A NETWORK MANAGEMENT SYSTEM FOR THE FASTPAC 2 SERVICE

PETER C. CRAIG AND GLENN R. COLVILLE[1]

***Abstract*—A network management system for Telecom Australia's public fast packet switching network was developed. The network management system is highly standards-compliant, and was designed to meet the needs of managing a nationally distributed telecommunications network. The business, functional and availability requirements of the management system and its interface to the FASTPAC network equipment are described. The paper discusses the major features of the software architecture of the network management system, and some of the processes used in the software development.**

***KeywordsKeywords*—Network management, software engineering, fast packet switching, telecommunications networks, computer communications, metropolitan area networks, DQDB, FASTPAC**

***Source of Publication*—Journal of Electrical and Electronics Engineering, Australia, Vol. 15, No. 2, June 1995, pp 203-213.**

1 INTRODUCTION

Telecom Australia provides a high speed packet switched data communications service, known as FASTPAC. The FASTPAC service is primarily aimed at the Local Area Network (LAN) interconnection market, offering performance in a Wide Area Network (WAN) comparable to that of Local Area Networks. The service is provided nationally and supports customer access classes at both 10 Mbit/s and 2 Mbit/s, known as FASTPAC 10 and FASTPAC 2. The service provides the customer with seamless interconnection of LAN bridged or routed networks, offering bandwidth on demand to meet peak throughput requirements. Customer interfaces available include IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring) at 4 Mbit/s or 16 Mbit/s, and a 2 Mbit/s open access packet interface similar to the Bellcore 2 Mbit/s SMDS service. These interfaces provide physical connectivity to industry standard LANs, bridges and routers, while the access class provides a total throughput capability for interfaces selected by the customer (see Figure 1). FASTPAC 10 is delivered in the customer access network (CAN) using 34 Mbit/s optical fibre transmission, while FASTPAC 2 is delivered in the CAN using 2 Mbit/s links over copper pair cables, thus enabling broad geographic coverage.

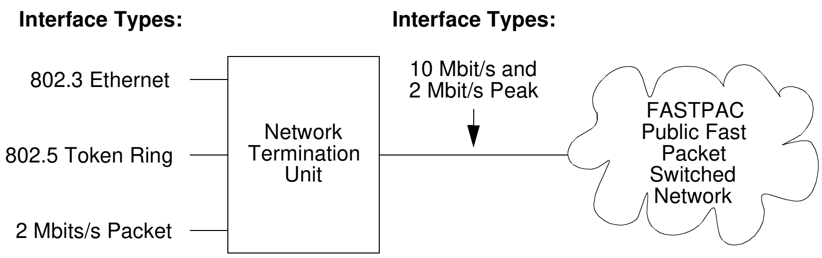

Figure 1: FASTPAC Interface Types and Access Classes

A network management system for the FASTPAC 2, or 2 Mbit/s access components of the network, was developed by CiTR under contract to Telecom Australia. It was a requirement that the service and network be fully managed, both within the core network and to equipment installed at the customer premises. As the FASTPAC service attributes include high availability, high security, and minimum fault restoration time, some demanding design constraints were imposed on the network management software.

1. Telstra

2 FASTPAC TECHNOLOGY

FASTPAC is a cell switched network based on the Distributed Queue Dual Bus (DQDB) algorithm [1]. The system enables provision of very high bandwidth, redundant and geographically diverse network infrastructure. Fixed bandwidth (isochronous) and bandwidth on demand, packet switched services can be supported.

The DQDB protocol has been standardised by the IEEE 802.6 committee [2] and forms the basis of the Metropolitan Area Network (MAN) standard. This technology was originally developed as a research project by the University of Western Australia [3]. A company, QPSX Pty Ltd, was set up to commercialise this research and it supplies the network equipment which forms the basis of Telecom's FASTPAC network.

The FASTPAC network consists of a number of MAN switching systems based primarily in capital cities and interconnected via interstate trunks. The core FASTPAC network uses long distance fibre-optic transmission systems running at 34 Mbit/s and 140 Mbit/s to interconnect the dual fibre rings which deploy the network throughout the metropolitan areas of Australia. This is illustrated in Figure 2.

Within the network, Closed User Groups (CUGs) are used to provide customer data security. Address mapping and screening features in the network are used to ensure that violations of the predefined groups are not possible.

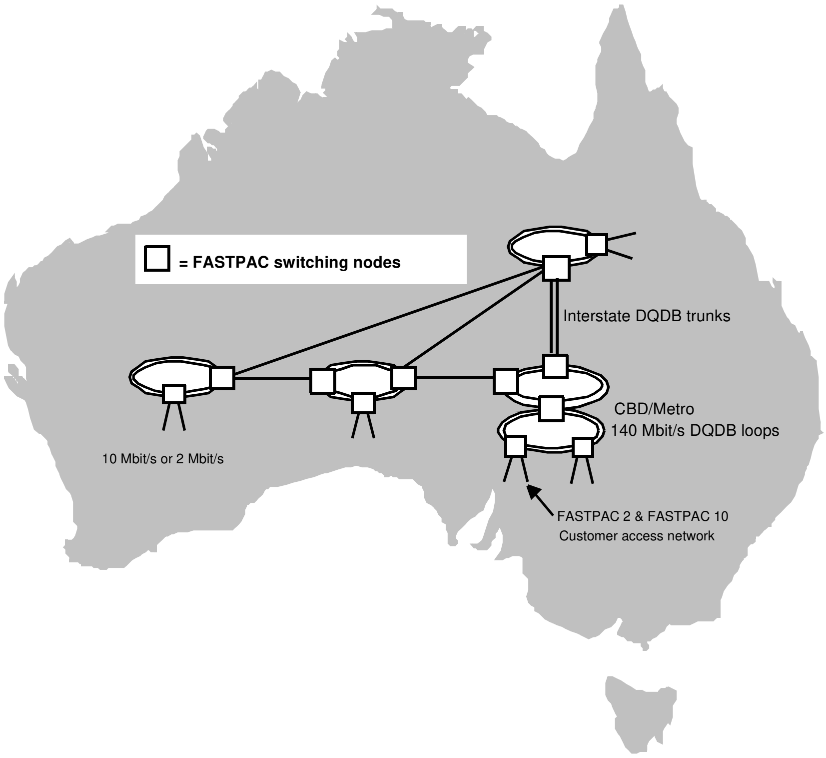

Figure 2: FASTPAC Conceptual Network Architecture

3 APPLICATIONS OF THE FASTPAC SERVICE

As the FASTPAC LAN bridging service is transparent to higher layer protocols it can comfortably support a mixture of industry standard protocols such as TCP/IP and UDP/IP, or proprietary protocols such as IPX, Appletalk or Decnet. Customer Premises Equipment (CPE) using these standard protocols and LAN interfaces can therefore connect seamlessly to the service, without any additional configuration by the customer. The LAN bridging service is explained in more detail in [4] and [5].

Applications suited to FASTPAC include high speed image transfer in industries such as the print or advertising media, rationalisation of IT facilities across regions or states, and shared multiple electronic work environments across wide geographic areas. The high service availability offered is also important to many applications, as typically the customer's business is critically dependent on its computer networks. Customers of the FASTPAC service are accustomed to the high availability provided by local area networks, which use cable plant directly under their control. Although the problems of simply maintaining physical connectivity increase when the network is extended off the customer site, a similar level of network availability is expected as for an isolated LAN.

4 FASTPAC 2 NETWORK ACCESS

The FASTPAC 2 service class is accessed through a Network Termination Unit (NTU) in the customer premises. Transmission at 2 Mbit/s operating over copper pair cables in the CAN connects the NTU to shared switching equipment in the FASTPAC exchange.

It is the NTU which provides the connection point to the customer. In the case of a FASTPAC 2 LAN bridged service, the NTU is a fully managed unit. That is, it is remotely configured, loaded and monitored for fault or performance information as with the rest of the network. In the case of a 2 Mbit/s packet interface (2MPI), the NTU simply terminates the transmission and signals to the network (and hence the management system) any error conditions in the transmission. In the FASTPAC exchange, the equipment that concentrates several customer accesses to the FASTPAC core network is known as a 2 Mbit/s Network Interface Unit (2NIU).

5 REQUIREMENTS FOR MANAGEMENT OF FASTPAC 2

5.1 INTRODUCTION AND DEFINITIONS

The network equipment providing the FASTPAC 2 service is widely distributed throughout Australia. This collection of equipment will be referred as “the network” henceforth. The network consists of various types of equipment which can be remotely configured from the management system. An item of network equipment is referred to as a network element. Equipment types capable of interacting with the management system via a management communications protocol are known as managed network elements.

The management environment depends on the integration of all of the following:

- functionality in each managed network element accessible via a standard management protocol,
- a management network which is a data network carrying management traffic between the managed network elements and a management system,
- a management system consisting of a host computer and specialised software providing the network management functions, and
- an operations centre where operators use graphical displays to access the management system to manage the network elements.

5.2 THE MANAGEMENT NETWORK

The data communications network which connects the management system to the managed network elements is called the management network. A specialised piece of network equipment, known as a 2 Mbit/s Management Interface Unit (2MIU), provides an interface between the management system and the management network. The 2MIU also provides a protocol conversion function between the management system and the network elements.

There are multiple links from the management system to the management network to provide redundancy. Each link requires a 2MIU. The operation of the 2MIUs is also managed directly by the management system.

The management network is a virtual network which is supported within the FASTPAC network infrastructure. This approach was preferred to a dedicated management network. The level of management reliability required can be achieved at a lower cost using multiple 2MIU access points to the network and the inherent redundancy within the DQDB loops and FASTPAC switching nodes.

5.3 BUSINESS REQUIREMENTS

The management system for the network must meet several broad objectives. It must:

- enable Telecom to meet or exceed its customer service assurance targets for the FASTPAC 2 service (service availability is 99.9%, whilst fault restoration requires a 2 hour response on a 24 hour, 7 days per week basis),

- simplify and automate network operations procedures where possible,
- provide the tools to allow a network operator to work effectively, and with increased efficiency, and
- integrate with Telecom corporate systems and business processes.

Specifically, the management system provides a tool which assists the network design and operations staff to carry out functions such as:

- service design and provisioning,
- maintaining service availability,
- monitoring of network performance,
- isolation of faults and service restoration, and
- configuring network equipment.

A centralised approach to management of the FASTPAC 2 network equipment was taken. The management system itself is known as the FASTPAC 2 Management System (F2MS). Its functional requirements are detailed below.

5.4 FUNCTIONAL REQUIREMENTS

5.4.1 PROVISIONING

The F2MS provides automation of the procedures associated with installation, alteration, and recovery of network equipment in response to customer service orders. These activities are designed to support Telecom's business processes for the provisioning of customer services. The essential information associated with each network element is recorded in a data repository which contains both customer-oriented and network-oriented information about installed network equipment. Information in the data repository can be viewed and modified by operators via the user interface. Additionally, provision is made for access to this information by report applications.

Installation of a new network element causes certain data associated with that network element to be made available to it via a configuration data updating process which involves real-time interaction between the management system and the network element. This is necessary to reconfigure the network equipment to activate the new customer service being installed.

5.4.2 NETWORK ELEMENT BOOTING

Availability of the network management system is important as the network elements are dependent on it for downloading software images and configuration data files during a restart. This function will be referred to as the boot response function. These restarts occur when the equipment is first installed in the network, and can also be initiated by the network operators via the management system.

5.4.3 PERFORMANCE MONITORING

Another key function of the management system is performance monitoring of the network. The network is configured to generate periodic performance reports and the management system is responsible for collecting the performance events, logging the raw data to disk and forwarding the events to an external system for more detailed performance analysis of the network.

5.4.4 FAULT MONITORING

The F2MS is responsible for monitoring the network for faults. Certain network events and some other conditions detected by the management system, such as loss of communications with a network element, are considered to be alarm conditions. These are reported to the network operators and are sent to an external corporate system, the Alarm Management System (AMS).

5.4.5 NETWORK ELEMENT CONFIGURATION

The management system provides the network operators with the facility to directly manage the network equipment via an application which allows access to the network elements to view and change their internal data. This provides dynamic control of some aspects of the equipment operation. Another function allows operators to reconfigure data defining the operation of network equipment. While this allows control of overall aspects of the network element's configuration, the reconfiguration is not effective until the next download of configuration data to the network element.

5.4.6 SECURITY AND INTERLOCKING

Multiple security levels and a task-based interlocking mechanism ensure that management of the network is restricted to authorised operators, and that the management activities of the operators do not conflict. Security between the management system and the network itself is ensured through access restrictions and verifications within the management protocol.

5.5 PERFORMANCE AND AVAILABILITY REQUIREMENTS

The F2MS is required to provide a reasonable response time to all operator activities under normal loading conditions. The normal load on the management system includes the collection and processing of alarms and performance events from the network. The system must support a continuous throughput of 12 events per second and a peak rate of 60 events per second. The choice of system hardware and the software architecture must ensure that the system is scalable to allow for growth beyond these limits.

The system is required to provide a high availability for both automated network management activities and those functions directly involving an operator. As high availability is a key objective of the FASTPAC service, those functions associated with network monitoring, fault identification and fault restoration are of critical importance. As an example, the boot response function is specified to have an availability of greater than 99.95%.

5.6 OPERATOR INTERFACE REQUIREMENTS

Operation of the FASTPAC network is the responsibility of a group of operators located in one or more management centres around Australia. Each operator is provided with a high resolution colour graphics display including a keyboard and mouse. The interaction between the operators and the management system is via an X Window System graphical user interface (GUI).

The GUI allows the operator to access the functionality of the management system described in the previous section. The FASTPAC network elements are organised as a hierarchy for management purposes. The operator must be able to select a network element for management action by navigation within the hierarchy of network elements, or by searching based on customer or network-oriented information associated with the network element.

The F2MS must provide a means for the operator to continuously monitor the overall state of the network.

6 MANAGEMENT COMMUNICATIONS PROTOCOLS

Communication between the management system and the managed network elements uses a standard network management protocol. Management communication protocols are upper layer protocols. A key characteristic of upper layer protocols is that they have a few simple interactions, but extremely complex structured data is carried within each interaction. This complex data structure is necessary to represent the internal state of the managed network elements.

The set of data attributes which characterise the internal state of the network elements is known as the Management Information Base (MIB). These data attributes are grouped into sets of data which constitute managed objects. The MIB interface is used both to determine information about the network element and to effect commands from the management system to the network element, for example to cause it to block traffic on a particular port. In the case of the FASTPAC 2 network equipment, the MIB is defined by the manufacturer of the network equipment to contain the base functionality of MIB-II [6] as well as proprietary managed objects which are required for the management of the network's internal operations.

7 ARCHITECTURE OF THE NETWORK MANAGEMENT SYSTEM

7.1 HARDWARE ARCHITECTURE

There is no hardware redundancy provided in the selected host platform. The availability of a single host was not adequate to meet the very high availability requirement of the network management system's boot response function. This necessitated a dual host hardware configuration. This is shown in Figure 3.

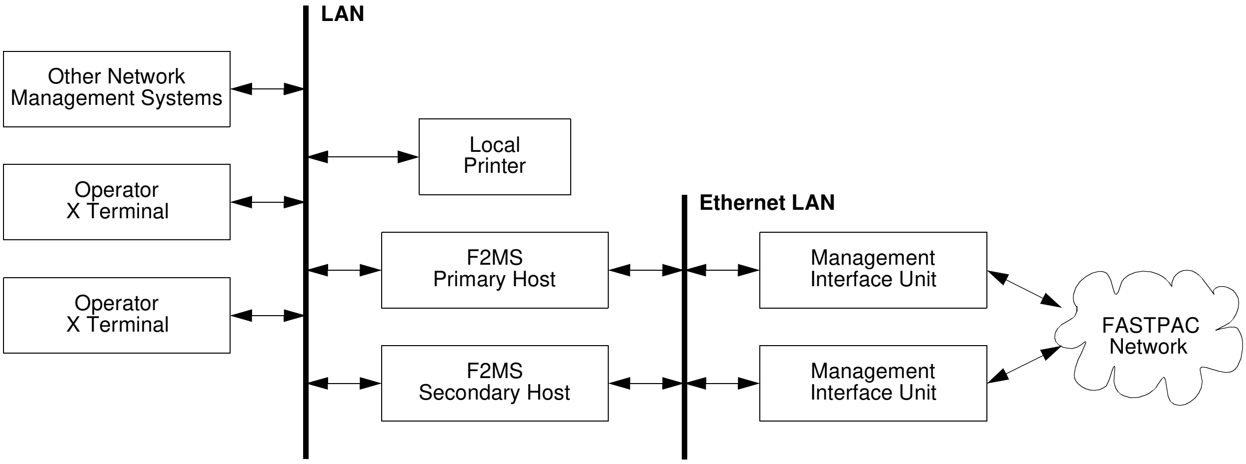

Figure 3: Hardware Configuration

The first level of hardware redundancy is the provision of two host machines with replication of the data files necessary for network element booting. The secondary host is responsible for providing the boot response function, in the event that the primary host is unavailable due to failure or planned maintenance. This function is essential to support a high level of FASTPAC network availability.

Also, should the primary host be unavailable for an extended period, the full functionality of the primary host may be started on the secondary. An important consideration in the system design, particularly in the area of database management, was to ensure the time to restart the full functionality on the primary host was minimised.

The management system interface to the FASTPAC network is provided by a redundant set of Management Interface Units, which are connected locally to the management system via an Ethernet LAN. These interface units provide protocol conversion which allows the management system to interact with remotely located items of network equipment as if they were directly accessible via the management LAN.

An important feature is that FASTPAC network operators can be located remotely from the management system hosts. This is achieved by providing an X Window System based user interface, which decouples the display device from the management host. Further, the operator access to the management system host may be via a data network, rather than a single LAN. In this way, independence between the location of the network operations centre and the management system host is provided. Redundant access links are available between the management system host and the operator X terminals.

The partitioning of the operators' user interface traffic from the management traffic was an important architectural choice. The management system has been designed to process a high rate of performance events which are generated by the FASTPAC network. The peak data rate of performance events can consume a significant amount of the capacity of the Ethernet. Thus it is desirable to isolate this Ethernet traffic from the LAN supporting the network operators, in order to minimise interference with user interface activities.

A further consideration is that the system is supported within Telecom Australia's Standard Operating Environment (SOE). Hardware and software chosen for the management host and terminal access is compliant with systems and platforms currently specified within the SOE.

7.2 SOFTWARE ARCHITECTURE

While there were several network management solutions available on the market, these platforms were not sufficient to support the F2MS requirements in their own right. The approach used was to develop custom software to meet Telecom requirements for functionality, distribution, system integration, scalability, operator efficiency, and reliability which were not available in these standard solutions. However, an industry standard package was used to supply basic facilities such as the management communications protocol and ASN.1 encoding of data structures. This enabled a minimal development time, cost and risk when integrating the F2MS with the network.

The system requirements imposed some key design constraints on the selection of platform software, some of which stem from SOE compatibility. Among these constraints were the use of:

- the HP OpenView platform,
- the INGRES relational database management system,
- the HP-UX operating system, and
- the Motif style [7] for the GUI.

Within these constraints, it was clear that many software solutions were possible.

The software architecture was derived by identification of the subsystems responsible for different functions of the management system. The requirements of the overall system were allocated across the numerous subsystems.

Functions of the management system were separated into management applications and management services layers. Figure 4 illustrates this layered view of the software. Management application processes are responsible for interacting with the network operators using an X Window System GUI to display information about the state of the network equipment, and to allow the operators to interact with the network management system for service provisioning, routine management and network element reconfiguration. These processes communicate with the management services of the F2MS, which are responsible for shared services such as data repository access, network event collection, and coordination of management access by the operators to network equipment.

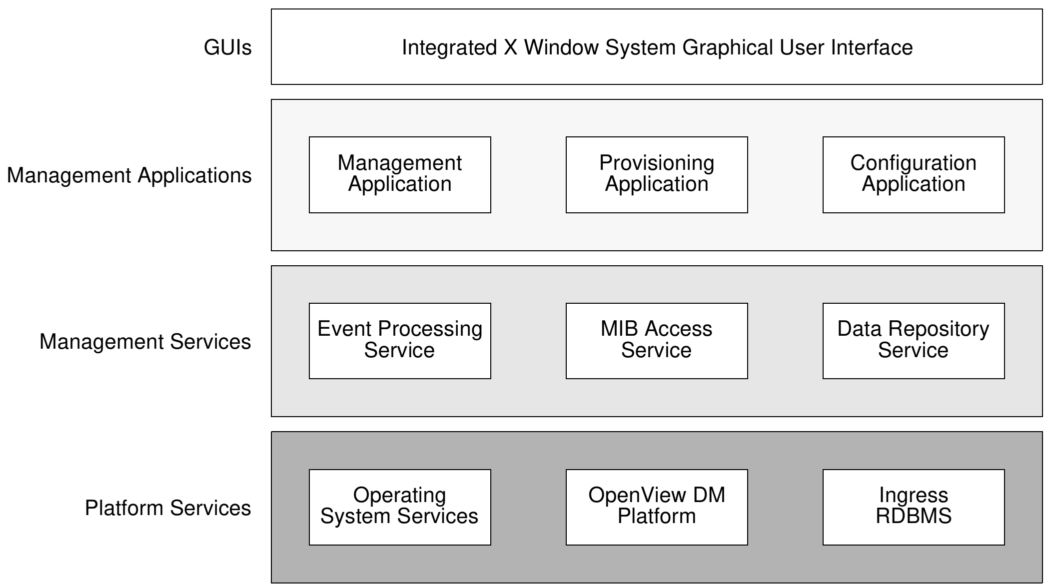

Figure 4: Management System Software Architecture

Communications between the management applications and management services use a client-server model. The client-server interactions are implemented using a socket-based interface. The architecture chosen makes possible distribution of the management system across multiple hosts by separation of the management applications and servers.

The management processes depend on services provided by the platform software. The platform software includes the OpenView Distributed Management (DM) platform, the INGRES Relational Database Management System (RDBMS), and the HP-UX operating system. Underlying all of this are the system hardware interfaces. Apart from the communications interface to the FASTPAC network, the F2MS communicates with external systems such as the AMS. The interface to external management systems is provided via a second Ethernet card installed in the primary host.

The role of the OpenView DM platform software is to provide management communications with the network equipment using standard network management protocols. This platform software isolates the management system from many low-level protocol details, simplifying this aspect of the management system software.

One of the major services provided by the OpenView platform is the handling of encoding and decoding of the data contained in protocol data units which are structured according to the ASN.1 [8] Basic Encoding Rules (BER). ASN.1 allows structured data (including sets, sequences, and other compound data types) to be represented in a machine-independent linear octet stream for transmission across a telecommunications link, and the encoding and decoding rules are complex. The OpenView platform provides services which abstract out some of the details of ASN.1 encoding and decoding.

The high-level software design in Figure 5 shows the relationships between the major processes of the management system. This diagram also shows the partitioning of functionality into application and server processes.

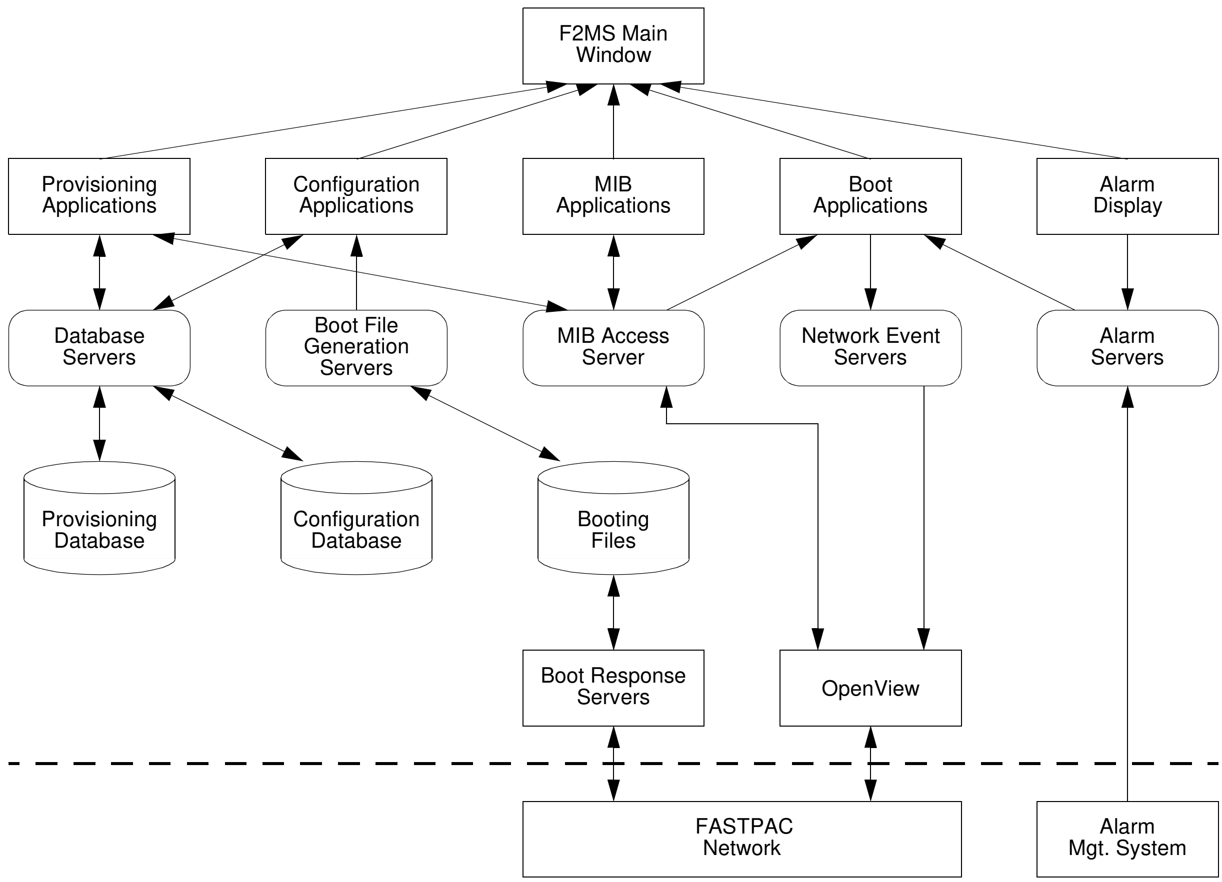

Figure 5: High-Level Software Design

7.3 MANAGEMENT SYSTEM FUNCTIONS

The configuration data management application is important to ensure optimum performance of the network equipment. The network equipment was designed with a great deal of flexibility, which means that there are many hundreds of optional and mandatory parameters which characterise the operation of the network equipment. To manage this complexity all the parameters are classified as being:

- defined during the installation process for that network element, e.g. its address,
- configurable for a particular network element, or
- configurable for all network elements of the same type.

A general defaulting strategy for parameter values in the configuration data management application simplifies the operator's task in setting up the configuration data for the network elements. While a parameter may be configurable for a particular network element, a default value is provided for all network elements of the same type if the parameter is mandatory. Thus the operator needs to enter data for the parameter only if the network element has a non-standard configuration. A "compilable specification" approach was used for defining the data structure and the initial default values for each network element type. The benefits of this approach include the minimisation of coding errors and the ease of introduction of new data structures that may occur with the introduction of new versions of network software.

Another important feature of the F2MS is concurrent support for multiple versions of network element software. This support enables different network elements to run different software versions whilst ensuring full network manageability. For example, it allows different external interfaces such as the network element data structure and alarm format for a network element type. The benefits to Telecom include minimising any customer disruption during network migration, and the introduction of new network or customer features in a timely and phased manner.

Events received from network elements are used to monitor the health of the network equipment. Loss of communication with a network element is an indicator that it may be unavailable to carry customer traffic. When this condition is detected, the management system immediately generates an alarm both to the local display and to the AMS. A management server process maintains an in-memory database of the state of all installed network equipment. This information is always available to the operators via their display of the network.

The very high peak rate of performance events which the F2MS was required to process meant that an efficient buffering mechanism was required. This was implemented in RAM with a circular buffer strategy. The relatively high continuous rate of events received from the FASTPAC network required some effort in speed optimisation of the network event processing software. The optimisations included the use of data caching to minimise accesses to the database during the processing of an event, and optimal design of the event data flow through the system.

The requirement to provide very high availability of the network management system required careful design of the database server. Ensuring that the system is continuously available to perform management functions requires that the contents of the database be backed up without making the system unavailable for operator activities. A strategy was implemented which allows the database to be copied while in a consistent state, without there being any apparent break in the availability of the management system from the operator's perspective.

It is necessary to maintain data synchronisation between the two hosts, because of the dual host hardware configuration. The Boot File Generation server is responsible for maintaining the software image and configuration data files for all installed network elements on the primary host, and for periodically transferring these files to the secondary host. This allows the secondary host to provide the boot response function with the most up-to-date network element data.

A key design principle was to keep the management system as open as possible to extensions. For example, the relational database is used to store all essential data associated with the installation of a network element into the network. An interface is provided to the management system's database to allow the F2MS to be easily extended by the addition of new applications, for example reporting applications which can access the database via this interface. Additional applications or extensions may also be mapped to the operator menu. This flexibility and integration with the core system has enabled a number of smaller applications, for example network test facilities, to be added quickly to the system when an operational or productivity need has been identified.

Further processes within the management system are responsible for internal supervision of the management system itself. This self-monitoring is essential to meet the system's availability requirements.

8 SOFTWARE DEVELOPMENT

Before the specification and development of the production software, a prototype was developed to assist in identifying the business and technical requirements of the management system. This prototype also identified the advantages of using "compilable specifications", that is, providing part of the system specification in machine readable form in a language which can be translated directly into code.

The complete set of system requirements for the F2MS was identified from a requirements analysis phase as well as from experience gained with the prototype system. These requirements were captured in a System Requirements Specification (SRS) document which was constructed to the IEEE 830-1984 standard [9]. The

F2MS software was developed using a conventional software life-cycle with analysis, design, building and testing phases. The design documentation was developed to conform to the IEEE 1016-1987 standard [10], which specifies recommended practices for documenting the design of large software systems.

An object-oriented implementation was not adopted for this development. At the time the project commenced, the choice of C as the implementation language was assessed as having a substantially lower technical risk. Further, the platform services on which the software is built provided C language interfaces.

The design and development phases were conducted in accordance with CiTR's internal design, coding and review standards. These collectively define processes which are applied to map the input documents of a software lifecycle stage to the output documents of that stage. The review process verifies that the input document's requirements have been met.

In the production system, the GUIs and internal data structures of both the MIB browsing and the configuration data management subsystems are automatically generated from specifications. The MIB definition was provided in a restricted subset of the ASN.1 language. An ASN.1 compiler developed for this project was used to generate the internal structures. The definition of the configuration data was expressed in a proprietary language which was developed for this purpose. The advantages of the "compilable specification" approach include a more general coding model, which led to a reduction in the coding and testing effort, and the flexibility to easily accommodate changes in the specification.

The production software contains more than 100,000 source lines of C code, several thousand lines of lexical analysis and compiler-compiler source language, and approximately 25,000 lines of data which was automatically translated into C from specification documents.

9 CONCLUSION

The development of a standards-compliant network management system for the FASTPAC 2 service has been described. This system was designed to have high availability in order to support the requirements of managing the customer services provided by the FASTPAC 2 network access equipment, which are generally critical data links within the customer's enterprise-wide computer networks. The system's functional and performance requirements and their influence on the software architecture have been discussed.

The technique of automatically generating application code from compiled specifications was found to be accurate and flexible, and it led to a reduction in the total software development effort. It allowed for specifications of the data interfaces of network elements to be changed late in the software development cycle without affecting the delivery date for the system.

The commercial release of the F2MS software has been in service for over 12 months managing the FASTPAC 2 network equipment, and the operational experience with the management system indicates that it fully meets the system requirements. This illustrates the benefits of applying a process-oriented methodology in the development of large and complex software systems.

10 ACKNOWLEDGEMENT

The authors wish to thank the staff members of the F2MS development team who contributed to the ideas described above. The contribution of Ian Rose to the design of this system is especially acknowledged.

The permission of the Manager, Data Platforms, Telecom Australia, and the Managing Director, CiTR, to publish this paper is acknowledged.

REFERENCES

[1] J.L. Hullett and P. Evans, "New proposal extends the reach of metro area networks", *Data Communications*, Vol. 17, No. 2, February 1988, pp. 139-147.

[2] IEEE Std 802.6, "Metropolitan Area Network Access Method and Physical Layer Specifications", *IEEE*, 1991.

[3] R.M. Newman and J.L. Hullett, "Distributed Queueing: A Fast and Efficient Packet Access Protocol for QPSX", ICCC, Munich, 1986.

[4] Austel Technical Standard 021, "General Requirements for Customer Equipment Connected to a Public Fast Packet Switched Network", Austel, 1993.

[5] R. Pretty, "Fastpac - Nationwide High Speed Networking", *Australian Communications*, March 1991,

pp. 44-55.
[6] K. McCloghrie and M. Rose, "Management Information Base for Network Management of TCP/IP-based Internets: MIB II", RFC1213, 1991.
[7] "OSF/Motif Motif Style Guide V1.1", Prentice-Hall, Englewood Cliffs, New Jersey, 1991.
[8] ISO 8825, "Open Systems Interconnection—Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)", ISO, 1988.
[9] IEEE Std 830-1984, "IEEE Guide to Software Requirements Specification", *IEEE*, 1984.
[10] IEEE Std 1016-1987, "IEEE Recommended Practice for Software Design Descriptions", *IEEE*, 1987.