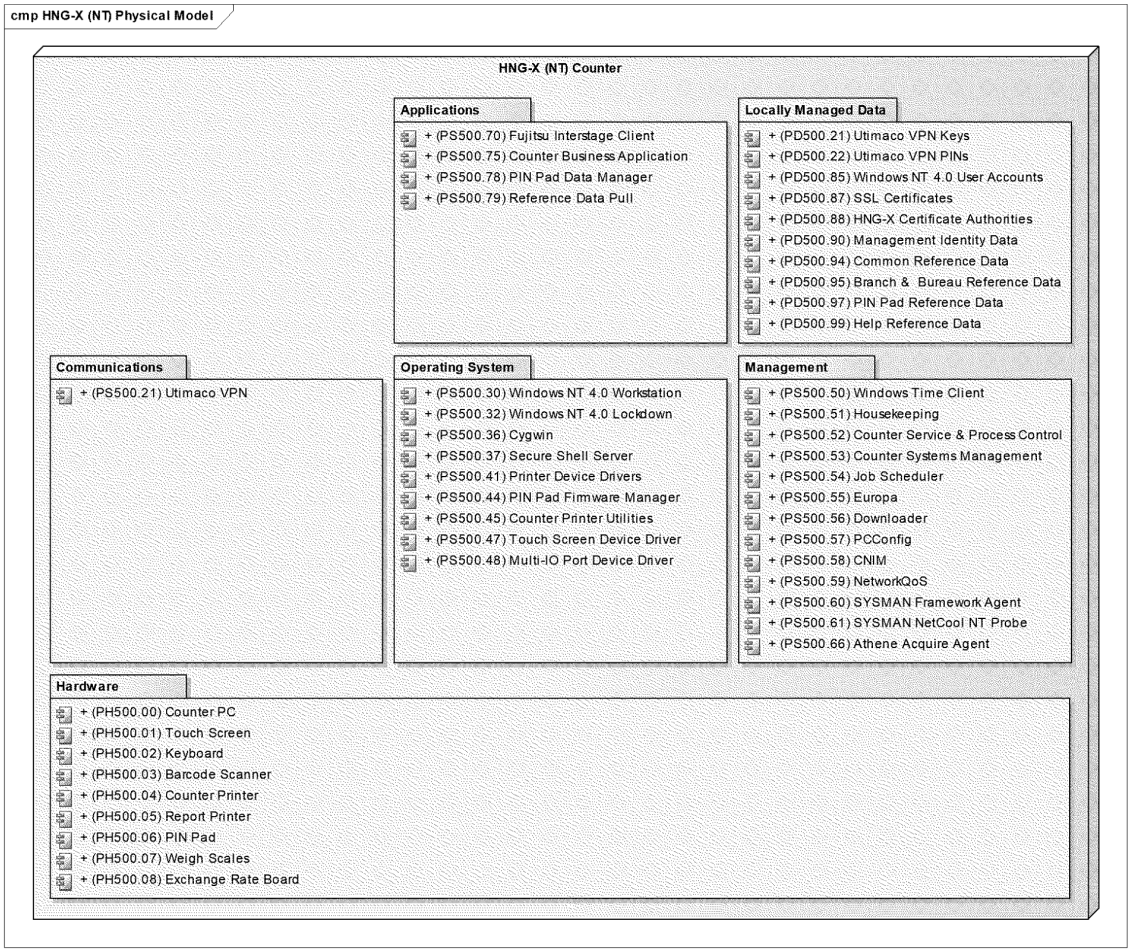


Figure 2 – Physical View of the Counter

2.5.2 Physical Hardware Components

For further information, see the *Counter Hardware Design Specification (BP/DES/003), HNG-X Counter Physical Platform Design (DES/PPS/PPD/0016)* and *HNG-X Mobile Counter Physical Platform Design (DES/PPS/PPD/0127).*

2.5.2.1 Counter PC (PH500.00)

Two variants of the counter workstations exist:

2.5.2.1.1 Fixed Position Counter PC

The Fixed Position Counter PC is based on the Fujitsu Siemens ErgoPro x365/400 Personal Computer, with the following specification:

WITN11070106

- 1 x 400 MHz Intel Pentium II processor
- 512 KB L2 Cache
- 256 MB RAM
- 1 x Hard Disk Drive
- 1 x Intel 82558 LAN 10/100 card with RJ-45 connector
- ATI Rage Pro Turbo 2x AGP graphics card with 4 MB 100 MHz SGRAM
- Specialix I/08 + adapter to provide 8 additional RS232 serial ports (see http://www.perle.com/products/IO8-ISA-Serial-Card.shtml)
- 1.44 MB diskette drive, disabled in BIOS

For historical reasons, many Counter PCs have one or more of the following additional components which are not required for HNG-X. These devices will not be utilised on HNG-X Counter PCs, and not present on new spares:

- A second Hard Disk Drive in a removable frame
- EICON Diva Classic ISDN adapter.
- Conexant ADSL Modem Card

The size of the hard disk drives fitted to counters in the live estate range from the original Horizon specification 4.3 GB drives, to drives in excess of 12 GB. Horizon Change Proposal CP2510 was raised to replace the smaller 4.3 GB hard disk drives still in use in the live estate. A small number of these machines still exist in the estate that have these drives smaller drives.

In addition, during design a number of counters were identified in the live estate with particularly inaccurate clocks. This results in the need to synchronise more frequently with NTP servers, and may lead to periodic unavailability of the business application. For further information, see the *HNG-X Time Synchronisation High Level Design (DES/NET/HLD/0013)*.

The Fixed Position Counter PC and all its peripherals are certified by suppliers to conform to EN54014, as indicated by the presence of a “CE” mark.

For further information regarding the physical design of the fixed position counter, see the *HNG-X Counter Physical Platform Design (DES/PPS/PPD/0016)*.

2.5.2.1.2 Mobile Counter PC

The Mobile Counter PC, referred to as the PHU 2.0, is based on the Geller TS-650P with the following specification:

- 1 x 1 GHz Intel Pentium 4 Celeron processor
- 256 MB RAM
- 1 x 40 GB Hard Disk Drive
- 1 x Integral 10/100 LAN with RJ-45 connector
- Intel 82852/82855 GM/GME Graphics Controller (supports 1024 x 768 x 32 bit)
- 12.1” 800 x 600 TFT Colour LCD display
- Touch screen
- 6 x RS232 Serial Ports (2 x DB9, 4 x RJ12)
- 1 x Parallel Port

WITN11070106

- 3 x USB Ports (inaccessible under Windows NT 4.0 Workstation)

The Geller is equipped with a built in touch screen, eliminating the need for a separate peripheral. The touch screen interface is accessed using a "mouse" device driver. This is the same approach used with the separate touch screen peripheral (PH500.01).

The screen is capable of supporting a resolution of 800 x 600 pixels with 32-bit colour quality.

The Mobile Counter PC and all its peripherals are certified by suppliers to conform to EN54014, as indicated by the presence of a "CE" mark.

For further information regarding the physical design of the fixed position counter, see the *TS650P (Pilum Hybrid) Hardware Specification (IMP/GEN/SPE/0001)* and the *HNG-X Mobile Counter Physical Platform Design (DES/PPS/PPD/0127)*.

2.5.2.2 Touch Screen (PH500.01)

The Touch Screen monitor allows Post Office staff to press on-screen button to navigate around the application.

A number of different models are in use in the existing branch estate capable of supporting a screen resolution of at least 800x600 pixels with 32-bit colour quality, and all must be supported under HNG-X.

On fixed counters the monitor is connected to the Counter PC using two cables, one for the video signal and one for touch-screen support.

The touch screen interface is accessed using a "mouse" device driver.

Under Horizon, the video display is configured to use 8-bit colour. During migration, it will be necessary to reconfigure the display driver settings to 16-bit colour (higher bit rates such as 24-bit & 32-bit may be available, but have been found to work in an inconsistent fashion).

2.5.2.3 Keyboard (PH500.02)

The 99-key LIFT keyboard incorporates a Magnetic Swipe and Smart Card reader. The cable from the keyboard splits into two, and connects to the Counter PC's keyboard socket and also one of its serial sockets.

2.5.2.4 Barcode Scanner (PH500.03)

A bar code reader is provided with the Counter PC to allow users to scan barcodes on products. This scanner is connected to the Counter PC using a PS/2 cable, and takes its power from the keyboard using a separate serial cable.

2.5.2.5 Counter Printer (PH500.04)

An Epson TMJ7100 inkjet printer is connected to each Counter PC using a serial cable. Amongst other things, this printer is used to print receipts, branded Gift Vouchers and Postal Orders.

2.5.2.6 Report Printer (PH500.05)

Each branch has a single back-office A4 printer, primarily used to print accounting statements and reports.

To protect the existing investment, various Report Printer models will be used. The current list of supported printers is:

- OKI 8p LED printer

WITN11070106

- OKI 8p+ LED printer

The printer is connected to just one counter at each branch using a parallel cable, and then shared on the network using Windows printer sharing. The printer is always connected to the counter with the lowest Counter Id.

Whilst Fixed Counter PCs shall always able to access the Report Printer, it is only available to Portable Counter PCs when they are connected to their base location's Local Area Network.

2.5.2.7 PIN Pad (PH500.06)

A HyperCom HFT117 PIN pad is connected to each Counter PC using a serial cable, for use with Chip and PIN payment cards. Unlike the other counter peripherals, the PIN pad is usually mounted outside the "fortress" serving position, where it can be accessed by the customer.

Each PIN Pad is managed from a specific counter position, so PIN Pads must not be moved between Counter PCs by Post Office staff.

Whilst most peripherals can be safely interchanged between live and training counters, CTO counters must use specially-configured PIN Pads, which are pre-loaded with different configurations to those used in the live estate.

2.5.2.8 Weigh Scales (PH500.07)

Many counters are supplied with electronic weigh scales, which are connected to either one or two Counter PCs using separate serial cables.

A number of different models are in use in the existing branch estate, and all must be supported under HNG-X.

2.5.2.9 Exchange Rate Board (PH500.08)

Optionally, a Bureau de Change rates board can be connected to one Counter in each branch, which can then be configured to display current exchange rates to customers.

A number of different models are in use in the existing branch estate, and all must be supported under HNG-X.

2.5.3 Physical Software Components

2.5.3.1 Operating System

2.5.3.1.1 Windows NT 4.0 Workstation (PS500.30)

The Horizon platform is based on Windows NT 4.0 Workstation, and this platform will be used to run the Counter Business Application.

No operating system changes will be required to support the Counter Business Application.

2.5.3.1.2 Windows NT 4.0 Lockdown (PS500.32)

Today's Horizon platform is "locked-down" to reduce the risk of security problems and simplify usability and problem determination. This lockdown customisation and configuration will form the basis of the Windows NT 4.0 Lockdown component for HNG-X, though some minor change may be necessary to

WITN11070106

address any new threats posed by the new counter components introduced by HNG-X, or to enable those components to operate.

Settings applied to the BIOS will be considered as part of the lockdown, as well as those applied to Windows itself.

Specific provision must be made for development and test environments when designing the Windows NT 4.0 Lockdown to ensure that it remains possible to construct test Counters which permit console access to the underlying operating system for automated testing and problem determination.

2.5.3.1.3 Cygwin (PS500.36)

Cygwin is an open source Linux-like environment for the Windows operating system, providing access to a collection of commonly used GNU tools such as the *sh* command line interpreter, *patch*, *diff*, etc.

These tools are mainly used by 3rd line support via the Secure Shell Server to access evidence files on the counter.

In addition, the Counter Business Application makes selective use of a number of the Cygwin tools (patch, cksum, unzip).

All Cygwin components are dynamically linked against the cygwin1.dll.

2.5.3.1.4 Secure Shell Server (PS500. 37)

Under HNG-X it has been decided to retain the modified version of the OpenSSH Secure Shell (SSH) software provided by Cygwin as used under Horizon.

The server listens for incoming requests for shell sessions from users logged onto the SAS server.

For further information, refer to the document *Remote Access and Diagnostics (ARC/SYM/ARC/0004)*.

2.5.3.1.5 Printer Device Drivers (PS500.41)

The Report Printer is the only counter peripheral that will not use JavaPOS based “drivers”.

Instead, native operating system drivers will be used.

The Counter Printer will be accessed via a JavaPOS driver to enable access to functionality that is not usually provided through operating system drivers.

Under Horizon, the Counter Printer was set to emulate the older Ithaca printer. This emulation mode will not be preserved in HNG-X, and the native mode will be used instead.

2.5.3.1.6 Touch Screen Device Driver (PS500.47)

Under Windows NT 4.0 Workstation additional Operating System device drivers are required to allow the touch screen to be used as a “mouse” device. In addition, the installation provides a utility that allows the touch screen to be calibrated.

2.5.3.1.7 Multi-IO Port Device Driver (PS500.48)

Under Windows NT 4.0 Workstation additional Operating System device drivers are required to allow the Specialix I/08 multi-IO port card to be used.

WITN11070106

2.5.3.1.8 Counter Printer Utilities (PS500.45)

Under Horizon Change Proposal 4260, Epson will deliver utilities to replace the firmware and stored logos on Epson Counter Printers. The utilities demand access to the printer's serial port, and an administrative level of access to the counter's operating system is required.

The utilities will not need to be updated for HNG-X.

The full set of utilities provided by Epson is comprised of:

Application	Description
CMPFWVER.EXE	Compares the firmware version in a given file with that of the connected Epson printer.
FLASHERR.EXE	Analyses errors from TMFLASHWRITER.EXE.
PRNCHBR.EXE	Changes the baud rate of the connected Epson printer.
PRNCHEMU.EXE	Changes the emulation mode of the connected Epson printer between native Epson mode and Ithaca emulation mode.
PRNLGMGR.EXE	Uploads TLG format logos to the connected Epson printer.
PRNRST.EXE	Resets the connected Epson printer.
PRNSPEED.EXE	Returns the printer's current speed, or returns an informative error code.
PRNTYPE.EXE	Returns the printer's type, or returns an informative error code.
TMFLASHWRITER.EXE	Overwrites the firmware of the connected Epson printer.

Readers should refer to *Counter Printer Replacement Design Proposal* (AS/DPR/031) for more details.

2.5.3.1.9 PIN Pad Firmware Manager (PS500.44)

A custom-written utility (PPCHKUPG.EXE) exists on Horizon counters, and is invoked by SYSMAN to check for the availability of new PIN Pad firmware on a distribution server within the data centre.

The requirements for this utility remain the same in HNG-X as in Horizon.

As on Horizon, this utility will download the new firmware, which is comprised of both the firmware, and a firmware "downline loader". The "downline loader" checks the validity of the accompanying firmware, and then loads it onto the hardware directly. To allow this direct access, any other components using the device must be stopped, or instructed to relinquish control whilst the PIN Pad Firmware Manager is running.

2.5.3.2 Communications

2.5.3.2.1 Utimaco VPN (PS500.21)

Under Horizon, the Utimaco VPN product is used to provide a VPN solution protecting all network traffic, both between counters in the branch, and between counters and the data centre.

The VPN has been configured to encrypt traffic using the Red Pike cipher.

HNG-X will continue to use the Utimaco VPN solution to protect all network traffic both counters in the branch and between counters and the data centre.

WITN11070106

Unlike Horizon, the keys will be global to the live estate. Under Horizon, each branch was assigned branch specific keys. This level of protection is no longer deemed necessary under HNG-X, as business traffic will be further protected using SSL.

The VPN requires the presence of both the Utimaco VPN Keys (PD500.21) and Utimaco VPN PINs (PD500.22) to operate.

For further information refer to the *VPN on HNG-X NT High Level Design (DES/MIG/HLD/0006)*.

2.5.3.3 Management

2.5.3.3.1 Windows Time Client (PS500.50)

Under Horizon, time synchronisation was achieved using a bespoke scheduling solution (CAS), that was dependent on software supplied by Escher. Non-gateway counters took their time from the Branch's Gateway Counter, which took its time from the Horizon Correspondence Servers.

This time synchronisation is no longer available in HNG-X. Instead, the Windows Time Service (W32Time) will be used on each counter, to periodically synchronise that counter's system clock with the clock of one or more authoritative time sources.

The configuration of a Windows XP counter using time synchronisation outside an Active Directory infrastructure is discussed at http://support.microsoft.com/kb/314054/, and a similar approach will be used for Windows NT counters.

For further information, refer to the *Time Synchronisation High Level Design (DES/NET/HLD/0013)*.

2.5.3.3.2 Job Scheduler (PS500.54)

The Job Scheduler runs with Windows administration privileges to read the Job Schedules, and invoke those jobs according to the schedule.

The existing Horizon CAS scheduler will be replaced with the operating system provided job scheduler.

It should be noted that Tivoli managed jobs are not managed via the local counter scheduler, as these jobs are managed centrally through the data centre.

2.5.3.3.3 Athene Acquire Agent (PS500.66)

Metron's Athene Acquire Agent will be installed on all counters to collect Windows native performance data from the Windows registry at pre-defined intervals, and store it in files on the counter hard disk in case it is needed subsequently for problem determination. The files are of pre-defined maximum sizes, so once they fill, older data begins to be overwritten.

The agent does not require network access. If it proves necessary to analyse the locally-stored data, support teams will gather the data from the counter and store it centrally for the duration of the analysis; alternatively SYSMAN tasks can be scheduled to collect the data.

Under Windows NT 4.0 Workstation it will be necessary to enable disk performance logging in order to collect meaningful data.

2.5.3.3.4 Europa (PS500.55)

This component is a hardware testing utility which checks the presence and operations of both internal hardware devices and external counter peripherals. In the lifecycle of a typical counter, it runs only twice — once during the initial counter build by Fujitsu Services subcontractors, and once when the counter is deployed to the branch and is being set up by the field engineer. The utility reports errors to the screen

WITN11070106

where they must be acknowledged by the engineer before the boot can complete, thus avoiding situations where faulty hardware components are left on-site after an engineer's visit.

It is worth noting that Europa can be invoked before all of the Counter's software components are installed, or running, so it cannot rely on JavaPOS drivers for device access. Instead it will access devices in the same way that Horizon's Europa component does. Many of the existing Horizon Europa calls may be immediately re-usable on HNG-X NT Counters.

Although Europa is not a particularly intuitive name for this component, it is one which is already familiar to Fujitsu Services Horizon support staff. The component itself is deemed to be of little direct interest to Post Office Ltd, so the name is preserved in HNG-X.

2.5.3.3.5 PCConfig (PS500.57)

Both Fixed and Portable counters will be pre-built by Fujitsu Services subcontractors using a standard software build.

However, once fully-installed each counter has its own unique identity. Furthermore, in order to distribute load amongst similar sets of Data Centre servers, there are some situations where different branches must be pre-configured to communicate with different servers in the same server pool.

The PCConfig component runs when a new counter is first deployed to a branch. It controls the boot process, establishes contact with the HNG-X Boot Platform Server using a temporary network address and credentials, and then downloads and applies the unique configuration data associated with that counter.

2.5.3.3.6 CNIM (PS500.58)

CNIM monitors and manages network connectivity within the branch, and is responsible for producing network statistics, which are subsequently aggregated and transmitted to the data centre via the CasQoS component.

Version 2.0 of CNIM used under HNG-X is a significant revision of the version used under the current Horizon solution, and will be delivered prior to the rollout of the Branch Router.

CNIM receives broadcast error event data and notification of changes to the NST from the local Branch Router, correlates the data with other local events, and then writes summary events to the Windows Event Log if necessary.

Although it runs on all counters, at any given time it is only active on a single counter in each branch. At system start-up and periodically thereafter, CNIM polls other counters on the LAN to check that an instance is running somewhere else, and only switches to active mode if it cannot find another active instance.

Where an active instance fails and cannot be restarted immediately, the remaining counters hold an election to agree which of them will switch to active mode. The machine which failed does not assume priority when it is recovered, so will not typically attempt to switch to active mode at that stage.

CNIM provides an interface that can be used by other software components to interrogate the current state of the LAN/WAN.

For further information, refer to the *CNIM Low Level Design (DEV/APP/LLD/0084)*.

2.5.3.3.7 NetworkQoS (PS500.59)

NetworkQos is a replacement for the CasQoS component found on Horizon counters. It is responsible for processing Quality of Service data from CNIM and the Counter Business Application, and reporting the aggregated statistics to the data centre. The statistics are written as Windows Events, and subsequently sent to the data centre by the NetCool Probe.

WITN11070106

For further information, refer to the *HNG-X NetworkQoS High Level Design (DES/APP/HLD/0125)*.

2.5.3.3.8 Downloader (PS500.56)

The Downloader component complements PCConfig, running immediately after it to establish connectivity with the SYSMAN framework, whereupon the counter will request any software updates available from the SYSMAN distribution servers and commit them.

The Downloader also checks for personality clashes by listening on the branch LAN to check that new and replacement counters do not attempt to request Boot Server File (BSF) data using Management Identity Data which they are already identified with.

2.5.3.3.9 SYSMAN Framework Agent (PS500.60)

The SYSMAN Framework Agent is based on the IBM Tivoli Framework Agent 3.7.1. It runs on the counter with administrative privileges to:

- Execute pre-defined problem determination tasks on behalf of the support teams.
- Monitor and correct the status of key services and other processes.
- Receive and action software distribution instructions from SYSMAN.

All distributed software is packaged using common standards outlined in document *HNG-X System and Estate Management – Overall Architecture (ARC/SYM/ARC/0001)*. It keeps copies of the software updated, allowing updates to be regressed to previous versions.

2.5.3.3.10 SYSMAN NetCool NT Probe (PS500.61)

The SYSMAN NetCool NT Probe runs on counters to collect system, application and security events from the Windows event logs, and forward them to the NetCool Object Server Proxy so they can be alerted to operators, correlated to other events and used in problem determination.

The list of security events forwarded to the NetCool Object Server Proxy will be agreed with Post Office Ltd.

This component will be distributed to and activated on the existing Horizon counters prior to migration to HNG-X.

2.5.3.3.11 Counter Systems Management (PS500.53)

This component is responsible for providing an interface between the Counter Business Application and the Systems Management components.

This interface is used by the Counter Business Application to trigger the retrieval / delivery of Reference Data via SYSMAN.

For further information, refer to the *SDAM Horizon Support High Level Design (DES/SYM/HLD/0012)*.

2.5.3.3.12 Counter Housekeeping (PS500.51)

For some years, Horizon counters have run a scheduled housekeeping utility called “Clear Desk”. Similar behaviour will be continued on HNG-X counters. The utility will run once each night (or on-demand) and will have local Windows administration rights on each counter. To prevent “event storms” occurring routinely, the precise time at which Counter Housekeeping runs will be staggered slightly across the estate, and care will be taken to ensure that frequently occurring Counter Housekeeping events with severities other than “Warning” and “Error” are filtered out.

WITN11070106

The housekeeping process must also check that the attached Slip Printer is running in the correct mode and at the correct speed, and upload any updated firmware and/or logos using the Counter Printer Utilities prior to restarting the Counter Business Application.

For further information, refer to the *HNG-X Counter Infrastructure Service & Process Control High Level Design (DES/APP/HLD/0057)*.

2.5.3.3.13 Counter Service & Process Control (PS500.52)

This component provides a set of services that are executed at start-up during the OS boot sequence, replacing the standard user "shell", intercepting system key sequence (eg. CTRL-ALT-DEL), and starting and monitoring the Counter Business Application.

In addition, a utility is provided by this component that interfaces with the PIN Pad Firmware Manager. This utility is responsible for "pulling" new PIN Pad firmware from the data centre, and then invoking the accompanying utility to validate and apply the new firmware.

The start-up process must also check that the attached Slip Printer is running in the correct mode and at the correct speed, and upload any logos using the Counter Printer Utilities prior to starting the Counter Business Application.

For further information, refer to the *HNG-X Counter Infrastructure Service & Process Control High Level Design (DES/APP/HLD/0057)*.

2.5.3.4 Applications

2.5.3.4.1 Fujitsu Interstage Client (PS500.70)

The Fujitsu Interstage Client provides the functionally of two logical components, which can effectively be treated as an execution environment (as opposed to cohabiting application components):

2.5.3.4.1.1 Application Server Client (LS600.70)

The Fujitsu Interstage Client contains a set of executables and libraries which support the Counter Business Application. Amongst other subcomponents, it includes a Java Virtual Machine (JVM) to run Java bytecode, and Java Swing libraries that are used to construct user interface widgets for the Counter Business Application.

2.5.3.4.1.2 Encrypted Network Communications (LS600.20)

The Fujitsu Interstage Client provides the Java Virtual Machine that is used by the Counter Business Application. The Java Virtual Machine uses the standard Sun security library that implements the Secure Sockets Layer (SSL) protocol, as well as providing the necessary tools for key management.

SSL sessions will be used to encrypt all business traffic destined for the Branch Access Layer servers between the Counter and the SSL termination point in the network infrastructure at the Data Centre.

Traffic not destined for the Branch Access Layer servers is not encrypted by this component.

2.5.3.4.2 Counter Business Application (PS500.75)

The Counter Business Application provides the functionally of a number of logical components:

2.5.3.4.2.1 Business Applications (LS500.75)

The Counter Business Application is used to deliver all business functionality to Post Office counter staff.

WITN11070106

Significantly, field engineers will also have access to the Counter Business Application to invoke engineering functions from within the application. These engineering functions will closely parallel those found in Horizon and documented in the document *Horizon OPS Menu Hierarchy (SD/SPE/016)*, including the installation, configuration and testing of peripherals, the application and the network.

The application will need to leverage interfaces exposed by cohabiting components on the counter to fulfil the requirements of these engineering functions. These interfaces include:

- CNIM
- Counter Systems Management
- PIN Pad Data Manager

In addition, the application will need to expose interfaces to:

- Counter Service & Process Control

Special consideration during the design stage needs to be given to the requirements associated with CTOs to ensure that the same version of the application can be used for both live and training environments.

For more detail about this component the reader should refer to the document *HNG-X Counter Business Applications Architecture (ARC/APP/ARC/0009)*.

2.5.3.4.2.2 Reference Data Services (LS500.77)

The Reference Data Manager will run periodically to compare the version of the local copy of the Application Reference Information with the latest available version on distribution servers. If an unacceptable discrepancy is found then it takes action to request and upgrade the local copy to a more current version. If the local copy of the application reference information has expired, immediate action is taken to upgrade the local copy

The large number of counters in the live estate can make it difficult to distribute updates to this data quickly to all counters, so provision will be made to hold both data which is currently valid, and also data which will become valid in the near future. To further reduce the impact on distribution servers at peak times, this component will check for updates at staggered times across the estate.

The Reference Data Manager is covered in greater detail in the document *HNG-X Reference Data Architecture (ARC/APP/ARC/0001)*.

2.5.3.4.2.3 Peripheral Controller (LS500.40)

The Counter Business Application makes use of JavaPOS, a set of Application Programming Interfaces (APIs) which are used to communicate with peripheral devices commonly associates with Point of Sale (POS) systems.

JavaPOS “Drivers” will be written for each of the HNG-X counter peripherals (excluding those devices where native support exists in the Java Runtime Environment). These drivers are integral to the Counter Business Application and will pass instructions to the ports to which the peripherals are connected, using appropriate operating system drivers.

A set of coding guidelines will be established in conjunction with the security architect to ensure that no preventable security vulnerabilities are introduced into these drivers.

2.5.3.4.2.4 Peripheral Maintenance Services (LS500.44)

The implementation of the logical component Peripheral Maintenance Services is split across a number of physical components.

The component is responsible for interacting with a peripheral for the purpose of loading reference data or configuration from reference data.

WITN11070106

The Counter Business Application is responsible for implementing this functionality for those devices where all the necessary interaction with the peripheral can be achieved using solely JavaPOS drivers.

This includes all devices apart from:

- Counter Printer (where the Epson Printer Utilities are used)
- PIN Pad (where the PIN Pad Data Manager is used)

2.5.3.4.3 PIN Pad Data Manager (PS500.78)

Horizon currently supports the upgrade of PIN Pad Reference Data using a custom-written driver. This will no longer be available under HNG-X, so a new custom-written tool will be developed for HNG-X.

2.5.3.4.4 Reference Data Pull (PS500.79)

When the Reference Data Manager (a component of the Counter Business Application) determines that new Reference Data is needed on the counter, then this data can be retrieved either through the application, or via SYSMAN, as indicated by the Branch Access Layer.

Where the data needs to be delivered to the counter via SYSMAN, the Reference Data Pull component is used to provide a simple interface between the Counter Business Application and the SYSMAN Framework.

For further information refer to *SDAM - Horizon Support (DES/SYM/HLD/0012)*.

2.5.4 Physical Data Components

2.5.4.1 Windows NT 4.0 User Accounts (PD500.85)

Support users must authenticate before accessing counters to perform problem determination. To enable this authentication, those users will hold credentials which can be validated locally on each counter.

In addition, a number of local Service Accounts are required, allowing services to run using a more constrained set of access privileges.

Windows also has a number of in-built user accounts and groups which it is not possible to remove, though these accounts will be secured as far as possible using settings in the Windows NT 4.0 Workstation component.

For further information on security requirements that apply to these accounts, see section 6.

Locally-stored Windows accounts will be stored in the encrypted Security Accounts Manager (SAM) database.

2.5.4.2 Utimaco VPN Keys (PD500.21)

The Utimaco VPN requires cryptographic key material to establish a VPN connection with the data centre. Keys use the Red Pike cipher, and are stored and managed locally on each counter.

Unlike Horizon, the keys are global to the live estate. Under Horizon, each branch was assigned branch specific keys. This level of protection is no longer deemed necessary under HNG-X, as business traffic will be further protected using SSL.

In the event of new keys being activated, these will be distributed to the estate via the Counter Business Application, which will receive new keys during logon.

When a counter is replaced in the live estate, pre-distributed keys will be used. In the event that the keys have been updated, AutoConfig will download the current active keys from the data centre.

WITN11070106

Keys are stored on the counter's local file-system, and protected using operating system access control.

For further information, please refer to the document *VPN on HNG-X NT High Level Design (DES/MIG/HLD/0006).*

2.5.4.3 Utimaco VPN PINs (PD500.22)

In addition to cryptographic keys, Utimaco VPN requires a PIN to activate a key.

PIN seeds are stored in the counter's registry, and protected using operating system access control.

For further information, please refer to the document *VPN on HNG-X NT High Level Design (DES/MIG/HLD/0006).*

2.5.4.4 SSL Certificates (PD500.87)

An SSL certificate, signed by a sub-CA of the HNG-X Certificate Authority, will be stored locally on each counter.

The SSL certificate will be required to connect to the SSL termination point within the data centre, currently defined as being the ACE blade.

Only a single estate wide certificate will be used. There will not be individual certificates per branch or counter. A different certificate will be used in the test environment to protect the integrity of the live certificate.

In the event of new certificates being issued, these will be delivered to counters using the software distribution capabilities of the SYSMAN Framework Agent. When new certificates are delivered to the counter they may be accompanied by a certificate revocation list to revoke existing certificates installed on the counter.

Certificates will be stored on the counter's local file-system in a Java "key store" and protected using operating system access control.

2.5.4.5 HNG-X Certificate Authorities (PD500.88)

The HNG-X Root Certificate Authority and sub-Certificate Authorities are delivered to the counter to allow the counter to validate the integrity of SSL certificates.

The SSL Certificates (PD500.87) will be signed using the sub-Certificate Authorities.

In the event of the root or sub CA's being updated, they will be redistributed using the software distribution capabilities of the SYSMAN Framework Agent, along with an appropriate Certificate Revocation List.

Certificate Authorities will be stored on the counter's local file-system in a Java "key store" and protected using operating system access control.

2.5.4.6 Management Identity Data (PD500.90)

Various Estate Management and Systems Management components on the counter maintain their own information about that counter's identity. Under HNG-X, consideration will be given to consolidate this data into a single data file wherever possible during High Level Design, so that it can be maintained as a single unit.

2.5.4.7 Job Schedules (PD500.91)

The Job Schedules contain the list of operational jobs which must be invoked on the counter according to a pre-defined schedule. This flat-file data will be maintained using SYSMAN software distribution.

WITN11070106

It should be noted that Tivoli managed jobs are not managed via the local counter scheduler, as these jobs are managed centrally through the data centre.

2.5.1.8 PIN Pad Reference Data (PD500.97)

This data is the set of IIN definitions and rules imposed by payment card companies and by Post Office Ltd. It is fairly volatile, so must be refreshed periodically throughout the lifetime of the counter.

Unlike other PIN Pad Reference Data, PIN Pad key materials and PIN Pad firmware will not be stored on counters beyond the time it takes to download them to the PIN Pad peripheral.

For more details on PIN Pad data, readers should refer to the document *HNG-X Architecture - Reference Data (ARC/APP/ARC/0001)*.

2.5.1.9 Common Reference Data (PD500.94)

Common reference data and the graphical image used on Gift Vouchers are fairly large making them suitable for distribution via SYSMAN's software distribution functionality.

For more details on reference data, consult the document *HNG-X Architecture - Reference Data (ARC/APP/ARC/0001)*.

2.5.1.10 Help Reference Data (PD500.99)

The mark-up and image files used to provide application help are fairly large making them suitable for distribution via SYSMAN's software distribution functionality.

For more details on reference data, consult the documents *HNG-X Architecture - Reference Data (ARC/APP/ARC/0001)* and *High Level Design of HNG-X Counter Help System (DES/APP/HLD/0102)*.

2.5.1.11 Branch and Bureau Reference Data (PD500.95)

Bureau de Change data and branch-specific reference data are fairly small and volatile. SYSMAN is unable to deliver packages to specific branches. Therefore, branch-specific reference data is distributed to the counter from the Branch Database via the Branch Access Layer servers.

For more details on reference data, consult the document *HNG-X Architecture - Reference Data (ARC/APP/ARC/0001)*.

2.5.1.12 CNIM QoS Data (PD500.50)

CNIM captures network Quality of Service data, and using a peering topology it consolidates the quality of service data between all of the counters in the branch.

Overnight, the NetworkQoS "master" will write the Quality of Service data to the Counter PC's Event Log so that it can be transmitted to the data centre via the NetCool Probe.

2.6 Mapping Logical Components to Physical Components

The table below shows how the logical components described above are realised as physical components on the counter.

The table is also used to show which HNG-X team is likely to take primary responsibility for the development of each component.

WITN11070106

Note: There is notionally a one-to-many relationship between the physical components and the products that will be delivered as part the software stack. The mapping between the physical components and products will be documented in the relevant component High Level Designs.

Logical Component	Physical Components	Development Team
Counter Workstation	Counter PC	Platforms and Storage
	Touch Screen	Platforms and Storage
	Keyboard	Platforms and Storage
	Barcode Scanner	Platforms and Storage
	Counter Printer	Platforms and Storage
	Report Printer	Platforms and Storage
	PIN Pad	Platforms and Storage
	Weigh Scales	Platforms and Storage
	Exchange Rate Board	Platforms and Storage
Operating System	Windows NT 4.0 Workstation	Platforms and Storage
Secure Build	Windows NT 4.0 Lockdown	Platforms and Storage
Command Line Environment	Cygwin	TBA
	Secure Shell Server	Systems Management
Peripheral Maintenance Services	PIN Pad Firmware Manager	Crypto
	Counter Printer Utilities	Integration
Network Time Client	Windows Time Client	Integration
System Process Controller	Counter Service & Process Control	Counter Infrastructure Development
System Housekeeping Service	Housekeeping	Counter Infrastructure Development
Estate Management Agent	Europa	Estate Management
	PCConfig	Estate Management
	Downloader	Estate Management
	CNIM	Networks
	NetworkQoS	Networks
Systems Management Agent	SYSMAN Framework Agent	Systems Management
	SYSMAN NetCool NT Probe	Systems Management
	Counter Systems Management	Counter Infrastructure Development
	Job Scheduler	Integration
	Athene Acquire Agent	Integration
Application Server Client	Fujitsu Interstage Client	Counter Development
Encrypted Network Communications	Utimaco VPN	Networks
Security Information	Windows NT 4.0 User Accounts	Integration
	Utimaco VPN Keys	Networks
	Utimaco VPN PINs	Networks
	SSL Certificates	Security
	HNG-X Certificate Authorities	Security
Peripheral Controller	Printer Device Drivers	Integration
	Touch Screen Device Driver	Integration
	Multi-IO Port Device Driver	Integration
	Counter Business Applications	Counter Development

WITN11070106

Business Applications		
Peripheral Controller		
Reference Data Services		
	PIN Pad Data Manager	Counter Development
Management Information	Management Identity Data	Estate Management
Application Reference Information	PIN Pad Reference Data	Reference Data Team
	Common Reference Data	Reference Data Team
	Branch and Bureau Reference Data	Reference Data Team
	Help Reference Data	Reference Data Team

Table 1 – Mapping Logical Components to Physical Components

WITN11070106

2.7 Counter Training Offices

To simplify the development, build and testing of the counter one of the requirements of HNG-X is to produce a single counter build.

Special consideration needs to be given the requirements associated with CTOs during the design stage to ensure that this requirement can be met.

The Branch Access Layer will be responsible for differentiating between live and training counters, and redirecting traffic from CTO counters to emulated services, thereby exposing an identical interface to the Counter.

A PIN Pad must be used in training environments that contains test keys, and not the “live” keys. Replacement of PIN Pad keys is a non-trivial activity, and rather than waiting until deployment time, it is more expedient to build the PIN Pads with the appropriate key set pre-loaded.

For further information refer to the *HNG-X Counter Training Offices Architecture (ARC/SOL/ARC/0005)* and the *HNG-X Training System High Level Design (DES/APP/HLD/0096)*.

WITN11070106

3 Platforms

3.1 Overview

The HNG-X Counter platform is described in section 1 ("Architectural Description").

3.2 Spares Strategy

Under Horizon, seven different counter variants currently exist:

Variant	Description	Estimated Volume
HORIZON SCO	Single Counter Outlet	8,000
HORIZON MCG	Multi Counter Gateway	4,000
HORIZON SLAVE	Slave	18,000
PHU 1.5	Geller Mobile	70
LUGGABLE	Bespoke Portable	250
VSAT SCO	Broadband Satellite	60
VSAT MCG	Broadband Satellite	
		30,380

Under HNG-X, the number of variants will be consolidated into two:

Variant	Description	Estimated Volume
HNG-X COUNTER	Generic Counter	30,000
PHU 2.0	Geller Mobile	500
		30,500

This simplification is achieved through the introduction of the branch router, which consolidates all WAN connectivity into the Branch Router, thereby removing the need for WAN specific hardware in the individual counter variants.

For further information, please refer to the *Spares Strategy for Horizon And HNG-X Migration (DES/INF/HLD/0001)*.

3.2.1 PHU Spares

Special consideration needs to be given to the migration of the mobile counters from the PHU 1.5 through to the PHU 2.0.

The PHU 1.5 is initially being deployed into the live estate using a Sarian ISDN router.

During the introduction of the branch router, the Sarian ISDN router will be replaced with the Branch Router.

WITN11070106

However, a new spare will not be mastered for the PHU 1.5 + Branch Router under Horizon. A new PHU 2.0 spare will be mastered for HNG-X.

As a result, in the event of a PHU + Branch Router failure under Horizon requiring replacement with a spare, the spare would require provisioning using a Sarian ISDN router before migrating to use Branch Router.

During the high level design, consideration will be given to how to simplify the provisioning of the mobile counters in this scenario.

WITN11070106

4 Networks

4.1 Overview

This section of the document describes the position of the Counter with respect to other related nodes, and explains any assumptions which are made about the network architecture upon which it relies.

For more details about the HNG-X network architecture, readers should refer to *HNG-X Network Architecture (ARC/NET/ARC/0001)*.

4.2 Counter Networks

As shown in figure below, all Counters are physically located in Post Office branches, and connect to HNG-X Data Centres via a Branch Router which is also physically located at each branch. Horizon Gateway Counters will be rendered obsolete by the roll-out of HNG-X and will downgrade to a standard HNG-X Counter.

Some branches have multiple counters, but a large number of smaller branches have only one. Because of the relatively large number of branches, it is cost-effective to deploy different network topologies at branches of different sizes. Thus:

- At branches with only one or two Counters, each Counter is connected directly to the Branch Router.
- At branches with more than two Counters, the former gateway counter will be connected to the Branch Router, and all other Counters are connected to an unmanaged Ethernet hub, which is also connected to the Branch Router.

Training branches are connected to the network in exactly the same way as live branches, but may use PSTN which will be connected to either to a Gateway Counter or a Branch Router.

All Ethernet connections at the branch use a single CAT-5 Unshielded Twisted Pair Ethernet cable with RJ-45 connectors.

WITN11070106

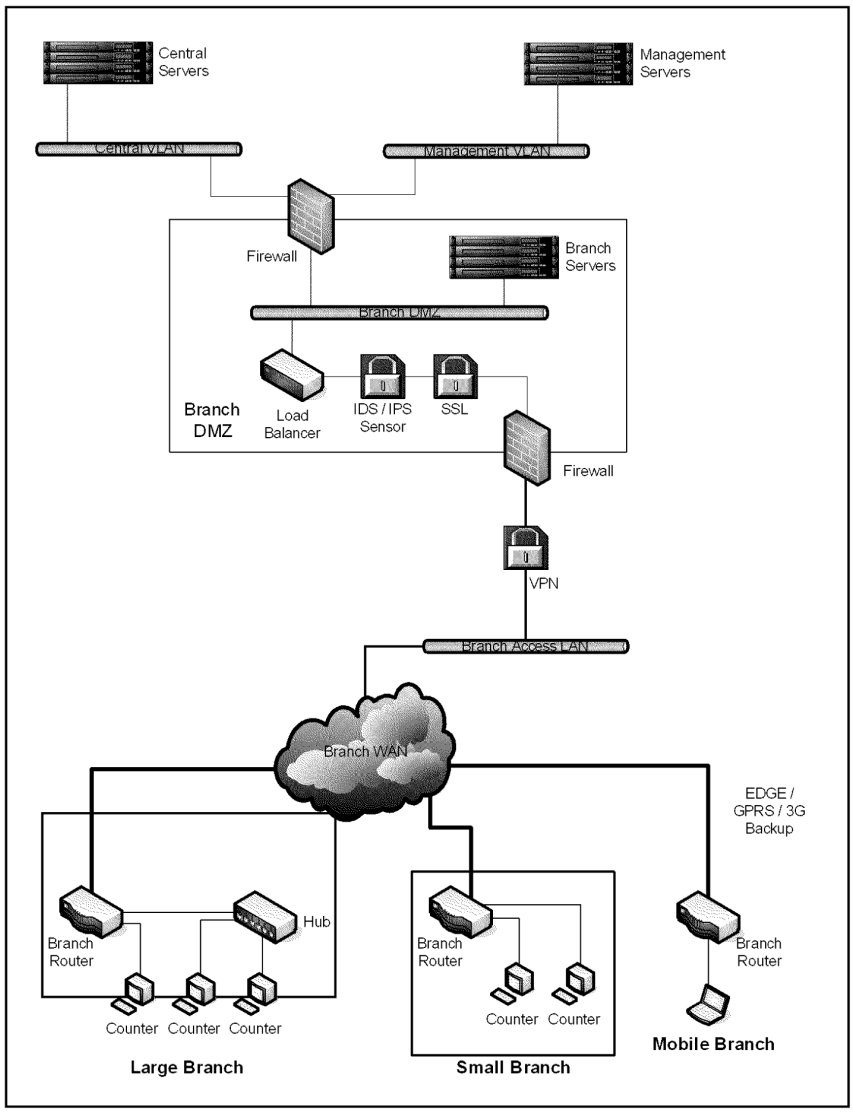


Figure 3 – Counter Networks

Counters can invoke **outgoing** communications with the following nodes:

In the Branch

- Their local Branch Router
- Other Counters

In the Branch DMZ

- Utimaco VPN
- ACE blades

WITN11070106

- Branch Access Layer Servers
- SYSMAN Gateway Servers
- NetCool Object Server Proxies

Management Servers

- Estate Management servers (upon installation only)

Counters can accept **incoming** communications from the following nodes:

In the Branch

- Their local Branch Router
- Other Counters

In the Branch DMZ

- Utimco VPN
- SYSMAN Gateway Servers

Management Servers

- Secure Access Servers (SAS)

WITN11070106

5 Manageability

5.1 Overview

All software components can produce diagnostic trace and other output such as diagnostic events. The high level designs for these components must document what diagnostic trace and diagnostic events are produced.

All software components should follow the principal of reporting incidents through the Windows Event Log. Action must be taken to avoid event storms, for example by limiting the number of times particular errors are reported in any given period.

Log files should be written to a centralised location, where they can be rotated / pruned by the systems management infrastructure. Where individual applications are unable to comply with this requirement, the applications should provide their own 'housekeeping' script that should be executed during daily housekeeping activities.

Components implemented as Windows services can be monitored and restarted if they stop unexpectedly.

Where the user needs to be notified of errors, messages should be displayed to the user via the Counter Business Application to ensure messages are displayed in a consistent manner.

Athene is used to monitor processor and memory usage and can be used to generate events when thresholds are exceeded.

For a full understanding of the manageability aspects of the Counter, the High Level Designs for the individual software components described in section 2 ("Architectural Description") should be consulted.

The Systems Management and Estate Management solutions underpin the Counter's manageability, and are described in the *HNG-X System and Estate Management – Overall Architecture (ARC/SYM/ARC/0001)*.

Any counter hardware changes will be reflected in the contract controlled *Counter Physical Platform Design* document (SD/DES/236) so they can be referred to by Fujitsu Services support staff.

5.2 Data Driven Architecture

The Counter Business Application relies heavily on Reference Data to drive the behaviour of the application.

This reliance on reference data brings us the following benefits:

- Selectively target software enablement at individual branches ("Soft Launch").
- Rapid deployment of new business functionality.
- Rapid deployment of application "fixes".

Within the Reference Data Testing environment special provision needs to be made to allow the counter to run using future dated sets of reference data. All such provisions will be implemented via the Reference Data Manager (see section 2.5.3.4.2.2).

For further information refer to the *HNG-X Counter Business Application Architecture (ARC/APP/ARC/0009)* and *HNG-X Reference Data Architecture (ARC/APP/ARC/0001)*.

WITN11070106

5.3 Software Updates

New and updated software products shall be remotely delivered to the counter by the software distribution and inventory mechanisms in the SYSMAN Framework Agent (see section 2.5.3.3.9).

For further information refer to the *HNG-X System and Estate Management – Overall Architecture (ARC/SYM/ARC/0001)*

5.3.1 SWDistrib

SWDistrib is a utility that allows a software update to be “peered” between counters in a branch.

To enable this capability, the SWDistrib component may be packaged with the update.

The SWDistrib component is not itself listed as a physical component of the counter. This is due to its transient nature, necessary as it contains password prediction algorithms that if left permanently in place on the counter could pose a security threat.

5.3.2 Rendezvous

Periodically, it is essential that software updates are applied uniformly across a branch.

To enable this level of synchronisation a “Rendezvous” component may be packaged with the update. It is the responsibility of the Rendezvous component to ensure that the update is applied uniformly across all of the counters in a branch.

The component will first of all make sure that all of the peer counters are turned on, and in a ready state to apply the software update. On completion, the component will poll the peers until the update has been successfully applied, or until a failure scenario is hit.

In the event of one or more counters failing to successfully apply the update, the update is backed out on all the counters in the branch.

The Rendezvous component is not itself listed as a physical component of the counter. This is due to its transient nature.

5.3.3 Soft Launch

In addition to being able to roll out estate wide software updates, the Post Office has a requirement to selectively enable business functionality on a branch by branch basis.

Within the existing Horizon solution this capability is referred to as “Soft Launch”.

As this capability only applies to business functionality, it is the Counter Business Application that shall provide a similar data-driven capability within the HNG-X solution.

For further information refer to the *HNG-X Counter Business Application Architecture (ARC/APP/ARC/0009)* and the *HNG-X Strategy for Supporting Multiple Counter Versions (DES/APP/STG/0001)*.

WITN11070106

5.4 Remote Support

The HNG-X Counter provides an SSH server to allow access by 3rd Line Support personnel.

SSH access provides command line access to counters, and is used to examine evidence files on the counter, and determine the state of the counter.

In addition, the Counter Business Application provides an interface that allows the application to be started, stopped, and restarted. This interface is available to support users. Invoking this interface will forcibly log off the current user of the application.

Access via SSH is provided by the “Secure Access Server”, which is responsible for authenticating the request to connect to counters in the branch estate, as well as servers residing in the data centre.

For further information, refer to the document *Remote Access and Diagnostics (ARC/SYM/ARC/0004)*.

3rd Line Support also has a requirement to allow remote control of counters in the branch estate using VNC or a similar technology. Unfortunately, this requirement will not be satisfied by HNG-X Release 1 due to both cost and security issues.

WITN11070106

6 Security

6.1 Overview

This section of the document summarises counter software and other measures taken on counters for conformance with the document *HNG-X Security Architecture (ARC/SEC/ARC/0003)*.

6.2 BIOS Settings

To reduce the possible means by which a counter may be compromised, the BIOS settings will be configured as follows:

- A BIOS password will be set to inhibit unauthorised access to the BIOS settings.
- The BIOS will be configured to only boot from the primary IDE hard drive.
- By default, other IDE devices will be disabled, requiring access to the BIOS to add additional devices.

In addition, connection of USB devices is not supported under Windows NT 4.0, rendering this means of compromising the counter void.

However, there are no measures in place to prevent physical intrusion.

6.3 Windows Hardening

The Windows operating systems used on the counter will be hardened using “lockdown” settings, as described earlier in the document.

In addition, the standard Windows NT Graphical Identification and Authentication library (MSGINA.DLL) will be stubbed, allowing key strokes that are used by the operating system to be trapped and overridden (eg. CTRL-ALT-DEL). For further information, see *HNG-X Counter Infrastructure Service & Process Control High Level Design (DES/APP/HLD/0057).*

No additional software will be provided on counters to remove, obfuscate or encrypt transaction, identity or credential information stored in Windows swap files and/or caches.

NB: Within the System Test and Reference Data Test teams, due to the fact that these environments will not be managed by SYSMAN, it will be necessary to provide counters that do not have this level of hardening enabled.

6.4 Authentication

6.4.1 Post Office Users

For Post Office users, user authentication at the counter is performed by validating user-supplied credentials against data in the Branch Database, accessed via the Branch Access Layer Server. The Windows authentication mechanism on counters will be changed so that when counters boot-up, the default logon prompt will be application-generated.

To obviate the need for Post Office user passwords to be transferred across the network during login, only the user’s account name will be transferred from the Counter to the Branch Access Layer server. A token encrypted with a symmetric key derived from the user’s password will then be returned to the Counter, and this token will be decrypted at the Counter using the password entered by the user. If the

WITN11070106

token is decrypted successfully, then it will be returned to the server along with a new asymmetric public key created on the Counter and valid for all future communications within the current user session.

Once users are logged in, their screens will be locked automatically after a period of inactivity. Furthermore, if the period of inactivity is long enough, users will be logged out automatically.

Users will only be granted access to functionality running on counters at their branch.

It has been agreed that for HNG-X, two-factor authentication where a user has to provide a smart card in conjunction with a password will no longer be required for Post Office users, and that the two-party authentication (as currently provided by Horizon's Postmaster Logon [PoLo]) will not be required following the reboot of a counter.

6.4.2 Global Users

Despite the fact that counters will present an application logon prompt after booting, there must still be some mechanism to allow global users such as field engineers to access the counter, especially as they may be required to perform diagnoses or repairs when there is no connectivity to the Data Centres.

When there is network connectivity to the Branch WAN, global users will authenticate in exactly the same way as Branch users, with the Branch Access Layer providing this transparency.

When there is no network connectivity to the Branch WAN, the counter must allow a field engineer to access network diagnostic data provided by CNIM, and other peripheral functions, but no business transactions will be available.

A global user account will also be responsible for the final provisioning of new branches, where it will be their responsibility to create the post master's account (and optionally any other accounts needed).

6.4.3 Remote Support Users

Remote shell access to counters will only be possible from the Secure Access Server (SAS), and only via the SSH Server on the counter.

Remote support user passwords will be stored on local hard disks, but only in encrypted form.

It will also be possible to invoke pre-defined diagnosis scripts (often called "remote tasks") remotely, and have output redirected to a SYSMAN console, though this access will be via SYSMAN, so will not demand separate authentication on the counter.

SSH makes use of public / private key pairs authenticated by the Secure Access Server. For further information, see the *Remote Support High Level Design (DES/SYM/HLD/0017)*.

6.4.4 Service Accounts

A number of software components on the counter will need special Windows accounts, and in some cases these accounts will need local administrator access.

Passwords for these accounts will be stored locally on each counter, but Post Office users and field engineers will not have any access to them.

In the case of locally-installed Systems and Estate Management components, these accounts may then be used to perform scheduled SYSMAN tasks, or pre-defined ad hoc diagnosis tasks on behalf of remote users. However these accounts will not be used for undefined interactive shell sessions.

Details of the required system users must be defined during the high level design and documented in the relevant high level design documents, including the minimum privileges that these users should be assigned.

WITN11070106

In-built Windows system accounts which are not required (such as “Guest”) will be changed or disabled as part of the “lockdown” of the operating system (see earlier).

All such accounts should follow the principles of “least privilege” from the point of view of the file system, registry, and network access.

Service accounts requiring a password must be secured using a 22 character randomly generated password. The password will never be changed unless it is suspected/detected that the account has been compromised.

For file system access, security should be applied at the directory level rather than file level, although there may be exceptions to this (such exceptions must be justified and agreed with the Security Architect).

Network access should only be provided if explicitly required and, even then, must be restricted to the minimum level necessary.

Registry access must be read only unless otherwise required.

Service accounts must not be used for interactive console or remote login.

Generally, service accounts should not be Administrator equivalent. If there is a requirement to make a service account Administrator equivalent, this must be justified and agreed with the Security Architect.

Applications must use service accounts in the following order (i.e. “Logon As”): [1]

1. Local Service
2. Network Service
3. Unique User Account (with minimal permissions necessary to work)
4. Local System (should not be used unless unavoidable)
5. Local Administrator (should never be used unless agreed with security)
6. Domain Administrator (must never be used)

NB: Any service not using (1) or (2) must be approved by the Security Architect.

The standard naming conventions for service accounts as defined by the Security Architect should be used.

6.5 Interactive Users

Each co-habiting application on the counter that is exposed to the end-user should run under its own unique Windows user/identity.

Such accounts should be non-privileged accounts, and follow the security principal of least privilege, and only enable access to those resources necessary to function as intended.

6.6 Access Control

The principle of least privilege will be applied to all interactive and non-interactive counter users. A set of roles will be defined, and users and system components will only be granted the roles they require to perform the tasks required of them.

Each role will correspond to a set of HNG-X application rights, a set of Windows NT file access rights, and a set of Windows NT system rights. All HNG-X users authenticating with the Branch Database will

[1] This list is provided s part of the HNG-X security guidelines, and primarily applies to Windows 2003 and later, but the principals should be adhered to under Windows NT 4.0 where feasible.

WITN11070106

share a single Windows user account, so will inherit the same set of underlying Windows rights, but access to use those rights will be further restricted by the application role.

In practice this principle is constrained somewhat by the prevalence of Commercial Off-The-Shelf (COTS) Windows software which is written assuming local administrator access, so in many cases it may be necessary to grant administrative access to several locally-installed software components.

6.7 Encryption

All network traffic between the counters in the branch, and between branch counters and the data centre will be encrypted over a VPN using the Red Pike cipher.

In addition, all business traffic between the Counter Business Application and the SSL termination points in the Data Centres will be encrypted using SSL encryption.

Public server key data for SSL termination devices will be created by Certificate Authority servers, and pre-distributed as signed certificates to all live counters.

Certificate Revocation Lists (CRLs) and new certificates may be distributed by SYSMAN as required.

If there are more Counters than expected operating at a branch, extra ones will be prevented from performing business transactions, and the variance will be reported. This functionality will be provided within the HNG-X Application rather than by the Counter infrastructure.

6.8 Non-Repudiation

Counter transactions will be written to the Branch Database in the Data Centres before they complete. Each transaction will be traceable back to a specific Post Office user account and a specific Post Office counter.

All remote interactions between support users and counters will be logged by the SAS Server.

It is worth noting that event data from Counters will not be archived for audit purposes, so any data necessary to support audits must be moved elsewhere.

6.9 Denial of Service

No new security updates are being produced by Microsoft for Windows NT 4.0 Workstation.

No anti-virus, anti-spam, anti-spyware or intrusion detection software will be installed locally on counters. This has been judged unnecessary. The risk of infection is relatively low, based on the protection offered by VPN, the secure sessions used between the Counter Business Application and the Branch Access Layer, coupled with the fact that no business data is stored on the Counter.

6.10 Data Security

In accordance with the *HNG-X Security Architecture (ARC/SEC/ARC/0003)*, no confidential or sensitive information shall be persisted on the counter, including within log files.

The Counter Business Application will be chiefly responsible for realising this requirement. For further information refer to the *HNG-X Counter Business Application Architecture (ARC/APP/ARC/0009)*.

WITN11070106

7 Recovery & Resilience

7.1 Overview

Counter failures have a more limited impact on the Post Offices overall ability to a service than failures that occur in the central Data Centres.

Nonetheless, it is important to consider Counter failure scenarios, making adequate provision for remedying or working around them.

This section considers a number of possible failure conditions affecting counters, and describes how they will be handled.

For more information, readers are referred to *HNG-X System Qualities Architecture (ARC/PER/ARC/0001)*.

7.2 Counter Hardware Failure

If permanent or intermittent failures occur in counter input or output devices such as printers, monitors, keyboards and scanners, they will be noticed quickly by Post Office staff attempting to use them, who will be trained to log helpdesk calls. Engineers will attend the branch to repair or replace the hardware using spare Counters at the most recent spare baseline.

For further information on the spares strategy, see the document *HNG-X Migration High Level Design for Branches (DES/MIG/HLD/0001)*.

Intermittent failures affecting internal subcomponents such as hard disk drives may not be visible to users, but should result in events being written to the Windows event logs, where they can be picked up by SYSMAN and subjected to event correlation, to see if a pattern of failure is developing.

Counters connect independently to the Data Centre via a Branch Router, so the failure of a single counter usually only affects one user and only until a repair or replacement can be affected. For this reason it will not be cost-effective to include redundant hardware subcomponents in Counters.

7.3 Counter Software Failure

If any software component experiences a pattern of software failure in testing, then root cause analysis will be undertaken and a fix applied.

Unfortunately, large-scale systems integration projects occasionally uncover patterns of software failure in Commercial Off-The-Shelf products, which cannot be reproduced or fixed by their vendors. If such problems are found, then alternative software will be considered, or additional SYSMAN or Housekeeping tasks will be incorporated to reduce their impact.

It is possible to configure SYSMAN so that fatal software failures experienced in the estate will be recognised by SYSMAN's monitoring agents, and events will be created, which will trigger alerts to operators who can intervene to diagnose the problem.

Non-fatal software failures experienced in the field are also likely to be reported in Windows event logs or in proprietary log files. Whilst these may not immediately have any effect on the service, they present a risk of more significant associated problems occurring later on. During pilot it may be necessary to make the filters that escalate events more restrictive where extraneous events are being created.

WITN11070106

7.4 Counter Data Failure

No transaction data is held locally on the Counter's hard disk drive, so there is no requirement for a data recovery process from failed Counter PCs.

All data stored locally on counters is used by at least one software component, so if software components discover data integrity or corruption problems in their data they will write error or warning events to their logs, which will then be forwarded to operators as for "Software Failure" (see earlier).

7.5 Failure of other Counters

In multi-counter branches there are some circumstances where the failure of one counter could cause an outage to the auxiliary functions on other counters at the same branch:

- Where the failed counter was acting as a local software distribution staging post.
- Where the failed counter was sharing a report printer.

The Counter High Level Design must consider how best to minimise the effect of the failure of one counter on other counters at the same branch.

7.6 Network Failure

All HNG-X branches will have their own locally-installed Branch Router, which will detect WAN connection failures, and switch to an alternative connection type without the need for users to restart their application sessions. Depending on their duration, WAN failures are classed as "transient", "longer" or "permanent", and the impact of each type of failure on the user depends on the type of transaction they are trying to undertake. For more details readers should refer to *HNG-X Branch Exception Handling Strategy - Agreed Assumptions and Constraints (REQ/CUS/STG/0002)*.

A network failure on the LAN is much less likely because of the relative simplicity of the network infrastructure, but could occur in a single counter, in the Branch Router, or in the Ethernet hub or cabling. If the LAN fails, all business transactions for all affected users will be prevented, so users will report the problem to the helpdesk who will deploy an engineer to repair or replace the faulty hardware.

The Counter Business Application will be aware of the state of the network by interacting with CNIM, and will not offer services to the clerk when no WAN connection is available.

7.7 Server Failure

Counters connect via the Branch Router to a number of server platforms. All such platforms are deployed in redundant configurations, such that a single server failure has no significant impact on counter operations.

7.8 Data Centre Failure

If the live Data Centre fails, Counter connections to Data Centre-resident servers will be broken.

No reconfiguration of the counter will be required in order for reconnect to the secondary Data Centre, though users will need to restart their sessions and re-authenticate.

WITN11070106

8 Performance & Capacity

8.1 Overview

This section describes the approach to performance engineering for HNG-X Counters.

For more information, readers are referred to the *HNG-X System Qualities Architecture (ARC/PER/ARC/0001)*.

8.2 Peak Volumes

Under normal operations, Counters are only involved in processing business transactions on behalf of a single Post Office user, so they are not subject to the same capacity peaks as central servers. This means that there is limited value in maintaining formal models of predicted counter transaction volumes.

More significant counter maintenance operations, which might otherwise affect response times for Post Office users, will be scheduled to run outside normal hours.

It will still be necessary to confirm that a single counter can perform all necessary business transactions and supporting functions for a peak day without adversely impacting response times, but the risk of problems at peak times is much lower on a counter, so this can largely be assessed during testing.

8.3 Normal Business Volumes

A general concern results from the relatively low specification of the current counter hardware.

Recent performance studies on the counter indicate good performance, but have focussed fairly narrowly on specific Java libraries and functions where the perceived performance risk was higher.

Early counter performance studies were more holistic, and also suggested that there is adequate capacity in both counter hardware and also on Branch LANs to run a J2EE application. However there is little documentary evidence of this.

To mitigate this risk, the performance and capacity of the counter will be subject to continuous assessment throughout the HNG-X delivery. As soon as new information emerges, the counter performance should be re-analysed, and as soon as prototype applications and other early releases of software components become available they should be loaded onto representative counter hardware and tested.

8.4 Known Performance Issues

8.4.1 Slow Drives

It is known that there are numerous hard drives installed in Counters in the Live Estate that have sub-optimal performance characteristics.

A study has been undertaken to asses the number of Counters in the estate that are affected, and the impact on performance that this has.

The study found that in excess of 70% of the estate is affected, and that the latency caused by these slow drives can affect the performance of operations that write to the hard drive considerably. In tests it was observed that operations can take up to 8 times as long as the replacement drives currently in use.

This is significant, and the design of software components must attempt to limit disk I/O as much as possible to mitigate this issue.

WITN11070106

WITN11070106

9 Migration

This section is not relevant one migration has taken place (HNG-X Release 1). It is left in this version of the document for information purposes.

9.1 Overview

Bearing in mind the large number of Horizon Counters, and the large number of sites amongst which they are distributed, it is worth giving some consideration in this document to the means by which the transition to HNG-X will be handled across Counter PCs.

Several of the HNG-X migration activities covered in the *HNG-X Migration Strategy (ARC/MIG/STG/0001)* will result in changes to the counters. These include:

- Branch Network Changes (A3)
- HNG-X Application Pilot and Rollout (X3 and X4)

No special consideration needs to be given to the migration of the mobile counter, the PHU 1.5 to the PHU 2.0, but there are some considerations that need to be given to the PHU spares strategy. These are discussed in section 3.2.1.

Detailed architectural information on all of these activities can be found in the *HNG-X Migration Strategy (ARC/MIG/STG/0001)*, but activities X3 and X4 affect Counter PCs so significantly that they warrant separate mention in this section.

9.2 HNG-X Migration Enabling Upgrades for Data Centres

No impact on the Counter.

9.3 Data Centre Build

No impact on the Counter.

9.4 Move Wigan Network Management Servers

No impact on the Counter.

9.5 Data Centre Preparation

No impact on the Counter.

9.6 Cutover Rehearsal

No impact on the Counter.

9.7 Migration of POL FS

No impact on the Counter.

WITN11070106

9.8 Migration of Batch Services

No impact on the Counter.

9.9 HNG-X Specific Services

No impact on the Counter.

9.10 Migration of Online Services

No impact on the Counter.

9.11 Migration of Audit Services

No impact on the Counter.

9.12 Migration of Branch Services

No impact on the Counter.

9.13 Move Bootle Network Management Servers

No impact on the Counter.

9.14 Decommission Wigan and Bootle

No impact on the Counter.

9.15 Horizon Counter Changes for PCI Compliance

Details of the changes required to the Horizon counter are outlined in the *Migration Strategy (ARC/MIG/STG/0001)* and covered in detail in the *Migration High Level Design for (DES/MIG/HLD/0001)*.

9.16 HNG-X Migration Enabling Upgrades for Counters

Details of the changes required to the Horizon counter are outlined in the *Migration Strategy (ARC/MIG/STG/0001)* and covered in detail in the *Migration High Level Design for (DES/MIG/HLD/0001)*.

9.17 HNG-X Application Pilot & Rollout

9.17.1 Software Distribution

New HNG-X components will be rolled-out to each branch's Horizon Gateway counter using the existing Horizon SYSMAN Software Distribution subsystem. The Gateway will then be used as a staging area from which other counters can copy HNG-X software files.

WITN11070106

The size of the HNG-X software will exceed the maximum which can efficiently be delivered in a single package, so multiple packages will be delivered, with larger components being split into multiple packages prior to transit if required.

9.17.2 Pre-Installation

A number of pre-requisite activities must have been completed at the branch before its Counters are upgraded to HNG-X. These include communication with branch staff, the application of a Horizon software upgrade which enables the migration function, the preparation of transaction summaries, and a series of pre-migration checks.

For more details please refer to *HNG-X Migration Strategy (ARC/MIG/STG/0001)* and *HNG-X Migration High Level Design for Branches (DES/MIG/HLD/0001)*.

9.17.3 Software Installation

The migration of the Horizon counters to HNG-X must be conducted as a unit of work at each branch. In the event of a failure to migrate a sufficient percentage of counters at a branch, or a failure to migrate the Gateway counter, all counters at the branch must be rolled-back to Horizon before trading can resume.

Each package will be able to be backed-out, irrespective of whether or not it installed successfully.

During migration counter identity data will be migrated (eg. Branch Id, Counter Id, etc).

For more details please refer to *HNG-X Migration Strategy (ARC/MIG/STG/0001)* and *HNG-X Migration High Level Design for Branches (DES/MIG/HLD/0001)*.

Special considerations apply to the migration of the Utimaco VPN from Horizon to HNG-X to ensure that connectivity between the branch and data-centre is retained during migration. For further information refer to the *VPN on HNG-X NT High Level Design (DES/MIG/HLD/0006)*.

A number of additional considerations will need to be addressed during migration, such as:

- The video driver settings will need to be set to be uniformly 800x600 resolution and 16-bit colour depth;
- The Epson counter slip printer will need to be set to native Epson mode, running at the highest available port speed.

9.17.4 Post-Installation

After a branch has been successfully upgraded, the Post Master will be required to run one or more post-migration reports. The post master will be prompted to accept the migration. On acceptance, there is no possibility of regressing to Horizon. This is referred to as the “point of no return” in the migration strategy.

Once the point of no return has been reached, all redundant software and data components will be removed or disabled on all of the counters in the branch. The following tasks will be undertaken to support this:

- Horizon’s Secure File Store will be securely deleted (using SDELETE.EXE).
- Horizon’s Connection Manager software will be removed.
- Horizon application software will be removed.
- Escher software will be removed.
- Any Windows NT services or drivers which are no longer required will be removed.
- Unused disk partitions will be removed.

WITN11070106

During high level design, consideration will be given to whether these activities need to be performed as a single activity, or can be split into a number of separate activities committed over a number of days.

For more details please refer to *HNG-X Migration Strategy (ARC/MIG/STG/0001)* and *HNG-X Migration High Level Design for Branches (DES/MIG/HLD/0001)*.

9.18 Branch Router Rollout

Branch Router changes apply to the Horizon Counter only, and for the purposes of this document and are out of scope. For further information, see the *Branch Router Topic Architecture (AR/NET/ARC/0003)*.

Completion of the Branch Router Rollout is a pre-requisite of the migration of both fixed position & mobile counters to HNG-X.

9.19 Counter Event Management Changes

Netcool Probe will be delivered to Horizon, and during the migration to Branch Router, the existing TecNTAdapter will be disabled, and Netcool Probe activated to allow event reporting to SYSMAN3.

For further information see *MON – Supporting Agents (DES/SYM/HLD/0002)* and *SYSMAN-HYDRA Support High Level Design (DES/SYM/HLD/0007)*.

The Counter Business Application and other components of the counter that are being replaced or modified under HNG-X will produce a different set of events when compared to Horizon. The details of these events will be documented in the relevant product design material.

9.20 Counter XP Upgrade

The migration to Windows XP is out of scope for HNG-X Release 1.

9.21 Post-Application ADSL Changes

No impact on the Counter.

9.22 Final Decommissioning

No impact on the Counter.

9.23 Estate Management Upgrade

No impact on the Counter.

9.24 Post Migration Spares Changes

Once the migration of the entire estate to HNG-X is complete, the counter spares pool will be updated, with all Horizon spares being decommissioned / rebuilt.

Specifically, the following changes will be necessary:

- Horizon counter spares will be rebuilt as HNG-X only spares.
- Counter slip printers will be rebuilt and configured in native mode at the HNG-X baud rate. Counter slip printers are currently built and configured to run in Ithaca mode running at a slower baud rate.

WITN11070106

10 Testing & Validation

10.1 Overview

Counters are regularly subjected to indirect functional testing, as they are used in most test environments to introduce business transactions to test systems. However this section focuses on any additional testing and validation considerations which relate specifically to the HNG-X Counter, and which might not be adequately addressed by functional testing alone.

The overall approach to testing, constructing test environments and test governance is documented in the *HNG-X Testing Strategy (TST/GEN/STG/0004)*.

10.2 Counter Variants

All hardware-sensitive tests must be run on all supported types of counter workstation, with all WAN protocol types and all supported types of peripheral.

10.3 Operational Business Change (OBC)

Tests must be run to confirm that new “spares” can be introduced into the estate, either in new counter positions or to replace failed counters. The tests should confirm that a newly introduced spare counter has an equivalent software baseline to a counter which has been live for some time, and has received a series of software and reference data updates.

Testing should concentrate on validating the behaviour of the System Activities associated with OBC and EST Use Cases that directly impact counters. Eg:

- Opening a Branch
- Closing a Branch
- Adding a Counter
- Removing a Counter
- Changing an attribute of a Branch / Counter

10.4 Security Testing

As well as testing the efficacy of the security controls designed into the system, Fujitsu Services will also employ independent vulnerability testers who will stage attacks from counters in test environments.

10.5 Recovery and Resilience Testing

The failure scenarios discussed in section 7 will be tested during the delivery of HNG-X.

10.6 Performance and Capacity Testing

A profiling tool (such as JProfiler) must be used during development of the Counter Business Application to test performance, and ensure that the memory footprint of the application does not exceed agreed limits.

If possible, automated performance tests will be incorporated into the Counter Business Application continuous integration environment.

WITN11070106

Testing tools such as Mercury's Quick Test Professional will be used to simulate counter transactions submitted to the Branch Access Layer Servers.

Prior to delivery, the Counter must be tested using an agreed "typical basket mix" of products to assure that similar levels of performance can be achieved or exceeded under HNG-X compared to Horizon.

Video benchmarking will cease to be used under HNG-X, with the Counter Business Application providing an integrated Transaction Benchmarking capability. Initial testing of the Counter should use both video benchmarking and the new integrated capability to ensure consistent timings.

10.7 Migration Testing

The HNG-X migration is phased, meaning that live counters undergo several state changes before it completes. Migration testing of each counter release is undertaken separately from its functional testing. Once a counter release has been functionally tested then separate tests are run to validate the process for migrating to that release. Selected functional tests are then repeated on the migrated counter to ensure that the migration process was successful.

In the event of a failure associated with migration, a counter should execute regression scripts to roll back to the state prior to migration. It is equally important that these regression scripts are thoroughly tested.

WITN11070106

11 Risks, Issues & Assumptions

11.1 Overview

This section captures the major assumptions, risks and issues relating to this topic architecture.

11.2 Assumptions

1. There will be sufficient spare disk space on counters to store and un-package software packages required for the HNG-X Rollout.
2. The replacement of all PHU 1.0 mobile counters and “luggable” counters (DOLT, SOLT) with the PHU 1.5 mobile counter is a pre-requisite of the commencement of the HNG-X counter migration (on a branch basis).

11.3 Risks

Risks associated with this architecture are tracked externally in the Architectural Risks / Issues Register.

11.4 Issues

Risks associated with this architecture are tracked externally in the Architectural Risks / Issues Register.

WITN11070106

12 Requirements Traceability

Traceability of Business, Customer Service and System Requirements is detailed in a separate Traceability Matrix designated *ARC/APP/RTM/0008*.