Host Terminal Facilities

Overview

NHDS have many years experience in producing high quality host terminal facilities for use with our remote monitoring products. These software packages provide a wide variety of facilities for handling remote monitoring systems of any size.

The function of the host terminal is to gather status information from remote units and present this information to the user in a suitable manner. The host terminal should additionally allow the user to review historical data and to configure and program the system as a whole as well as individual remote units.

Whilst NHDS provide a number of standard host terminal software packages for use with the product range, we can also provide bespoke solutions completely tailored to a customers specific requirements. In most cases, however, this is not necessary, as the standard software is constantly evolving as new features and interfaces are added, providing a user interface and system management tool that caters for most needs.

Scalability

NHDS host terminal software is designed to be used with any size system from just a few remote units talking to a single host PC right up to 10,000 unit systems with multiple host terminal displays across geographic regions. At the heart of each of these systems is the same basic piece of software.

In the most basic system, the host terminal software is installed on a single PC, which has a single modem connected to it for communicating with a number of remote monitoring units.

As more remote units are added to the system, additional modems can be added to the PC (utilising a multi-port serial card once the PC runs out of serial ports, or USB modems as an alternative) to provide more access to units in the field.

When more people require access to the host terminal, additional host terminals can be installed, using the same software, sharing database files across a simple local area network. Individual host terminals can be separately configured to provide differing facilities for each terminal.

For more robustness and to produce a true client/server system, an industry standard database, such as Oracle, SQL Server, SyBase Server, etc. is added to become the heart of the system. More client terminals with attached modems (acting as modem servers) can be added to increase fault tolerance. Client terminals can now operate over wide area networks, so remote offices can also access the system.

If more robustness is required, the database engine itself can be configured as a replicated database, so an up to date copy can be maintained at another location, which can be switched to in the event of a failure.

With a standard database engine in the system, a web server can be used to provide a web based interface to the system, so anyone with an internet browser can access the system over the local area network or even the Internet.

At any point, the NHDS host terminal can be configured to interface to a third party system (e.g. a customer's own management or SCADA system) using a variety of technologies. In this configuration, the host terminal can act purely as a "black-box" data concentrator.

Throughout all of these types of host system, the basic building block is the same standard piece of software. All that is changing is either configuration or the addition of widely available off-the shelf database software.

Protocols

One of NHDS's primary skills in providing host terminal packages is our extensive experience in communication protocols. NHDS have over 20 years experience in interfacing with equipment using an ever increasing variety of protocols, from simple ASCII serial interfaces, through to full SCADA protocols, such as DNP3.0 or IEC807 and including specific protocols from a variety of industries such as security, road transport, telecommunications, mobile data, etc..

NHDS have also, in the past, developed proprietary protocols for themselves and third parties.

NHDS were the first company in the UK to implement the RAM Mobitex protocol on an embedded device. We were also one of the first providers in the world to be invited by Motorola, Vancouver, to develop a host terminal operating over the DataTAC network, a terminal that was widely used in exhibitions around the world by Motorola and their partners to promote the then new mobile data network. NHDS host terminals were also amongst the first non-security application to operate over the British Telecom security network RedCare (also known as Telecom Red), acting as an "*Alarms Receiving Centre*" on the network.

Current standard protocols utilised by NHDS host terminals include (interface to remote units, third party systems or other equipment).

◆ DNP3.0 ◆ WISP+ ◆ Mobitex ◆ DataTac ◆ SIA Seciruty Protocols ◆ Red Care (Telecom Red) ◆ OPC ◆ ODBC ◆ MPT1327 ◆ MPT1379 ◆ Hayes AT ◆ NMEA ◆ IEC 870 ◆ RdLap ◆ NMCS2 ◆ ESI PMR ◆ MAP 27 ◆

Aside from the above, NHDS have also produced interfaces to numerous proprietary protocols, both those designed by NHDS and those used by customers.

Bespoke Development

Although the standard software can be configured and connected together to provide for most needs, NHDS recognise that it is impossible to cater for all requirements. We are therefore very flexible when it comes to customising software to cater for special needs.

We can provide simple tweaks to any of the basic software packages or can provide complete bespoke developed software solutions.

Basic Facilities

NHDS host terminals provide a host of common features. This feature list is constantly evolving as more facilities are added as a result of customer requests or development strategies. The current list of features include the following items:

- Ability to operate as a stand-alone software package or as part of a client server system with multiple client terminals providing the human interface to the system.
- Ability to handle up to 16 modems on a single PC for communication with the remote monitoring units. In a client/server system , any client terminal can be equipped with modems to act as a modem server. There can be any number of modem servers, giving greater resilience and fault tolerance.
- The terminal can use its own proprietary database format for storage or can interface to an industry standard database engine such as Oracle, Microsoft SQL Server, SyBase Server. This allows small systems with perhaps only one stand-alone host terminal to operate without need to purchase additional software to provide the required database facilities. Larger systems, however, have the ability to use a standard database management system to provide greater flexibility and security of the stored data. Using a standard database also allows mechanisms such as wide area network clients or database replication (where a copy of the database is maintained at another location, constantly being kept up to date, which can be reverted to in the event of a failure on the main database server) to be utilised.
- The current status of any or all units in the system can be displayed in a variety or formats. The user can customise the information displayed.
- There is the facility to view historical archives of events and to apply various levels of filtering to such displays.
- There is a report generation facility which can be used to produce a number of different reports derived from collected data. Reports can be configured to run automatically at given periods and for the resultant report to be emailed to one or more addresses.
- External indicating equipment (alarm panels, sirens, flashing lamps, etc.) can be interfaced to using fitted relay output cards. Any relay output can be configured to indicate one of a number of circumstances, ranging from the state a specific input on an individual remote monitoring unit to an indication there is something for a user to view on the host terminal (i.e. any fault on an any unit or a system specific fault such as a faulty modem).
- Data can be exported to and imported from third party database or spreadsheet packages, allowing manipulation and analysis of data offline.
- Data can be archived to external files to keep database sizes to practical limits.
- The system monitors units and warns of any units not reporting in. The system can also be programmed to attempt to contact any such units automatically (where units are contactable).
  When multiple client terminals are used, client terminals also monitor the status of key terminals such as

modem servers, reporting when such devices are offline or not responding. System faults, such as loss of a modem on a modem server are detected and reported to all client terminals in the system.

- Automatic backup of system data files, including the proprietary database files if used.
- The terminal can interface to third party systems such as SCADA hosts or management systems via a number of different methods including ODBC, TCP/IP, RS232, etc.
- When using GPS equipped remote units, the terminal can interface to a connected mapping package, such as Microsoft Autoroute or Mappoint, to allow real-time display of location. The terminal can be configured to actually turn on location monitoring of such units when certain alarm conditions are met (e.g. monitoring the location of a vehicle when the car alarm is triggered).

Interfacing to Third Party Systems

One of the main concerns of many customers is how to integrate an NHDS remote monitoring system into an existing enterprise management or SCADA system. In this regard , NHDS provide a wide variety of interface options to third party systems and are happy to provide custom solutions whenever required. The standard means of interfacing at the moment includes:

- ODBC - a connection to an industry standard database system such as Oracle, SQL Server or SyBase Server
- TCP/IP – connection can be made across a TCP/IP network using a pipe to a number of addresses simultaneously. The format of data can be customised by the user or specific protocols can be adhered to or developed for specific customer requirements.
- RS232 serial interface using a wide variety of protocols. Customer protocols can be developed on request.
- File based interfaces – exchange of data between systems using disk files
- Email – the standard system can generate and send email messages, in a user defined format, to any number of mail addresses.
- SMS Text messages – the system can transmit reported events to a number of mobile phones or pagers.

Case Study 1- Norweb/United Utilities

The system described here is a power outage monitoring system installed at United Utilities (formerly Norweb) in Manchester, with additional client software being installed at various regional offices and depots. The customer provides electricity supply to the north west of England and had a requirement to reduce the amount of *customer minutes lost* (CML) due to power outages. The electricity watchdog in the UK had introduced penalties for those regional electricity distribution companies that were not improving the figures associated with customers being off supply.

It was decided that the best way of reducing this amount of time was to increase the speed at which the electricity board was informed of faults in the first instance. Previously, in rural areas, it was often a call from a customer reporting a loss of supply that prompted an investigation into a fault. This call could be received some time after the actual fault had occurred, especially when faults occurred during the night, leading to unnecessarily long periods without power . The system installed by NHDS, known as the PODS system (power outage disturbance sensors), utilised several thousand POD sensors installed in domestic customers premises. These sensors are connected to a customers mains supply, usually via a domestic 3 pin socket, and also are connected to the customers phone line. When any loss or restoration of power (permanent or momentary) is detected, or voltages exceeding predefined limits detected, the POD units call the host system using a toll free phone number (so that the customer is not paying for the call) and report their status. The host system can then report such faults and also determine if a fault is confirmed or not by examining data from other POD sensors on the same high voltage (HV) circuit. This is to detect the situation where a customer unplugs a sensor temporarily or has a localised power loss, e.g. a circuit breaker tripping.

Using this system, United Utilities were able to reduce the amount of time it took to restore faults by an average of about about 10 to 20 minutes on rural areas.

The host system was also used to generate reports of *customer minutes lost* data for examination by the watchdog as proof that they were taking action to reduce the CML and *time to restoration* figures.

As the system was first installed, it was decided that other facilities could be added to the system, and as such, United Utilities commissioned a series of custom software packages and modifications to the standard software to enhance the system. These included a report generation client terminal that would generate a variety of reports specifically tailored to the customer, a relay control terminal that would control a series of external indicators so that problems could be flagged up in a busy control room without having to examine computer screens or listen to audible indicators and a custom client terminal that would look at data from multiple POD sensors to aid in pinpointing where a fault might lie on the distribution network (the standard client terminal would report which sensors had reported faults, but the custom one would report which area of the distribution network had a problem and aid in pinpointing the exact location of the fault.

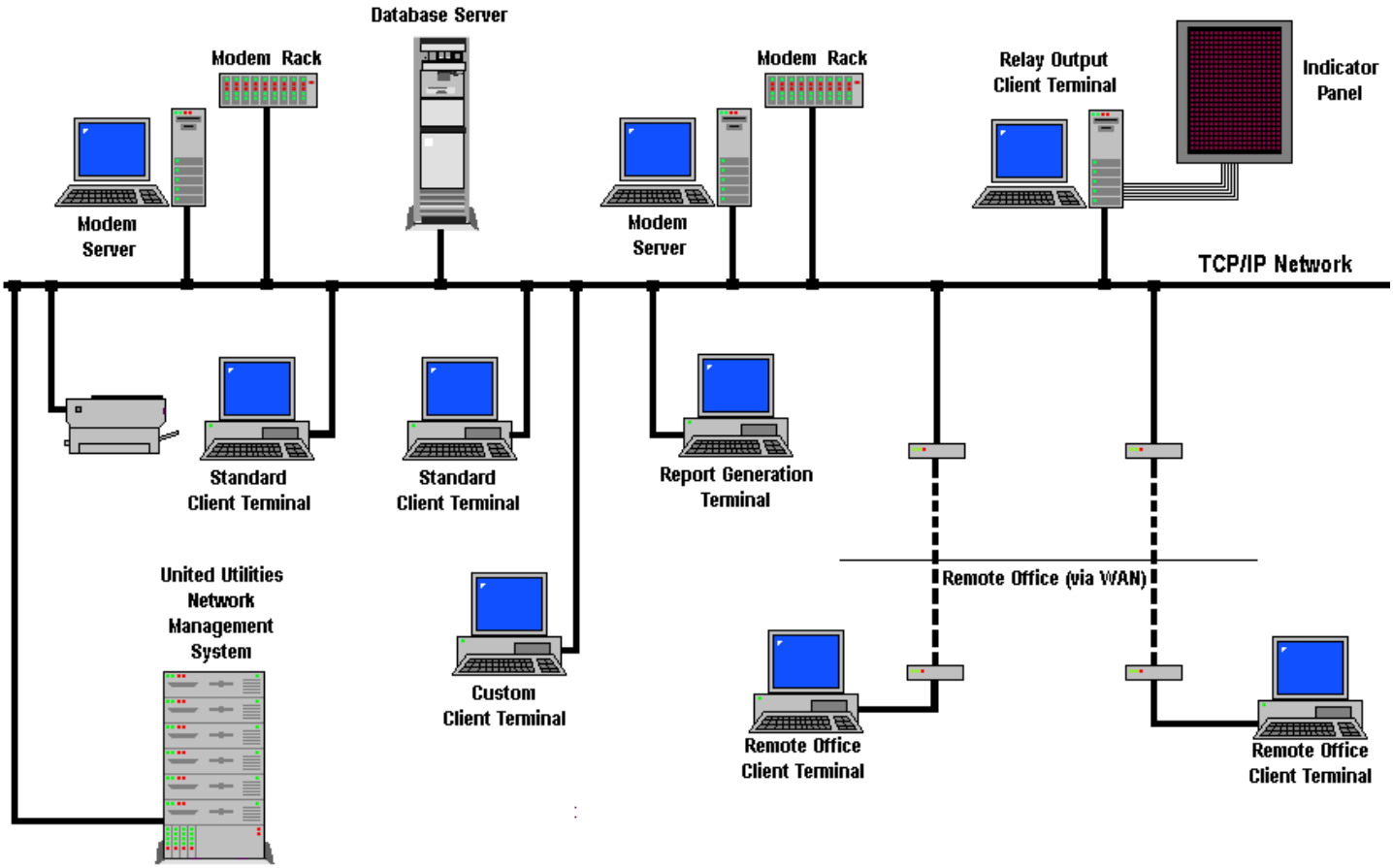
At a later stage, the system was modified again to interface to the network management system (NMS), which controlled and monitored the actual electricity supply network and also the TroubleCall system, which placed automated messages on the customer fault reporting phone lines informing callers that a fault was known about and being dealt with without operators having to be involved. Initially this interface was through file exchange, but this was eventually facilitated by SQL queries being run on the system database by the customers network management system and also the customers own report generation software run on individual terminals.

Additional benefits of the PODS system were that United Utilities were able to produce evidence when dealing with complaints from customers about quality of supply (voltages being too high or low at times, or spurious power outages occurring too frequently) and would install sensors at locations where complaints had been received to help in identifying and correcting such problems. The information gathered by the PODS system was also used in determining the schedule of when to cut trees close to overhead cables, as a report generated by the system could identify likely instances of nearby tress knocking against the lines and causing frequent yet short momentary power outages.

System Description

In brief, the system is comprised of a central database server holding the system database and there are two terminals acting as modem servers receiving calls from the POD sensors in the field. There were then 16 client terminals situated at a variety of geographical locations within the Norweb area. These consisted of the standard host terminal for those people who required full status information, the custom terminal for other positions which required details on where faults actually were, most of which were configured to just show the faults pertaining to particular areas. One client terminal was linked, via relay output cards to an indicator board in the electricity supply control room and the remaining terminals were report generation terminals, which were used on demand to produce statistical reports for internal use and for use with the watchdog authority.

The diagram below shows the main elements of the PODS system for United Utilities.



The individual of elements of this system are as follows:

- Database Server
  This is the heart of the system where all the status and historical data is stored. This was originally a low cost Sybase Server running on a Windows 98 desktop PC but was later changed to an Oracle 9 database management system running on a Windows 2000 server PC. The reason for the change was to maintain database standards with the rest of the organisation.
- Modem Servers
  The system contains 2 modem servers to receive the calls from the POD sensors. Each server consists of the standard host terminal software installed on a Windows 2000 server PC mounted in a rack in one of the customers server rooms controlling a rack of modems (attached via TCP/IP). There can be up to 16 modems on each server.
  Although these terminals are not used with permanent monitors or keyboards, as they are unmanned, they can be used as standard client terminals if desired.
- Modem Racks
  The modem racks contain up to 16 modems each and are 19” rack-mounted units that are connected to the modem servers via the local area network.
- Standard Client Terminals
  The standard client terminal software is used to provide system status and the viewing of historical event data. Some terminals are configured to view the entire system, but others are only associated with particular regions and their data is filtered accordingly.
- Custom Client Terminals
  The custom client terminal is a software package specifically written for United Utilities that presents status information in specific ways. It’s main purpose is to report HV network faults and their most likely places of occurrence as determined by status reports from individual POD sensors. Again, these terminals are used by some to show the overall system

status and by other users to show only the status for those areas of interest to the user.

- **Relay Output Client Terminal** — This is a special version of the client terminal which is equipped with relay output control cards that are used to control a number of external indicators (flashing lamps and message displays). These indicators are programmed to be activated when faults are detected in specific areas or when system faults are detected (modem loss, server being offline, etc.). Relay control is now built into the standard NHDS host terminal.
- **Report Generation Terminal** — This terminal was developed specifically for the customer. The standard host terminal is capable of compiling a variety of reports, but for this system, the customer had specific requirements to produce statistical reports of particular formats, both for internal use and for use by the external watchdog authority.
- **Remote Office Client Terminals** — The remote office client terminals consist or either the standard or custom client software but installed at remote locations, connected to the system database via the customers own WAN (wide area network). The interface to the system database and the network architecture ensured that these terminals did not have significant performance disadvantages over locally connected clients.
- **Network Management System** — The customers own network management system (NMS), used to control and monitor the entire electricity distribution for the region interfaces to the PODS system so that it can treat POD sensors in the same way as it treats its larger SCADA remote terminal units installed at primary substations. The PODS are treated as just another input and are transparent to the users of this system, so users of the NMS can benefit from the information gathered by the PODS system without referring to a second software package or having to interpret that information in a different manner. At first the interface between the NMS and the PODS system was made by means of file exchange, where the PODS system would periodically create files containing the current status of each PODS sensor or spreadsheets of historical event. Eventually, however, the NMS was modified to read the information directly from the PODS system database.

United Utilities are now developing their own clients in-house, with assistance from NHDS , by interfacing directly to the system database. This allows them to use their own in-house expertise to design their own system resources.

Case Study 2 - Crown Castle

Crown Castle UK, formerly the BBC Home Service Transmission Division, are a provider of wireless infrastructure and network services to broadcasters and telecommunications operators. They currently have approximately 3000 sites hosting equipment for Hutchison ***3*** (the UK 3G network), Vodafone, Orange, O2 and T-Mobile and had a requirement to provide a service to these users, charged on the basis of, amongst other things, the amount of power used on each site. Therefore a wireless meter reading solution was required. Additionally, as part of the value added service provided to their clients, Crown Castle had an additional requirement to be informed of loss of power to any of the sites so that interruptions to any site could be kept within the contractually agreed limits.

This solution was provided with a system based upon the NHDS Messenger 62 (M62) remote meter-reading and monitoring units. The M62 unit has 8 meter reading inputs and 8 digital inputs for monitoring alarms as well as the ability to monitor the mains supply. The unit uses the GSM mobile phone network to report to the host terminal system.

Initially, this system consisted of a single stand-alone PC running the Messenger host terminal software package and monitoring just under 1000 M62 units. This provided an initial trial system prior to going live with a system producing actual billing data for Crown Castle's customers.

The system was soon expanded, however, to run on a central server with remote clients, and a direct link from the host terminal system to the Technical Operations Centre (TOC) system, a department responsible for 24/7 monitoring of the companies equipment and sites.

At this stage, the Messenger system was deemed a mission critical system, and had to achieve the standards of fault tolerance, redundancy and disaster recovery required of such systems within the company. To this end, a duplicate, system was installed at a backup site in Sutton Coldfield, so that in the event of a major disaster at the headquarters in Warwick, all operations could be brought back online from the Sutton Coldfield site, without loss of data.

System Description

The system is based around an Oracle 9 database running on a Windows 2000 based rack-mounted server.

Communications between M62 units and the system is carried out with another Windows 2000 based rack-mounted server, running the standard Messenger host terminal software configured as a modem server. This software is installed to run as a Windows "Service", thereby avoiding the need for the server to be logged on as any particular user. This allows the software to be loaded automatically in the event of the server rebooting without user intervention.

Actual communications is handled by the use of a number of GSM modems, connected to the modem server PC directly via a multi-port serial card. Future expansion of the system is likely to lead to a direct connection into the T-Mobile GSM network using a network pipe, thereby replacing the need for any actual modems.

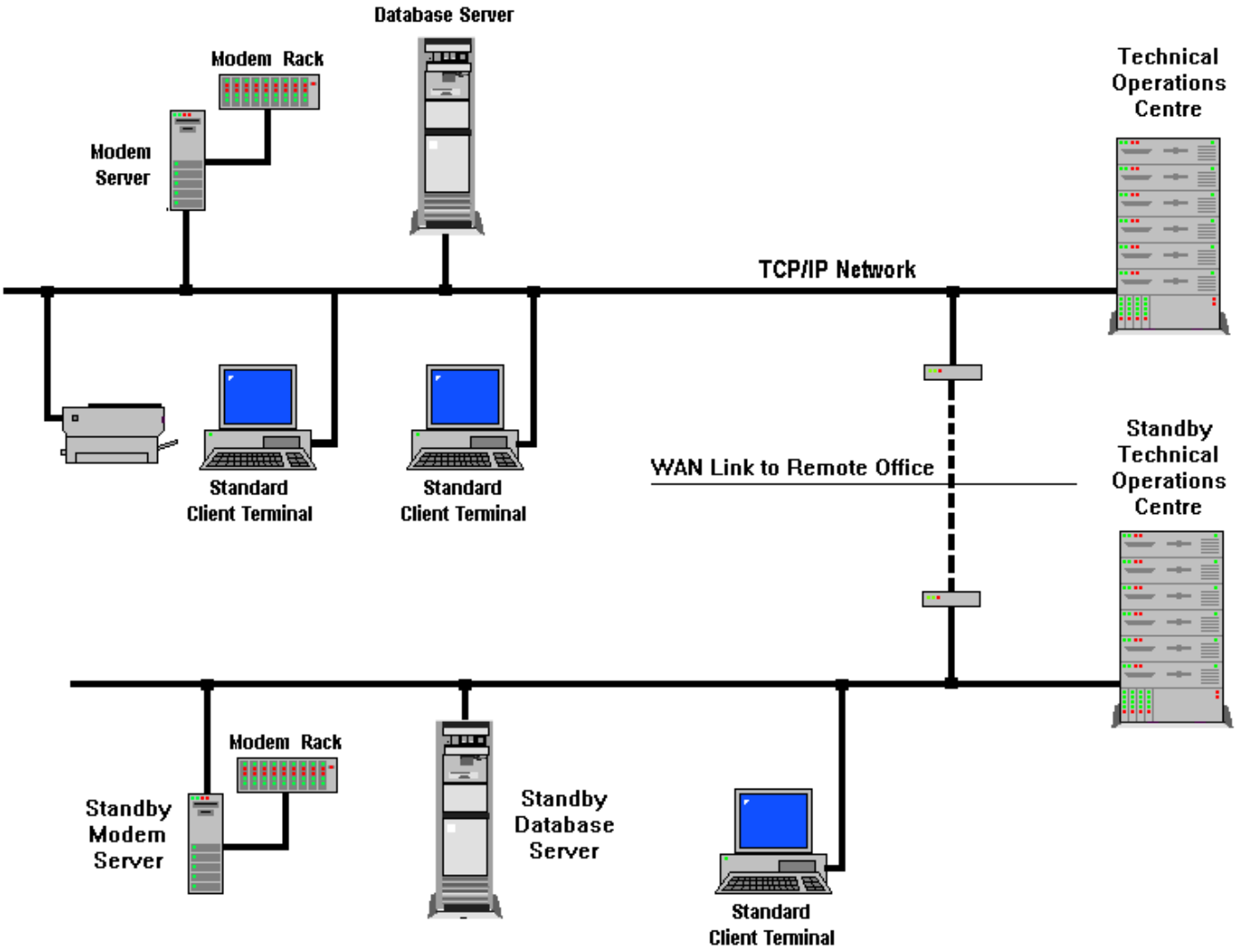
The modem server also communicates directly with the TOC system by TCP/IP pipes. The server passes all relevant status and event data to two different addresses, one for the main TOC system located in the same building and one for the standby TOC system at the backup site at Sutton Coalfield. This provides the TOC team with information regarding site mains failures and restorations directly to their management system, eliminating the need to run a Messenger client system in the TOC department. The system also has the ability to automatically send SMS text messages to on-duty field staff responsible for investigating and correcting site faults. For information purposes, emails of such alarm events are also automatically generated and sent to the personnel responsible for installing and maintaining the Messenger units themselves.

Billing reports are created automatically at defined intervals and forwarded to relevant parties ready for forward billing to Crown Castle's own customers.

A number of client terminals, fitted with the standard Messenger host terminal software are also used in the system, to be used for relevant personnel to be able to examine the current status of the Messenger units and to reprogram parameters and view/search historical archives of system events.

A duplicate database server and modem server are located at the Sutton Coalfield backup site ready to take over operations whenever required. The database will soon be linked to the main database server as a replicated database, where the data is kept in step with the main database so the two systems can run in parallel and hand-over to the standby system will be seamless.

The diagram below how the Crown Castle Messenger host system fits together.



The individual of elements of this system are as follows:

- Database Server — This is the heart of the system where all the status and historical data is stored. This is comprised of an Oracle 9 database management system running on a Windows 2000 server PC.
- Modem Servers — The system contains 2 modem servers, one on the main site and one on the backup site, to receive and make calls from/to the M62 units. Each server consists of the standard host terminal software installed on a Windows 2000 server PC mounted in a rack. The software in installed as a Windows “Service” to avoid the need for user intervention in server power up or the need for a server to be logged on for the software to un. Although these terminals are not used with permanent monitors or keyboards, as they are unmanned, they can be used as standard client terminals if desired.
- Standard Client Terminals — The standard client terminal software is used to provide system status and the viewing of historical event data. Client terminals in this system are usually used in an ad-hoc basis, where the software is run on demand.
- Technical Operation Centre — The Technical Operations Centre (TOC) is the Crown Castle department responsible for maintaining 24/7 monitoring of Crown Castle equipment and sites. Two TCPI/IP pipes are established from each of the modem servers to the TOC management systems (both the main system and the backup system at Sutton Coalfield) to pass information regarding the loss or recovery of power from monitored M62 sites.