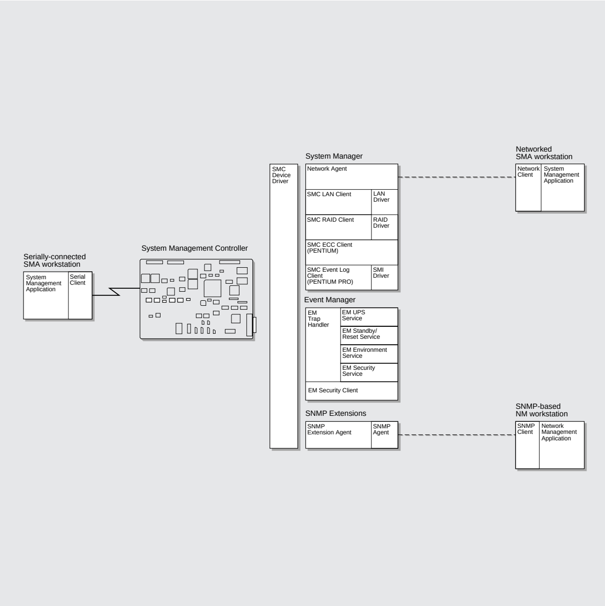
MITSUBISHI

apricot

AMS

Overview



APRICOT MANAGEMENT SUITE OVERVIEW

2ND EDITION

Information contained in this document is subject to change without notice and does not represent a commitment on the part of Apricot Computers Limited. Any software described in this manual is furnished under a license agreement. The software may be used or copied only in accordance with the terms of this agreement. It is against the law to copy any disk supplied for any other purpose than the purchaser's personal use.

Published by:
Mitsubishi Electric Personal Computer Business Division
Apricot Computers Limited
3500 Parkside
Birmingham Business Park
B37 7YS

MITSUBISHI ELECTRIC

Printed in the United Kingdom

Preface

This manual, as its name suggests, provides an overview of Mitsubishi Electric PC Business Division's **Apricot Management Suite** (AMS). It also includes a functional overview of the system management hardware.

It is intended to be read by network managers, server operators and service engineers.

More detailed information about each of the packages that comprise the AMS is provided in the following documents:

- *AMS Installation Guide*
- *System Management Application User's Guide*
- *Event Manager User's Guide*
- *SNMP Extensions User's Guide*

This manual refers to "supported" third-party LAN and RAID systems. To find out which systems are currently supported, please contact your Apricot supplier.

CONTENTS

1 INTRODUCTION

The Apricot Management Suite (AMS) is a software collection that allows network managers, server operators and service engineers to exploit fully the capabilities of the server's built-in System Management Controller (SMC). The SMC monitors, and to an extent controls, the server's subsystems.

The AMS consists of three packages, each package in turn containing several co-operating software components:

- System Manager
- Event Manager
- SNMP Extensions

System Manager

The System Manager package allows authorised users to manage servers remotely, either through a dialled-up serial connection or across an enterprise network. Up to 16 servers, located in different parts of the network, can be managed simultaneously from a single, central management workstation.

The package includes the Windows-based System Management Application (SMA), protocol drivers, and server-resident software that enables the System Management Controller to gather additional information from supported third-party LAN, RAID and ECC subsystems.

Event Manager

The System Management Controller firmware includes a range of pre-programmed responses to AC power outages, inappropriate use of the front panel controls, overheating, unauthorised attempts to access the machine's interior, and so on.

The Event Manager package augments the SMC's programming by providing a set of OS-specific services which respond to these situations in accordance with a script defined by the network manager or server operator.

SNMP Extensions

These allow a network manager to integrate the AMS with third-party network management products based on the industry-standard Simple Network Management Protocol.

Design principles

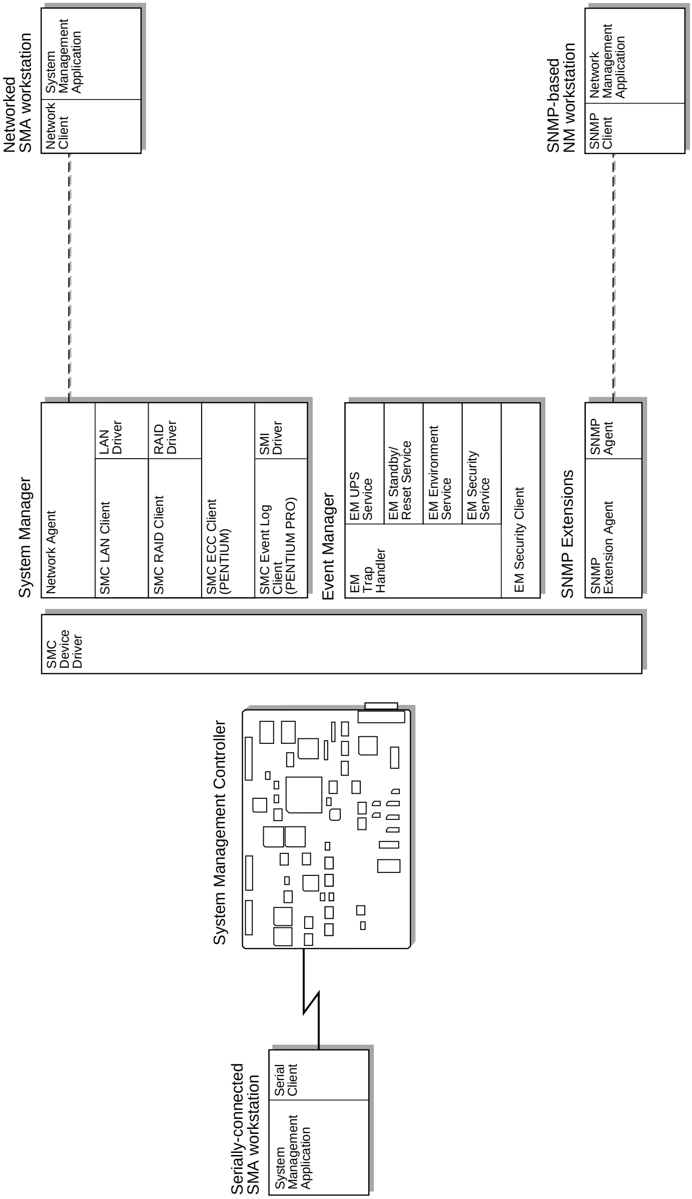
Taken together, the packages of the AMS provide a set of tools which embody two key design principles:

- Local autonomy
- Commonality of remote and local management

Local autonomy

Servers with SMCs are able to look after themselves. The SMC embodies enough intelligence in its firmware to respond to hardware failures, security violations and exceptional conditions such as power outages and overheating. When these responses are augmented by the Event Manager, the server can reliably be left on its own and will require little attention even if circumstances require it to be shut down.

- At boot time, key hardware components are tested and can be disabled if found to be faulty or if confidence in them falls. After booting, major subsystems are continually monitored for evidence of errors or exceptional conditions.
- If the AC power supply fails, the server switches immediately to UPS battery power and can keep running long enough to bring the operating system down gradually, with minimum inconvenience to users and no loss of data.
- If the built-in LOC Technology™ security system is enabled and armed, any attempt by unauthorised personnel to use the front panel buttons or access the server's interior will trigger a security alarm.


Networked
SMA workstation
Network Client
System Management Application
SNMP-based
NM workstation
SNMP Client
Network Management Application
System Manager
Network Agent
SMC LAN Client
LAN Driver
SMC RAID Client
RAID Driver
SMC ECC Client (PENTIUM)
SMC Event Log Client (PENTIUM PRO)
SMI Driver
Event Manager
EM Trap Handler
EM UPS Service
EM Standby/ Reset Service
EM Environment Service
EM Security Service
EM Security Client
SNMP Extensions
SNMP Extension Agent
SNMP Agent
SMC Device Driver
System Management Controller
Serially-connected
SMA workstation
Serial Client
System Management Application

- Inappropriate use of the front panel STANDBY or RESET buttons while the operating system is still running will be caught, and the operating system safely shut down before the button is actioned.
- The operating system can also be shut down, and the server powered off, if the SMC detects that the server is starting to overheat.

By using the Event Manager and SNMP Extensions packages, users throughout the network can be informed of exceptional conditions at the server. The SMC itself can alert up to sixteen network managers located at SMA workstations. If a modem is attached to the SMC's external port, one of these SMA workstations can be alerted through a dialled-up serial connection, even if the operating system is not running.

Commonality of remote and local management

The System Manager package is the key software component that allows a server to be managed either remotely or locally.

A network manager running the System Management Application from a remote workstation can connect to the server over the enterprise network or through a dialled-up serial connection to the SMC's modem port.

Service engineers and server operators can use the SMA for local management by connecting a portable or notebook computer directly to the SMC's modem port. A special serial cable is supplied for this purpose.

Each server can accept up to sixteen simultaneous connections: fifteen network connections and one serial connection (or sixteen network connections if the modem port is unused). A serial connection can be made even when the server is in Standby mode and its operating system is not running.

By using the SMA, a network manager can:

- Reset, power off or (through a serial connection only) power on the server, either immediately or at a scheduled time in the future.

- Review and amend the information in the SMC's database, and alter what actions the SMC takes when a monitored parameter changes or goes out of bounds. (This feature is discussed in more detail in the next chapter.)
- Review the alerts received from all the servers overseen from the SMA workstation.
- Automatically forward alerts to other destinations; for example, by Dynamic Data Exchange to other Windows-based applications, and by electronic mail to other users.
- Upload a new version of the SMC firmware.
- Use the SMA's Remote Console feature to monitor the server as it boots, or run the SMIC Flash Disk Utility to upload BIOS revisions and invoke the server's System/EISA Configuration Utility. (These features are available only to serially-connected SMA workstations.)

The SMA can work with the Windows-based DPT Storage Manager application to manage DPT RAID systems over a network or a serial connection.

In addition the SNMP Extensions mentioned earlier allow most of the variables in the SMC database to be viewed by supported third-party SNMP-based network management products.

2 SYSTEM MANAGEMENT HARDWARE

All the packages that comprise the Apricot Management Suite rely on the server's built-in system management hardware. This has two main elements:

- System Management Controller (SMC)
- System Management Interface Card (SMIC)

System Management Controller

The System Management Controller is a specially-designed circuit board mounted in the server's drive chamber. It has its own processor, firmware, and battery-backed memory. Its functions are:

- To test and/or monitor various subsystems within the machine, and to maintain a database in its memory recording the machine's state.
- To issue alerts when the values of certain database variables change or transgress their upper or lower thresholds. Alerts are sometimes referred to as traps or events.
- To allow the machine to be tested, diagnosed and configured from a remote management workstation, if necessary while the operating system is not running.
- To deter unauthorised access to or use of the server, and to authenticate remote connections. When the security subsystem is enabled and armed, attempts to open the side panels or use the front panel buttons can trigger a security alarm.

The SMC is also sometimes referred to as the Front Panel System Controller or FPSC.

System Management Interface Card

The System Management Interface Card is a specially-designed ISA expansion card. A ribbon cable connects the SMIC to the SMA via an internal power distribution board. The SMIC is effectively an extension of the SMC and provides the SMC with an interface to the motherboard and the server operating system.

The SMIC includes:

- A dedicated Diagnostic Processor.
- A two-megabyte Flash disk containing: a bootable DOS image, BIOS upgrade software, and the System/EISA Configuration Utility (SCU/ECU) with its associated adapter configuration files.
- An expansion BIOS that includes console redirection code and the SMIC Flash Disk Utility used to perform BIOS upgrades and invoke the SCU/ECU.
- A small amount of static random-access memory.

The SMIC has its own battery so that it can keep working even when the machine is powered off.

Interfaces

The SMC has a variety of interfaces through which it gathers information and communicates with remote SMA workstations and OS-resident client software.

Modem port

This is a dedicated serial port on the rear of the system unit which provides the SMC with a direct connection to the outside world. Typically, a modem is connected to this port to allow access from a single remote SMA workstation over a dialled-up telephone line. Alternatively, a service engineer or server operator can directly connect a portable SMA workstation to the port by using the special cable supplied.

The modem port allows the SMC to be accessed even when the server is in Standby mode and the operating system is not running.

Diagnostic port

The diagnostic port is an interface to the Diagnostic Processor on the SMIC.

The Diagnostic Processor is a low-level testing agent for the SMC. For example, it monitors the progress of the Power-On Self-Test (POST) routines by reading the “port-80” codes generated by the Motherboard BIOS. It also resets the motherboard when instructed to do so by the SMC firmware.

All of the information gathered by the Diagnostic Processor is accessible by the SMC and hence is potentially available to SMA workstations.

Control port

This interface allows the SMC to communicate with the SMIC BIOS (while the machine is booting) or with an SMC Device Driver (once the server has booted).

An SMC Device Driver enables the SMC firmware to communicate with any server-resident software that has properly registered with the driver (so-called “client software”). This includes:

- The Network Agent that enables the SMC to communicate with up to sixteen remote SMA workstations over the enterprise network.
- Software that allows the SMC to monitor features that neither it nor the Diagnostic Processor can access directly, such as the server’s LAN, RAID and ECC subsystems.
- Other packages such as the Event Manager and the SNMP Extensions.

Pass-through port

The pass-through port is an interface from the SMC, through the SMIC, to the motherboard. It appears to the operating system as a standard serial port (separate from the control port) but can be used only when the SMC is in pass-through mode.

In this mode the SMC's modem port is logically connected to its pass-through port, allowing two-way serial communications between a serially-connected workstation and the server.

Pass-through mode is activated by invoking the SMIC BIOS's console redirection code and then opening a Remote Console window within the SMA. When the Remote Console window is closed the SMC is forced out of pass-through mode by a "pass-through mode trigger". This is either a hardware break or a pre-defined sequence of characters called an escape sequence.

Other interfaces

The SMC has an interface to the Uninterruptible Power Supply which it uses to monitor AC and DC currents and voltages. The SMC can also use this interface to power on or power off the server.

The SMC has an interface with the buttons, LED indicators, infrared sensor and four-digit LCD display on the front panel, as well as with the lock on the door to the removable-media drive bay. With the exception of the POWER ON button, which is directly connected to the UPS, use of the front panel buttons is mediated through the SMC; in other words, the SMC firmware controls what happens when the buttons are pressed.

The SMC also has inputs from the cooling fans, the thermal sensor in the electronics chamber, and the side panel locks in the electronics and drive chambers.

Subsystems

For ease of management, the machine is divided into the major subsystems shown in the table below. Those subsystems that the SMC cannot access directly are tested or monitored on its behalf by other testing agents, and the results stored in the SMC's database.

Testing agents in PENTIUM systems include SMIC BIOS, SMIC Diagnostic Processor, SMC RAID, LAN, and ECC Client software. In PENTIUM PRO systems, the Motherboard BIOS performs many of the testing functions performed by the SMIC BIOS in PENTIUM systems.

Subsystem	Conditions monitored
Motherboard	Serial and parallel port failures; floppy disk drives; motherboard Flash disk.
Memory	SIMM or DIMM failures and Error Checking & Correcting (ECC) warnings.
Processor	Error conditions relating to up to four processors and their associated second-level caches.
EISA	Error conditions relating to the EISA slots.
PCi	Error conditions relating to the PCi slots.
SCSI Controller	Error conditions relating to the two on-board Adaptec PCi SCSI controllers.
RAID	Performance statistics on supported third-party RAID systems.
Network	Performance statistics on any of up to seven network cards.
Environment	Overheating conditions reported by the temperature sensors; fan failure; the locks on the removable-media drive bay door and the side panels.
System Controller	SMC initialisation; user profiles; modem; audit log.
UPS	Out-of-bounds AC or DC voltages; position of the circuit breaker switch; battery status.

Variables

The SMC maintains a database in its battery-backed memory recording the state of the machine, including predictions of failure.

This database is updated and changed by the SMC itself, by the SMIC BIOS, by client software, and by connected SMA workstations.

An SMC variable is a named item of information in this database. In this manual, all variable names are shown in *italic* type; for example: *ShutdownRequest*.

The SMC maintains four sorts of variables:

- Simple variables
- Subsystem descriptors
- User profiles
- Audit log entries

Simple variables

Simple SMC variables serve to record the current condition of the machine and also to direct the operation of the SMC itself. As such they either have a direct correspondence with some monitored parameter or are “housekeeping” variables such as timeouts and status flags.

Subsystem descriptors

A subsystem descriptor records the current status of a particular subsystem – normal, degraded or faulty – how it was initialised and tested the last time the server booted, and how it should be configured the next time the server boots. If a component can be individually detected, tested or disabled, it will have an associated descriptor in the SMC’s database.

Subsystems which consist of more than one component may have more than one descriptor. In some subsystems there is a hierarchy of descriptors; for example, each memory card in a PENTIUM system consists of up to three memory banks, each bank containing up to four double-sided SIMMs (single in-line memory modules). Memory cards, banks and logical SIMMs each have their own descriptors.

User profiles

User profiles identify up to sixteen users of the System Management Application at this server.

Each user has a SMC user name and logon password — these are completely unrelated to any network account the user may have.

The user’s workstation may be identified by a workstation identifier (for a networked workstation) or a modem telephone number (for a remote, serially-connected workstation). In the latter case the profile may also include the Force Traps attribute, which ensures that alerts (traps) are queued for that user and delivered when the workstation is next connected.

Some users have Administrator privileges. These allow the user to alter certain sensitive variables that are not accessible to ordinary users.

Audit log entries

The SMC maintains a log or audit trail of changes made to the simple variables and subsystem descriptors. Not all changes need be recorded; that depends on the variable's so-called "action attributes" (described below). The audit log has 64 entries which are used in a "round-robin" fashion.

Primitive variable types

There are four primitive variable types:

Type	Used for ...
Choice	Variables that can adopt only a limited set of values. For example, *DriveBayLockSensor*, which can have only the value "Locked" or "Unlocked".
Count	Variables that can take a continuous range of values. For example, *BatteryLife*, which records the number of seconds that the UPS batteries can support the machine during an AC power outage.
Time	Variables that specify a particular date or time of day. For example, the current *TimeAndDate* value.
String	Variables that provide descriptions. For example, *SMICBIOSVersion* describes the BIOS on the System Management Interface Card.

The simple SMC variables are all of one of these four types. Subsystem descriptors, user profiles and audit log entries are built up from these primitive types.

Attributes

The attributes of a variable determine who can access it and what actions the SMC should take if its value is changed or goes out of bounds.

A variable's attributes can be changed from within the System Management Application.

Access attributes

These specify whether the variable can be written (SET access) or read (GET access) by the SMC firmware, by SMC client software, or by the System Management Application. In the latter case, the variable may be marked as accessible only to a user of the SMA who has Administrator privileges.

In addition, some choice- or count-type variables can be deleted (marked as "not used") and re-created again if necessary.

Action attributes

These tell the SMC firmware what to do if the value of the variable either changes (change-triggered) or transgresses its upper or lower thresholds (threshold-triggered).

Usually, only subsystem descriptors and simple variables that record the machine state require action attributes. The action attributes of subsystem descriptors are all change-triggered by the current status of the system (normal, degraded or faulty).

Action attributes can tell the SMC to:

- Issue an alert through the SMC's modem and/or control ports. (See the section on "Alerts" below.)
- Record an alert in the SMC's audit log.
- Display the variable's index number on the LCD panel.
- Sound an audible alarm.
- Perform an emergency shutdown, either immediately or after a short hold-off time.

In the case of threshold-triggered actions, alerts are issued whenever the variable's value crosses a threshold. For example, an alert is issued when the value goes over the upper threshold, and again when the value drops back below that threshold. However, the other sorts of actions (audible alarm, LCD display, etc.) occur only when the value goes over the upper threshold or under the lower threshold. This prevents unnecessary actions occurring when a variable goes back to normal after being out-of-bounds, but ensures that alerts are issued to let users and client software know.

In most cases the sound triggered by the alarm attribute depends on the variable's index number. In a few cases the SMC firmware is pre-programmed to associate specific alarms with specific variables.

An immediate emergency shutdown should be used only in the most extreme cases. It causes the server to move to Standby mode (if AC power is applied), or Power Off mode (if AC power is absent). This will cause the operating system to crash with possible loss or corruption of data.

An emergency shutdown incorporating a hold-off time is less potentially damaging. The emergency hold-off time, if sufficiently extended, provides an opportunity to shut down the operating system manually. An emergency shutdown cannot be cancelled.

Special functions

In addition to the actions specified by a variable's action attributes, there can also be special functions that are triggered when a variable changes. These special functions depend on the details of the SMC's firmware programming, and cannot be altered with the System Management Application, except by uploading a new version of SMC firmware.

Alerts

The SMC can issue an alert when the value of a variable changes or if it transgresses its lower or upper thresholds. The alert includes the index number of the variable, its new value, and the date and time that it changed. The alert may be sent through the SMC's external modem port, or its internal control port, or both.

Modem port alerts

Alerts issued to the modem port are queued for each serially-connectable user who has the Force Traps attribute set in their user profile. The alert is then handled as follows:

- If a user is currently connected to the modem port, and the SMC is working in normal mode (i.e. not pass-through mode), the alert is sent to that user. In this case the trap is sent to the connected user irrespective of whether or not the user's Force Traps attribute is set.
- If a user is connected in pass-through mode, the alert is sent as soon as the SMC reverts back to normal mode provided that the user's Force Traps attribute is set. If the Force Traps attribute is not set, the alert is not sent.
- If no user is currently connected the SMC firmware attempts to dial out to one of the users for whom the alert is queued. Each eligible user is tried in turn and the alert is sent to the first workstation that answers.

When a user connects to the SMA, any undelivered alerts queued for that user are delivered automatically.

Alerts to the modem port are automatically suppressed if there is neither a modem nor a cable attached to the port.

Control port alerts

Alerts issued to the control port are picked up by the SMC Device Driver.

The SMC Device Driver passes on the alert to the Network Agent of the System Manager package, which attempts to forward copies of the alert to each of the network-connectable users identified in the SMC's user profiles (or at least, all those that have call-back information). If a particular user's workstation is not currently connected, the Network Agent queues the alert at the server and asks the workstation to connect. If the workstation is not running the SMA it will not receive this request, so the Network Agent repeats it at intervals. Eventually the Network Agent begins deleting the undelivered alerts, starting with the oldest.

The SMC Device Driver also passes on the alert to any other client software that might be interested; for example, the Event Manager and the SNMP Extensions.

Alerts to the control port are automatically suppressed if the SMC Last Client is unloaded.

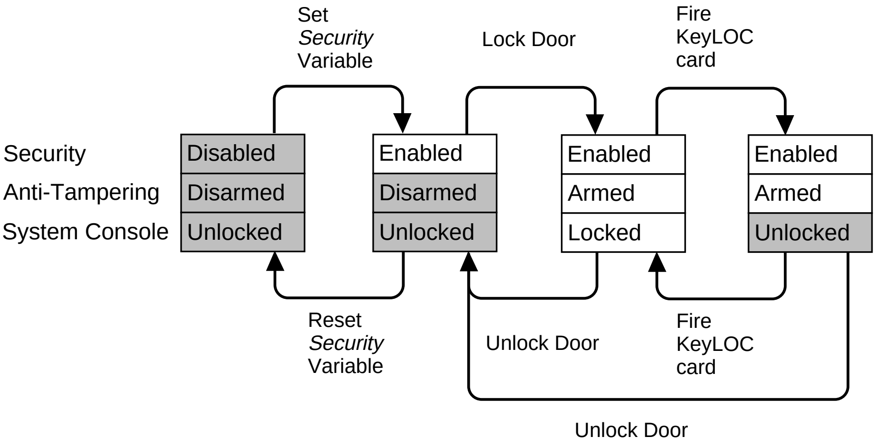
Security

Correct operation of the LOC Technology security subsystem depends on the System Management Application, possession of the key to the removable-media drive bay, and (optionally) special hand-held infrared devices called KeyLOC™ cards.

The security subsystem has three states, or levels of activation:

- Enabled
- Armed
- Locked

The diagram below shows the relationships between these states. Notice that security cannot be armed unless it is first enabled, nor locked unless it is armed.



Enabling the security subsystem

The security subsystem is enabled or disabled according to the state of the *Security* variable. Security is enabled by default but can be disabled by editing the *Security* variable with the System Management Application (refer to the SMA's on-line help for details). Note that the SMA is the *only* means of disabling security.

Arming the server's anti-tampering feature

While enabled, the server can be armed and disarmed by locking and unlocking the removable-media drive bay door. The key to this door is the "security token" that identifies an authorised operator of the computer. It is therefore very important to keep the key in a safe, secure place where it is accessible only to authorised personnel.

While the server is armed, it cannot be started by an unauthorised person, and opening the side panels or attempting to use the front panel buttons (except the Power On button) will trigger a security violation condition.

Starting the server

If the server is manually powered on – by pressing the POWER ON button – while it is armed, the boot process will halt and will not continue until the door to the removable-media drive bay is unlocked. This restriction does not apply to a remote or scheduled power on.

Security violations

If either of the side panels is unlocked while the server is armed, a security violation is triggered immediately, with an attendant "security violation" alarm. (However, the user is not physically prevented from removing the side panel, so additional methods of security are advisable.)

Normally, to prevent accidental use, the front panel STANDBY, RESET or CONTROL buttons must be held down for a few seconds – the actual duration is set by the variable *ShutdownSwitchHoldOffTime* – during which time an audible tone is heard. When the tone stops, the operator knows to release the button.

However, if a button is pressed while the server is armed the "security violation" alarm sounds instead of the usual tone, so that the user knows she is doing something wrong. Only if she persists in holding down the button until the *ShutdownSwitchHoldOffTime* expires is the security violation triggered. In any case, the button will not be actioned.

Once started, a security violation can be cleared by unlocking the door to the removable-media drive bay or by firing a registered KeyLOC card.

Locking the server console

Locking the door to the removable-media drive bay not only arms the server but also locks the server console, provided that the EM Security Client is loaded. This client, which is part of the Event Manager package, locks the console by blanking the monitor display and disabling the keyboard and mouse.

For as long as the server is armed, the console can be locked and unlocked by an infrared pulse from a registered KeyLOC card. Unlocking the console with a KeyLOC card un-blanks the display and re-enables the keyboard and mouse, but does **not** disarm security.

If the EM Security Client is not loaded, firing a KeyLOC card has no perceptible effect, other than silencing any on-going alarm and clearing the LCD panel.

Note
KeyLOC cards are registered with a special KeyLOC Card Registration Utility, which is also part of the Event Manager package. See the AMS Installation Guide *for more information.*

3 SYSTEM MANAGER

The System Manager package allows a network manager or service engineer to connect simultaneously to up to sixteen servers from a single SMA workstation; that is, a workstation running the Windows-based System Management Application.

SMA workstations connect to a server's System Management Controller (SMC) either across the enterprise network or by a serial connection to the SMC's external modem port.

Package components at the SMA workstation

The parts of the System Manager package installed at the workstation are:

- System Management Application
- Network Client
- Serial Client
- DPT Client (optional)

System Management Application

The SMA gives the user an easy-to-understand graphic representation of the state of each monitored server, plus a listing of the most recent alerts received from those servers.

The SMA has an on-line help system which not only contains information about the application itself but also provides definitions of most of the SMC variables.

See the section entitled "More about the System Management Application" later in this chapter.

Network Client

The Network Client is a dynamic link library (DLL) that implements the workstation end of the Reliable Packet

Communications protocol used to connect SMA workstations with remote servers across the enterprise network.

The Network Client is also responsible for finding out which servers are currently running the Network Agent (see below), and hence which servers the SMA can connect to.

Serial Client

The Serial Client DLL is used for remote (dialled-up) or direct serial connections between the SMA workstation and an SMC's external modem port. The Serial Client can handle multiple serial connections if the workstation is equipped with more than one modem.

DPT Client

This is useful if the SMA workstation has a serial connection to a server equipped with a Distributed Processing Technology (DPT) RAID system. The DPT Client updates the Communications Engine supplied with DPT's Storage Manager application. This allows Storage Manager to communicate with the server's DPT RAID engine over the authenticated serial connection used by the SMA (see the section on "Authenticating connections" for more information).

Package components at the server

The parts of the System Manager package that run at the server are:

- SMC Device Driver
- Network Agent
- SMC LAN Client
- SMC RAID Client
- SMC ECC Client (for PENTIUM)
- SMC Event Log Client and Device Driver (for PENTIUM PRO)
- SMC Last Client

SMC Device Driver

The SMC Device Driver sits on the SMC's control port and provides the link between the SMC and the server operating system. The device driver exchanges packets of information between the SMC firmware and server-resident software that has registered with the driver — so-called "client software". Client software includes the Network Agent, the SMC LAN, RAID, ECC and Event Log Clients, and (parts of) value-added packages such as the Event Manager and SNMP Extensions.

The driver allows client software to use various functions of the SMC – for example, to change the value of a variable – and get acknowledgements of success or failure. The driver also enables the SMC to pass alerts to client software. Client software, on registering with the device driver, specifies whether or not it is interested in receiving alerts.

Network Agent

The Network Agent effectively exports all of the SMC's functions across the network, with the exception of the routines used to authenticate connections to the SMC.

For security reasons, the Network Agent is responsible for authenticating connections from networked SMA workstations (see the section on "Authenticating connections" for more information).

The Network Agent is also responsible for passing on alerts to all of the networked SMA workstations recorded in the SMC's user profiles (see the section on "Alerts" in Chapter 2).

SMC LAN Client

The SMC LAN Client gathers performance statistics from the supported Ethernet cards installed in the server and writes this information into the SMC's database. The client is designed to work with most third-party network cards.

SMC RAID Client

The SMC RAID Client gathers performance statistics – which may include predictions of failure – from the server's RAID (Redundant Array of Independent Disks) subsystem, and writes this information into the SMC's database. The client is tailored to the specific hardware RAID system pre-installed in the server.

On a server with a DPT RAID system, the SMC RAID Client is also responsible for passing messages between the RAID engine and the DPT Storage Manager application running at a serially-connected SMA workstation.

SMC ECC Client (PENTIUM)

A PENTIUM-based system incorporates an automatic Error Checking & Correcting (ECC) capability which can correct single-bit errors detected in read and write operations to system memory. The SMC ECC Client gathers performance statistics about how often this feature is invoked, and writes this information into the SMC's database.

Note that this client is used only on PENTIUM systems. It is replaced by the SMC Event Log Client on PENTIUM PRO systems.

SMC Event Log Client and Device Driver (PENTIUM PRO)

On a PENTIUM PRO system several important conditions are monitored by using the System Management Interrupt (SMI) mechanism. Examples include ECC errors, CPU errors and certain voltage signals. (Note that on a PENTIUM system these conditions are monitored directly by the SMC or the SMIC, if they are monitored at all.)

When an SMI occurs the Motherboard BIOS records it in an internal event log.

If the SMI is "non-fatal", the operating system then resumes. Examples of non-fatal SMIs are those occasioned by corrected (single-bit) ECC errors and voltage signals that transgress pre-set warning thresholds. A device driver reads the event log at regular intervals and passes any new, non-fatal entries to the SMC Event Log Client, which updates the relevant SMC variables accordingly.

In particular, the SMC Event Log Client performs the functions of the SMC ECC Client on PENTIUM PRO systems.

Some SMIs generated by these monitored conditions are serious enough to be "fatal". In these cases the operating system is unlikely to survive. Examples include uncorrected (multi-bit) ECC errors, internal CPU errors and voltage signals that transgress critical thresholds. In these cases the BIOS itself updates the relevant SMC variables before generating a Non-Maskable Interrupt (NMI). What happens next depends on the operating system, but in most cases it is likely that the operating system will simply halt.

SMC Last Client

The SMC Last Client, as its name suggests, is always the last client to load when the server operating system is restarted, and the last to unload when the operating system is shut down. It has several important functions:

- On loading, it sets the *NextBootStage* variable to FFF0h, then 0000h. This lets the SMC firmware know that all the clients are loaded and that the SMC can now start sending alerts through the control port.
- Periodically, it refreshes the *WatchdogTimerOut* variable, which restarts the SMC's watchdog timer.
- It keeps the SMC's real-time clock slaved to the motherboard's clock.
- On unloading, it stops the watchdog timer and sets *NextBootStage* to FFE0h (thereby inhibiting any further alerts to the control port).

If the watchdog timer ever decrements to zero, the SMC firmware concludes that it has lost contact with the operating system. The SMC then issues an alert and may also sound an alarm or initiate a reset request (to restart the server) depending on the current value of the *WDTTimeOutAction* variable.

More about the System Management Application

This section summaries the main functions of the System Management Application, as it is typically used by a network manager.

Remote reset, power off and power on

An SMA user has the ability to command the SMC to reset, power off or power on the server. These actions can be done immediately or scheduled to occur at some specified time in the future.

If the Event Manager package is running at the server, this will ensure that the server is shut down gradually before a reset or power off request is actioned.

Disable and re-enable CPUs

You can set configuration options that will disable/re-enable a specified CPU the next time the server boots. You might want to disable a CPU if you suspect it to be faulty or intend to change it.

Remote upgrade of SMC firmware, etc.

The user can upload an entirely new version of SMC firmware, and then reboot the SMC, from within the SMA. In addition, by using the Remote Console feature, the user can also upload new BIOSes or upgrade the software on the Flash disk itself.

Reviewing and amending SMC variables

The values of those SMC variables which permit GET access by the SMA are displayed in a Server window within the System Management Application.

The SMA user can edit the values and attributes of those variables that also permit SET access. Some variables also require the user to have Administrator privileges.

Note that, depending on its attributes, altering the value of a variable can change the behaviour of the SMC or trigger an alert.

Alert monitoring

When an alert arrives at an SMA workstation, it is added to the list of alerts displayed in the Alert Manager window of the System Management Application. Optionally, the user can forward alerts to other destinations, for example by e-mail or Dynamic Data Exchange. The user can acknowledge the alerts and delete them from the list when necessary.

Remote Console

The Remote Console feature relies on the console redirection code in the SMIC BIOS and the SMC's pass-through mode to open a window to the server.

The Remote Console window can be used to watch the server as it boots, allowing the user to note the BIOS sign-on and POST messages. If the server is booted from the SMIC Flash disk, the Flash Disk Utility is started automatically. This lets the user upload new versions of BIOS and run the server's System/EISA Configuration Utility (SCU/ECU).

The Remote Console feature is available only at a serially-connected SMA workstation.

Authenticating connections

The connection between an SMA workstation and the SMC is authenticated, to maintain the integrity of server's management system.

Authorised users of the SMC are identified by a set of sixteen user profiles in the SMC's database. These profiles can be created and edited only by a user with Administrator privilege.

Each user has a user name and a password. A remote workstation is identified either by the telephone number of its modem or a network-specific identifier, depending on the type of connection.

Remote serial connection

When a user at remote SMA workstation attempts to dial-in to the server, the user name is validated by the SMC. If the user name matches one of the user profiles, the SMC returns a one-time encryption seed to the SMA, then breaks the connection and calls the workstation back using the telephone number contained in the user profile. The SMA encrypts the user's password using the seed obtained from the server, then the encrypted password is decrypted and validated by the SMC.

(Direct serial connections are authenticated in the same way, except that in this case the connection is not broken half-way through.)

Remote network connection

When a user at a networked SMA workstation attempts to connect to the server, the user name is validated by the Network Agent (using routines provided by the SMC firmware). If the user name matches one of the user profiles in the SMC's database, the Network Agent returns a one-time encryption seed to the SMA. The SMA in turn encrypts the user's password using this seed, and the encrypted password is decrypted and validated by the Network Agent.

4 EVENT MANAGER

The System Management Controller (SMC) tests and monitors various subsystems within the server. The current state of the server is recorded in a database of variables held in the SMC's battery-backed memory.

Typically, the first indication of an abnormal or significant event occurring within the server is when the value of an SMC variable changes or transgresses its upper or lower thresholds. Depending on the variable's so-called "action attributes", this may cause the SMC to issue a trap (also called an alert). The trap identifies the variable, its current value, and the date and time that it changed.

Traps can be sent through the SMC's external modem port, or its internal control port, or both. Traps sent through the control port are picked up by the SMC Device Driver and passed on to other software that might be interested, such as the Event Manager.

In a few cases it is possible for a change in a variable to trigger a special function within the SMC's firmware programming, explicitly responding to the event that caused the change.

The Event Manager augments the SMC's programming by providing a set of OS services which respond to certain traps in accordance with a script file. Examples of traps of interest to the Event Manager are those attending AC power outages, fan failure, inappropriate use of the front panel controls, and unauthorised attempts to access the server's interior.

The general idea is that by following the script file, the Event Manager will gracefully shut down the operating system in critical situations, and notify appropriate users in non-critical situations.

Package components

The Event Manager package consists of the following software components. Note that the services need not necessarily be implemented as separate programs.

- SMC Device Driver
- EM Trap Handler
- EM UPS Service
- EM Standby/Reset Service
- EM Environment Service
- EM Security Service
- EM Security Client
- KeyLOC Card Registration Utility

These software components make use of three data files:

- EM Event Mapping File
- EM Script File
- EM Log File

SMC Device Driver

The SMC Device Driver sits on the SMC's control port and provides the link between the SMC and the operating system. The driver passes traps from the SMC to the EM Trap Handler and allows the Event Manager to use various SMC functions — for example, to change the value of a variable.

EM Trap Handler

The EM Trap Handler uses the EM Event Mapping File to decide whether the trap is relevant to the Event Manager, and if it is, which service should deal with it. The EM Trap Handler tells the appropriate service that a significant event has occurred.

The EM Trap Handler is also responsible for monitoring the link to the SMC.

EM UPS Service

The EM UPS Service is concerned with the events surrounding a loss of AC power. In this situation the Uninterruptible Power Supply (UPS) takes over immediately but the time on battery power is limited. The UPS Service follows the commands in the user-defined EM Script File to shut down the server gracefully and in good time.

EM Standby/Reset Service

The EM Standby/Reset Service deals with shutdown and reset requests. A shutdown request is a request to move the server to an dormant mode (usually Standby mode but possibly Power Off mode). A reset request is a request to restart the computer.

These requests can be initiated in various ways: by someone pressing the STANDBY or RESET button on the front panel, by a command from the System Management Application, and so on. The EM Standby/Reset Service ensures that the server is properly shut down before the request is granted.

EM Environment Service

The EM Environment Service is concerned with overheating within the system unit. Overheating can degrade performance and damage system components. To detect overheating (or the risk of overheating) the SMC monitors thermal sensors and the cooling fans. The EM Environment Service alerts network managers and other users to the overheating condition.

EM Security Service

The SMC incorporates a LOC Technology™ security subsystem that deters unauthorised access to or use of the server. When the security subsystem is enabled and the server is armed, any attempt to open the side panels or use the front panel buttons can trigger a security violation condition. The EM Security Service alerts network managers and other users to security violations.

EM Security Client

The Event Manager package includes an EM Security Client which will, if loaded, blank the monitor display and disable the keyboard and mouse to lock the server console, and un-blank the screen and re-enable the keyboard and mouse to unlock the console, whenever the SMC recognises an infrared pulse from a special hand-held device called a KeyLOC™ card.

KeyLOC Card Registration Utility

Up to sixteen KeyLOC cards can be registered at a server, by means of the KeyLOC Card Registration Utility. For more information, see the *AMS Installation Guide*.

In the absence of an operating system, the System Management Application can be used to register KeyLOC cards. See the *SMA User's Guide* for more information.

EM Event Mapping File

As mentioned above, this file is used by the EM Trap Handler to decide which traps passed to it from the SMC Device Driver are relevant to the Event Manager package.

EM Script File

The EM Script File is a text file which can be amended by any text editor. The script consists of special **eventmgr** commands, or the equivalent operating system commands where available, grouped under labels which correspond to the events and conditions notified to the Event Manager by the SMC. Event labels can also be defined to schedule commands at regular intervals while a given condition persists, or at a set period before or after another event. When an event occurs, the appropriate EM service – UPS, Standby/Reset, Environment or Security – executes the commands listed under the corresponding label.

EM Log File

The EM Log File is a text file used by the Event Manager to log the occurrence of events and conditions. Log entries are made by including **eventmgr log** commands at the appropriate points in the EM Script File.

5 SNMP EXTENSIONS

The Simple Network Management Protocol (SNMP) is an industry-standard protocol for network management applications. The Apricot Management Suite does not use SNMP, but through use of the SNMP Extensions package the database of variables maintained by the System Management Controller (SMC) can be integrated with third-party SNMP-based products. This allows the user to view (GET) most of the SMC variables, and receive traps from the SMC.

Third-party SNMP-based applications

An SNMP-based network management application will typically include at least three elements:

- Management Information Base (MIB)
- SNMP Agent
- SNMP Client

Management Information Base

A MIB is a description of the objects (subsystems and variables) that the network management application can manage. All SNMP Agents support the vendor-independent information defined in one of the standard MIBs known as MIB 1 or MIB 2 (the former is a subset of the latter). In addition, vendors often provide private or enterprise-specific extensions to the standard MIBs that allow their particular SNMP Agents to access proprietary information.

SNMP Agent

The SNMP Agent resides on the server and is the software responsible for retrieving information and returning it to the remote network management workstation for display.

SNMP Client

The SNMP Client application runs at the remote network management workstation. The details will vary between different vendors, but all client applications can be expected to include a MIB Browser and some means of receiving and displaying SNMP traps. A MIB Browser is used to access the information described by one or more MIBs. SNMP traps may be issued by the SNMP Agents when the value of a monitored parameter changes or goes out of bounds.

If the SNMP Client is Windows-based it can conveniently be installed at the same workstation as the System Management Application (SMA).

Package components

The SNMP Extensions package consists of three main components:

- Apricot MIBs for PENTIUM and PENTIUM PRO systems
- SMC Device Driver
- SNMP Extension Agent

Apricot MIBs

There are separate Apricot MIBs for PENTIUM and PENTIUM PRO systems. Each Apricot MIB describes most of the variables held in the SMC's database. Some variables are omitted, chiefly for security reasons (SNMP is not an inherently secure protocol). So for example the user profiles, the audit log and critical variables such as *ShutdownRequest* are not included.

The Apricot MIBs must be compiled together with the other MIBs at the remote network management workstation so that the SMC variables can be read by the SNMP Client's MIB Browser. Note that the variables can only be read (GET access), not written to (SET access).

SMC Device Driver

The SMC Device Driver sits on the SMC's control port and provides the link between the SMC and the server operating system. The driver allows the SNMP Extension Agent to read SMC variables and also passes on alerts issued by the SMC.

SNMP Extension Agent

The SNMP Extension Agent is installed at the server in addition to the third-party SNMP Agent (described above).

The SNMP Extension Agent is also an SMC client; in other words, it communicates with the SMC firmware via the SMC Device Driver.

When the SNMP Client's MIB Browser asks to retrieve the value of an SMC variable, the SNMP Agent passes the request to the SNMP Extension Agent, which GETs the value from the SMC.

The SNMP Extension Agent also receives the alerts that are issued by the SMC through its internal control port. Those alerts that relate to variables in the Apricot MIBs are converted into SNMP-type traps and relayed back to the network management workstation via the SNMP Agent. Alerts relating to variables which are not included in the Apricot MIBs are discarded.

15691131

MITSUBISHI

apricot

MITSUBISHI ELECTRIC PC DIVISION

APRICOT COMPUTERS LIMITED
3500 PARKSIDE
BIRMINGHAM BUSINESS PARK
BIRMINGHAM B37 7YS
UNITED KINGDOM

http://www.apricot.co.uk