HYTEC ELECTRONICS LTD

1365 Ethernet CAMAC Crate Controller MK4

Technical Handbook

Issue 1

AMENDMENT RECORD

Issue	Date	Change	Author	Reviewed by
1	August 2001	New Document	P. Marshall	M.Woodward

Checked by :- Date:-

[P. Marshall] Authorising Engineer

The use of the equipment described herein does not constitute any health or safety hazards when used according to the instructions contained in this handbook. However, your attention is drawn to the following basic safety precautions, which should be observed.

1. Ensure that the instructions contained herein have been carried out and that users have received adequate training.

2. If in doubt regarding the safe operation and maintenance of this equipment, consult Hytec Electronics Ltd.

WARNINGS MUST BE OBSERVED AT ALL TIMES

THEY ARE PRINTED FOR YOUR PROTECTION.

Whilst every effort has been made in this handbook to instruct users in the correct methods of using the equipment, Hytec Electronics Ltd. accepts no liability for personal injury or damage to the equipment howsoever such injury or damage might be caused.

This handbook is believed to be accurate in all respects at the time of printing. However, customer’s special requirements and other circumstances might make modifications necessary from time to time.

Although every effort is made to keep the handbook relating to every part of this equipment in step with future modifications, users are advised that if any doubt exists regarding any statement, illustration or diagram, reference must be made to the supplier.

Hytec Electronics Ltd. acknowledges all registered trademarks.

This page is intentionally blank

1365 Ethernet Crate Controller MK 4
28/8/2001

FIGURES

TABLES

ABBREVIATIONS

These abbreviations are used throughout

Each abbreviation is shown in full when first introduced in each chapter.

ACB	Auxiliary Controller Bus
UTP	Universal Twisted Pair
COR	CAMAC Operation Routine
DOE	Department of Energy
DTM4	CAMAC Dataway Test Module– Type 4 (Available from Hytec Electronics Ltd. UK)
ECC	Ethernet Crate Controller
ECP	Ethernet CAMAC Protocol
ESONE	European Standards on Nuclear Equipment
FAP	Find Address Protocol
LAM	CAMAC Look at Me Interrupt
LLC	Logical Link Control
LSAP	Link Service Access Point
NTP	Network Time Protocol
PID	Process Identifier
QSPAN	Motorola-to-PCI bridge chip
TCP/IP	Transmission Control Protocol / Internet Protocol
UDP	User Datagram Protocol

CHAPTER 1

1 INTRODUCTION

This handbook is concerned with the Ethernet Crate Controller, type ECC 1365 MK 4. It is one of a range of CAMAC modules designed in the U.K. by HYTEC Electronics Ltd. Hytec is a long established hardware, software and systems company, which leads CAMAC development in industry and research.

1.1 How to use this Technical Handbook

The intended audience for this manual is both the purchaser of the ECC 1365 module who wishes to get it configured and operational and for the system implementer who wishes to learn about the module.

For the system implementer who wishes to learn about the module, he or she should read the chapters in the order presented.

For the purchaser of an ECC 1365 module who wishes to get it configured and operational, he or she should optionally read Chapters 1, 2 and 3 if familiarisation is necessary, and then proceed to Chapter 8.

It is essential that new purchasers read Chapter 8 thoroughly.

Installation of host software for VMS and UNIX is covered in the Installation Guide. In all cases, it is assumed the reader is familiar with CAMAC systems and Ethernet Local Area Networks.

1.2 An outline of the ECC 1365 MK 4 functions

The ECC 1365 MK 4 controller is the latest version in the ECC 1365 range. It is an enhanced performance version of the MKIII controller. It uses a 32-bit Motorola 50MHz 68EC060 processor with cache instead of the 68EC030 processor used in the MKIII. It also uses a later generation higher performance Intel 82559 PCI Fast Ethernet chip in place of the SONIC (System Oriented Network Interface Controller) chip used in the MKIII. Other functional changes described in detail in this document and highlighted in our sales literature are also present. The result is that the MK 4 controller is able to show a significant performance improvement over the MKIII version.

The HYTEC 1365 Ethernet CAMAC Controller (ECC 1365) is a two-width controller (ACB Master or Slave), designed to be driven from one or more hosts across an Ethernet local area network. This provides a fast and efficient interface between a CAMAC crate and a UTP Ethernet LAN.

The ECC 1365 MK 4 is based on a 32 bit Motorola 68EC060 processor with cache, with comprehensive firmware resident in 256 Kbytes of EPROM, plus processor working space in 2 Mbytes of RAM. Unused RAM can be configured to hold user-written downloaded commands and/or routines.

The front panel has one LAN connector – an 8-way MMJ-type 10/100 UTP connector. It also has an RS232 port (9-way D-type), for local diagnostic terminal support.

The following features are provided by the ECC 1365:

- Compliant with CAMAC ACB – can be Master or Slave
- Full specification 10/100 UTP Ethernet with Auto-negotiation
- Uses a Motorola 68EC060 processor (50 MHz) with cache
- Supports multiple concurrent hosts
- Network Time Protocol Support
- Provides data timestamping
- Supports Block mode and List mode facilities
- Responds to down-line-loadable user-defined commands
- Software support available for a range of hosts, including:

  Alpha AXP
  DEC VAX/VMS
  WindowsNT
  LINUX
  UNIX systems via User Datagram Protocol and Internet Protocol
  (Note: UDP is normally available as part of the TCP/IP protocol set)

- Compliant with ISO/IEC IS8802-3 CSMA/CD
- Supports standard ESONE /DOE subroutines
- Security, including controller-resident access tables
- Logical Link Control (ISO /IEC IS8802-2) support
- User Datagram Protocol / Internet Protocol (UDP/IP) support

CHAPTER 2

2 HARDWARE OVERVIEW

The Ethernet Crate Controller is a two-width CAMAC module. It consists of two PCBs. The left board (viewed from the front) is the main board and is known as the Controller Board. The right board is the support board and contains the N and L Line decoding and pull-up resistors.

The controller can act as a Master Controller (see Chapter 8, USING THE ECC 1365, Page 71) or as an Auxiliary ACB Controller.

Front-panel connectors are provided for Ethernet, i.e. there is a standard 8-way MMJ Type UTP connector, and a 9-way D-type diagnostic terminal connector.

2.1 The Controller Board

This full-size board takes up the left of the controller module and holds the:

50 MHz 68EC060 processor with cache

64K x 32–bit long words of EPROM (firmware)

512K x 32-bit long words of static RAM (all battery-backed)

Configuration Switches and jumpers

QSPAN PCI Bridge chip

Intel 82559 PCI Fast Ethernet chip

MC68901 multi-function peripheral chip for diagnostic terminal and timing functions.

Optional full 32-bit PCI socket for adding extra functionality

Xilinx-based CAMAC port and associated Ethernet address PROM.

2.2 The Support Board

The support board is a short board containing: -

~ The N Line decoders.
~ The N and L line pull-up resistor packs

2.3 The UTP Ethernet Connection

The 10/100 Mbit UTP connection is accessed at the front panel, via an 8-way MMJ-type connector. Data is passed between the ECC 1365 and the Ethernet via this connection. The Intel 82559 automatically connects at the highest available rate through auto-negotiation.

2.4 The Front Panel

The front panel is a standard two-wide panel from which all the ECC 1365 external functions are connected, see Figure 1.

This figure shows:

~ Twelve status LEDs, see below

~ Two Crate Address rotary switches

~ Three Request-Grant connectors

~ UTP Ethernet connector

~ A controller Reset / Normal / Diagnostic mode toggle switch

~ An RS232 Diagnostic connector (9-way D-type)

~ CAMAC ZED button

A full description of these functions is given in Chapter 8.1, Installing the ECC 1365, Page 68.

Front Panel Status LEDs

NOX	ON = No CAMAC X on last CAMAC cycle
NOQ	ON = No CAMAC Q on last CAMAC cycle
INH	ON = CAMAC Inhibit Line Asserted
SEC	ON = No Security table entries present (controller is OPEN)
DIAG	ON = Diagnostic mode selected. Normal operation not possible
DENB	ON = CAMAC demands enabled to at least one host
COMM	ON = Executing Command – Firmware is executing an internal command
FAST CAMAC	ON = Executing CAMAC transfers in Fast CAMAC mode (later enhancement)
CAMAC	ON = Executing CAMAC cycle
LINK	ON = UTP Link established
ACTIVE	ON = Network traffic active
SPEED	ON =100 Mbit link established.

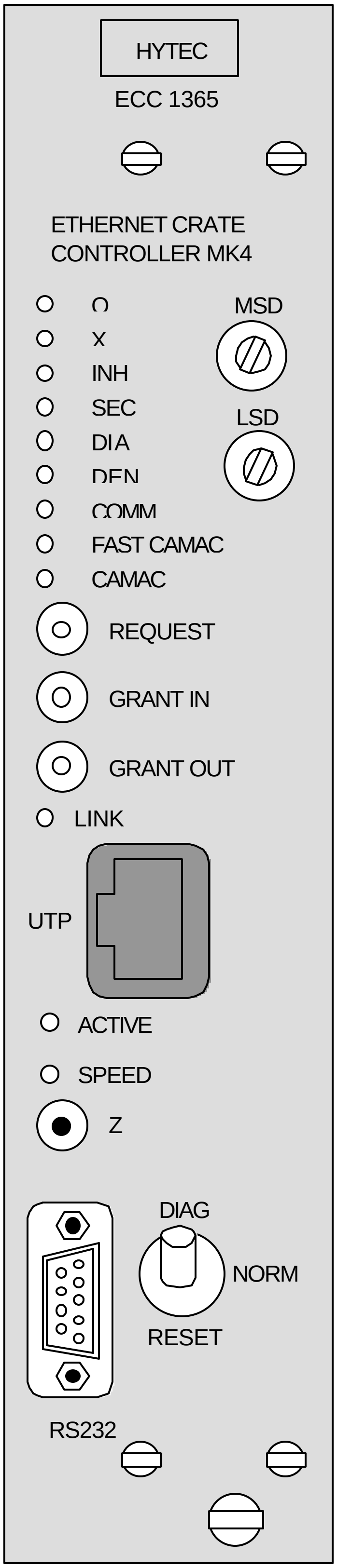


Figure 1 1365 MK 4 Front Panel Details

CHAPTER 3

3 SOFTWARE OVERVIEW

3.1 Host Software Overview

Host control of the ECC 1365 is achieved by specific CAMAC command and control messages, delivered to the controller by either Logical Link Control type 1 & type 3 protocols (LLC1 & LLC3) or the UDP/IP protocols. Users who prefer to implement their own host support can do so by using the protocol definition documents available from Hytec Electronics Ltd.

Host support for DEC VAX, running VMS via logical link control protocols, and UNIX Systems via the User Datagram Protocols are available. This includes device drivers, protocol handlers and system processes, to manage user process requests and to provide configuration and time protocol support.

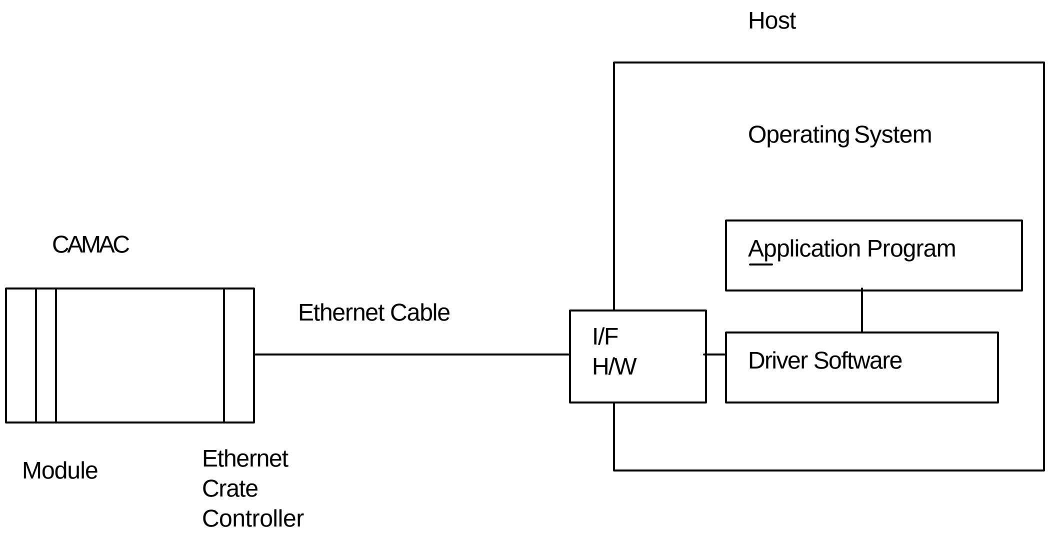


Figure 2:Ethernet/CAMAC System

High-level language support is provided through a library that includes the ESONE / DOE subroutines, with further routines to support the extra functionality of the controller. A command line interface is available, to display the known configuration and individual controller statistics on a host terminal.

Use of message utilities are made for error reporting and system information messages.

3.1.1 VMS Host Introduction

A detailed description of VMS host software is given in Appendix 3.

The host software is designed to provide user access to Ethernet Crate Controller (ECC 1365) modules on an Ethernet local area network. It runs under VMS (VMS is a trademark of Digital Equipment Corporation). It supports multiple users on a single host system accessing multiple ECC modules. Multiple host systems on the Ethernet are similarly supported.

The software is divided into two distinct parts; that which runs as part of a user's process and that which runs in the system, see Figure 3. The former is available to the user as a set of callable subroutines or a set of functions and these are provided in a l ibrary. The system software acts as the focus for users' access to ECC 1365 modules on the Ethernet.

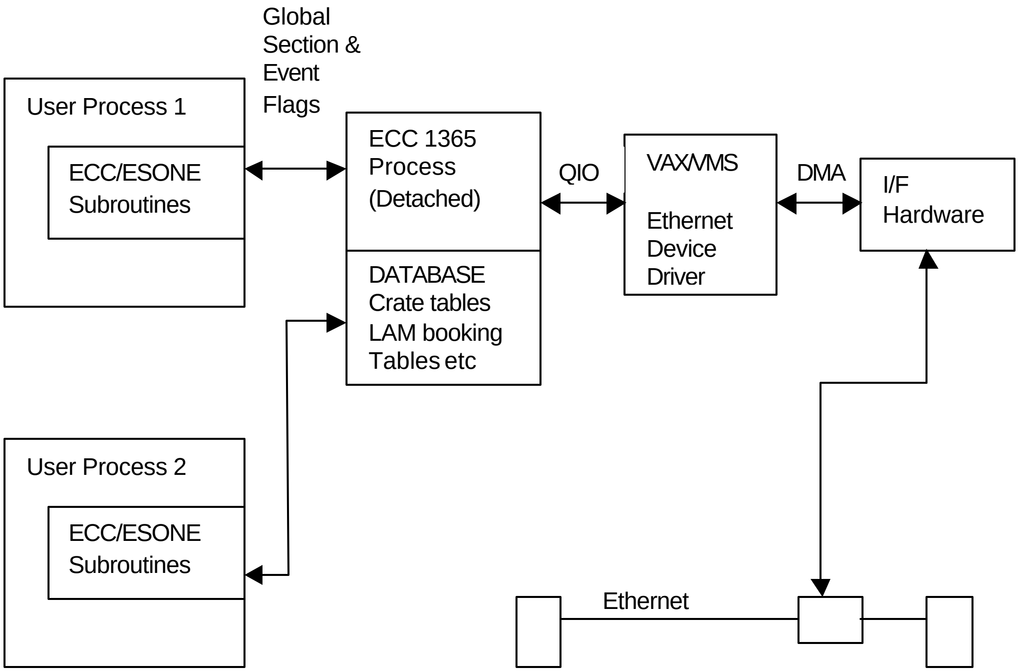


Figure 3 VMS Host Processes

3.1.2 Unix Host Introduction

The UNIX host software was originally written for the SUN Microsystems SUNOS Operating System. This is SUN's own version of UNIX, closely aligned to AT&T's System V. The protocols employed are the User Datagram Protocols and the Internet Protocols UDP/IP and are part of the TCP/IP Protocol suite.

It is th e UDP socket interface and the system calls for access and allocation of shared memory that are likely to have shades of difference between flavours of UNIX. Hytec will normally undertake to give the support necessary to get the UNIX Host Software operational on other UNIX versions.

A system process is provided, similar to the VAX/VMS option, with a user process interface using shared memory. The organization is similar to that shown in Figure 3.

3.1.3 User-based Software

A user process is able to communicate via the ESONE/DOE CAMAC subroutines (which do not return until the specified operation is complete) or via a set of extended subroutines (which return immediately). The latter require a user to call to a generalized wait routine, to receive the command completion status when it is available. The routines also exist as a set of function calls.

The subroutines make use of the CTSTAT subroutine to provide status information to the user-based software. The CAMAC functions return status directly to the user bas ed software, making the call to CTSTAT redundant.

An additional set of routines is provided to allow the user to access the full functionality of the ECC 1365.

All routine calls cause a parameter block to be built, based on the parameters passed as arguments, together with an internal identification code which uniquely identifies which routine has been called. First –order error checking is carried out at this stage and errors are available when control passes back to the user-level software.

The extended ESONE/DOE CAMAC routines have, as additional arguments, a variable identifying a local event flag (set on completion) and the address of an I/0 status block that contains, on completion, the final status of the command.

A description of the EOSNE/DOE Subroutines is given in a separate document – see ref. 13.

3.2 Firmware Overview

The standard firmware supplied with the ECC 1365 MK 4 is loaded into 4 on-board EPROMs.

The firmware supports both the Logical Link Control transport protocols recommended for use with VMS host-based configurations and the User Datagram Protocols (UDP)/Internet Protocols (IP) intended for use with UNIX host-based configurations.

Both versions support the same controller functionality for;

The command structure
Booking
Queuing
Interrupts.

The ECC 1365 and its associated software are designed to be used in a system with a configuration typically as illustrated in Figure 4.

Commands and data are passed across the Ethernet from the host system to the ECC 1365, using Logical Link Control procedures (LLC1) & (LLC3) or UDP protocols. Responses and data are received by the host from the Ethernet, using these protocols. The UDP protocols encapsulate the LLC protocols so that a UDP / IP host must also prepare the LLC protocol packets.

Each ECC 1365 can be controlled by more than one host; a CAMAC module-booking scheme is used by the ECC, to prevent more than one host attempting to control the same CAMAC module at any one time. This can be disabled by setting the module “promiscuous” bit in the controller-booking table.

Each host can control CAMAC modules in more than one ECC 1365. A multi -host / multi-ECC configuration is illustrated in Figure 5.

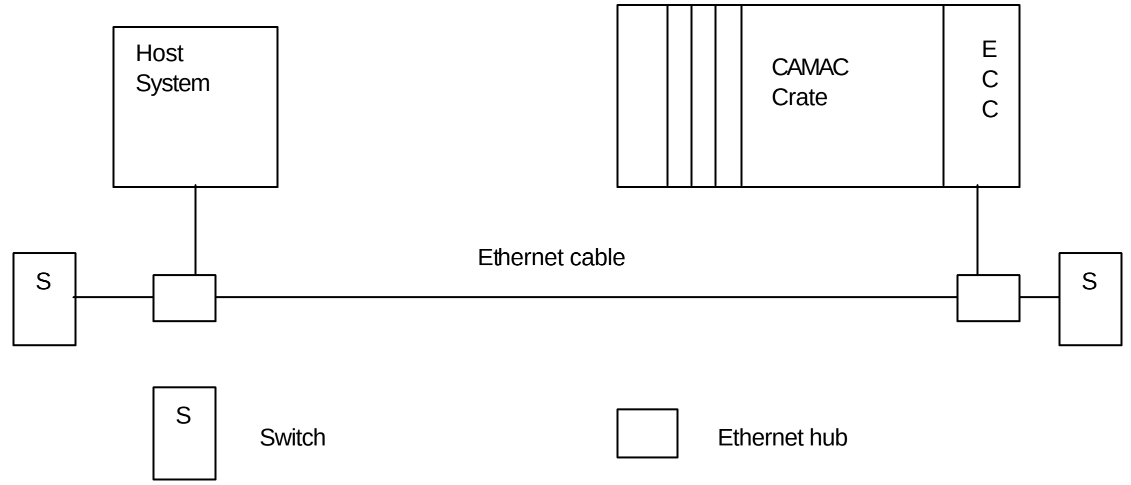


Figure 4 A simple System Configuration

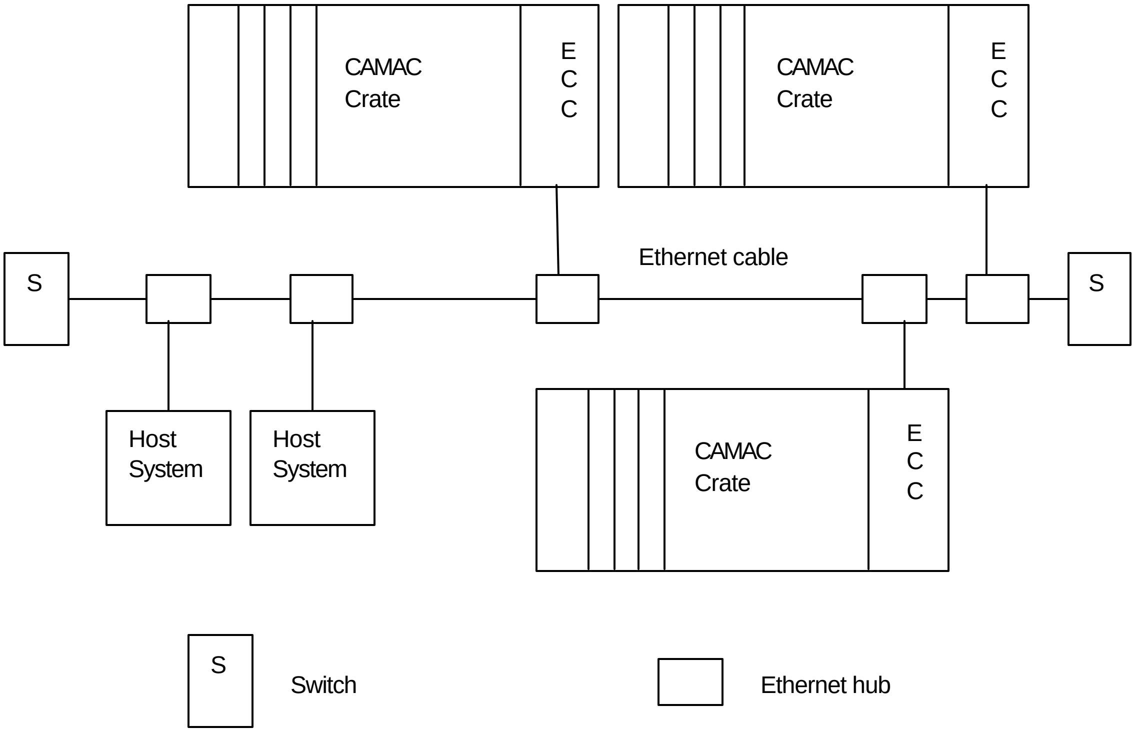


Figure 5 A multi host, multi-ECC system configuration

If a host has a multi-task operating system, each task within that host can control more than one ECC 1365, with each task acting independently.

The commands and data passed across the Ethernet are encoded in a format that allows efficient and flexible control of the ECC 1365. The standard ESONE / DOE subroutines are available in the host and later sections describe both the coding scheme andthe ESONE / DOE subroutine mappings. The coding scheme permits a more flexible control of the ECC than allowed by the ESONE / DOE subroutines.

One of the extensions available in this release of the software allows the host software to continue operation whilst an ECC 1365 action is in progress (asynchronous calls).

A common time is maintained across the components of the system (as described in5,NETWORK TIME, Page 36, Network Time). The host can request timestamps to be appended whilst an ECC 1365 request proceeds through the system.

A security feature is implemented which allows a system administrator to define which hosts can access the ECC 1365. Hosts can be denied access to the whole crate or to individual stations within the crate. Similarly, access to security table updating, issuing CAMAC Z, C and I or access to downloading new operation routines or commands can be controlled. When no data exists in the battery-backed RAM security table or the internal switch disabling security is ON, the whole controller is completely open. Note, module and LAM booking is still operational when the controller is OPEN.

For multi-tasking host environment an option exists to either enable or disable PID booking. PID booking enables booking of CAMAC stations and / or LAMs down to the individual process identifiers (PIDs) in the host system. If PID booking is off then the booking is to be the host ID only.

The automatic booking of stations when they are accessed for the first time is known as auto booking. This feature can be enabled or disabled.

3.2.1 Major Functions

~ Support for the QSPAN PCI bridge and Intel 82559 Ethernet chip set.

~ Driving the controller's internal CAMAC interface.

~ Driving the Logical Link Control (LLC1 & LLC3) protocols and the UDP/IP protocols (subset of TCP/IP).

~ Driving the Hytec-specific CAMAC command protocols.

~ Servicing and support for CAMAC interrupts.

~ Support for Block Mode & List Mode commands.

~ Support for down loadable user defined CAMAC operation routines or new complete commands.

~ Timer support, including controller timekeeping, network time protocol support and data timestamping support.

~ Maintenance of booking tables.

~ Booking tables for CAMAC station booking (booked to a single host on the network or to a single process in a multi-processing host).

~ LAMs can be booked to a single host on the network or to a single process in a multi-processing host.

~ Auto booking of CAMAC stations is optionally supported.

~ "Promiscuous" modes are supported, i.e. unrestricted access from any host or process.

~ Security features support. Security tables, in battery-backed RAM, control which hosts can access this controller.

~ Front panel terminal handling. This allows a standard RS232 terminal to be connected to the controller, to modify the security tables and examine the controller statistics tables.

~ Statistics-gathering support. The firmware will gather statistics on Ethernet messages, failures, errors, recoveries, etc. plus CAMAC statistics, such as a number of LAMs, double-booking attempts, security violations and Dataway timeouts.

3.2.2 CAMAC Functionality

These features combine to provide the controller with comprehensive CAMAC functionality. This includes;

- ~ Single action CAMAC commands
- ~ Block mode CAMAC commands, including

  Address scan modes
  LAM synchronised modes
  Controller synchronised modes
  All Q modes

- ~ List mode CAMAC commands. Command lists can be loaded and executed repeatedly.
- ~ Full Q, X and timeout error handling (by message to hos t).
- ~ Normal CAMAC controls of Z, Clear, Inhibit, etc.
- ~ Full CAMAC LAM support. Host processes are notified when booked LAMs occur. Block and List modes can be synchronised to LAMs.
- ~ User defined controller commands can be downloaded from a host and then executed (this permits applications to set up extra controller capability, if needed).

CHAPTER 4

4 SYSTEM PROTOCOLS

The controller supports both the Logical Link Control and the UDP/IP protocols.

4.1 Transport Layer Protocols

The firmware supports two transport layer protocols. Hosts can access the controller using either of these, the controller is able to deal with both simultaneously.

Logical Link Control was chosen as an efficient, lightweight protocol to provide guaranteed delivery, message sequencing and transaction processing. It provides a secure, low-overhead system and is the protocol used with Hytec's VAX/VMS host implementation.

UDP/IP is supported to satisfy the increasing number of UNIX environment users.

User Datagram Protocols (UDP) is a member of the TCP/IP protocol set and is generally supported on UNIX implementations. When using UDP protocols, the Logical Link Control protocols are still used. The message, must be a normal LLC protocol message, then passed to the controller using UDP to encapsulate it. See figure 6.

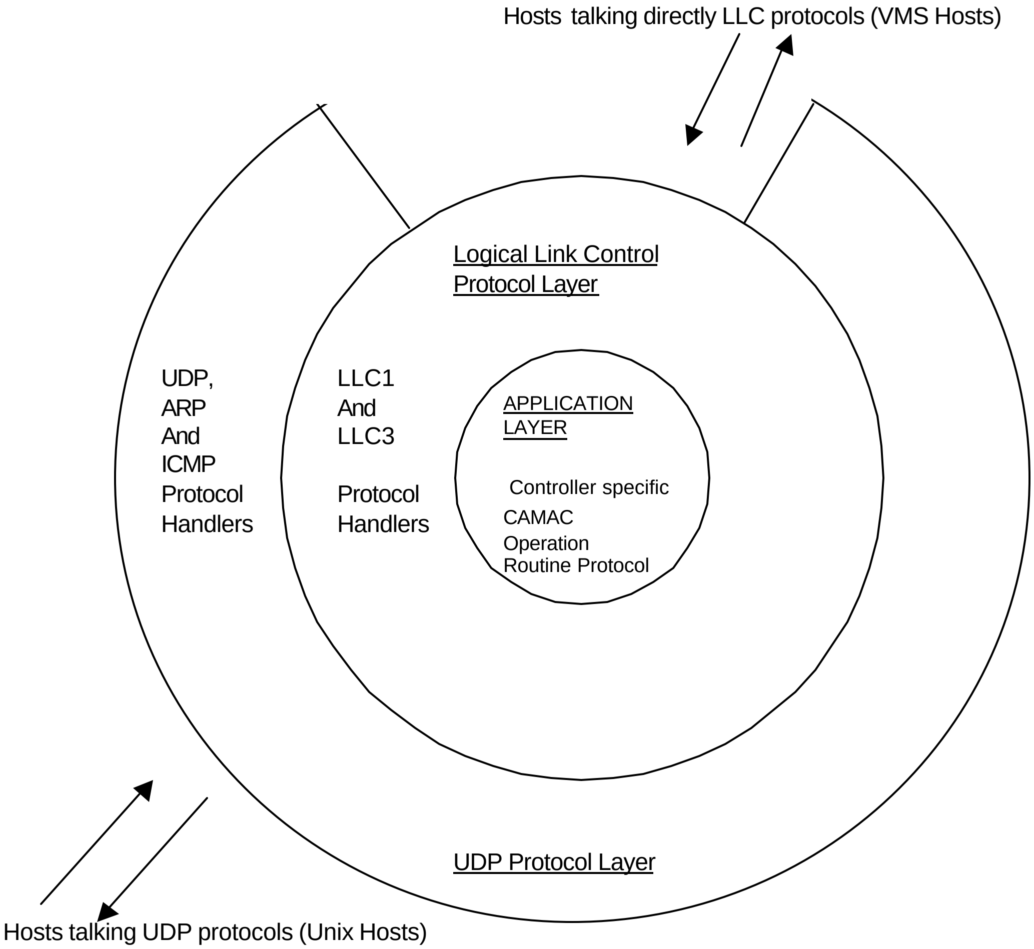

Hosts talking directly LLC protocols (VMS Hosts)
Logical Link Control Protocol Layer
UDP, ARP And ICMP Protocol Handlers
LLC1 And LLC3 Protocol Handlers
APPLICATION LAYER
Controller specific CAMAC Operation Routine Protocol
UDP Protocol Layer
Hosts talking UDP protocols (Unix Hosts)

Figure 6 Protocol Layer model for the ECC 1365

4.1.1 Logical Link Control

Both Logical Link Control (LLC1 and LLC3) procedures are used to transfer information between the host(s) and the Ethernet Crate Controller(s) (ECC(s)).

LLC1 is used for:

Timer updates
ECC 1365 status requests
ECC 1365 reset requests
Find Crate address requests.

LLC3 is used to transmit command blocks to the ECC 1365 and to return the ECC's response. Two methods of operation are available:

Immediate response, where the command block is executed as soon as possible after reception by the ECC 1365.

Deferred response, where the command block is queued by the ECC 1365 for later execution.

The network interactions for these methods of operation are illustrated in Figure 7. A pair of (LSAP) addresses are used, one for commands issued by the host and the other for commands issued by the ECC 1365.

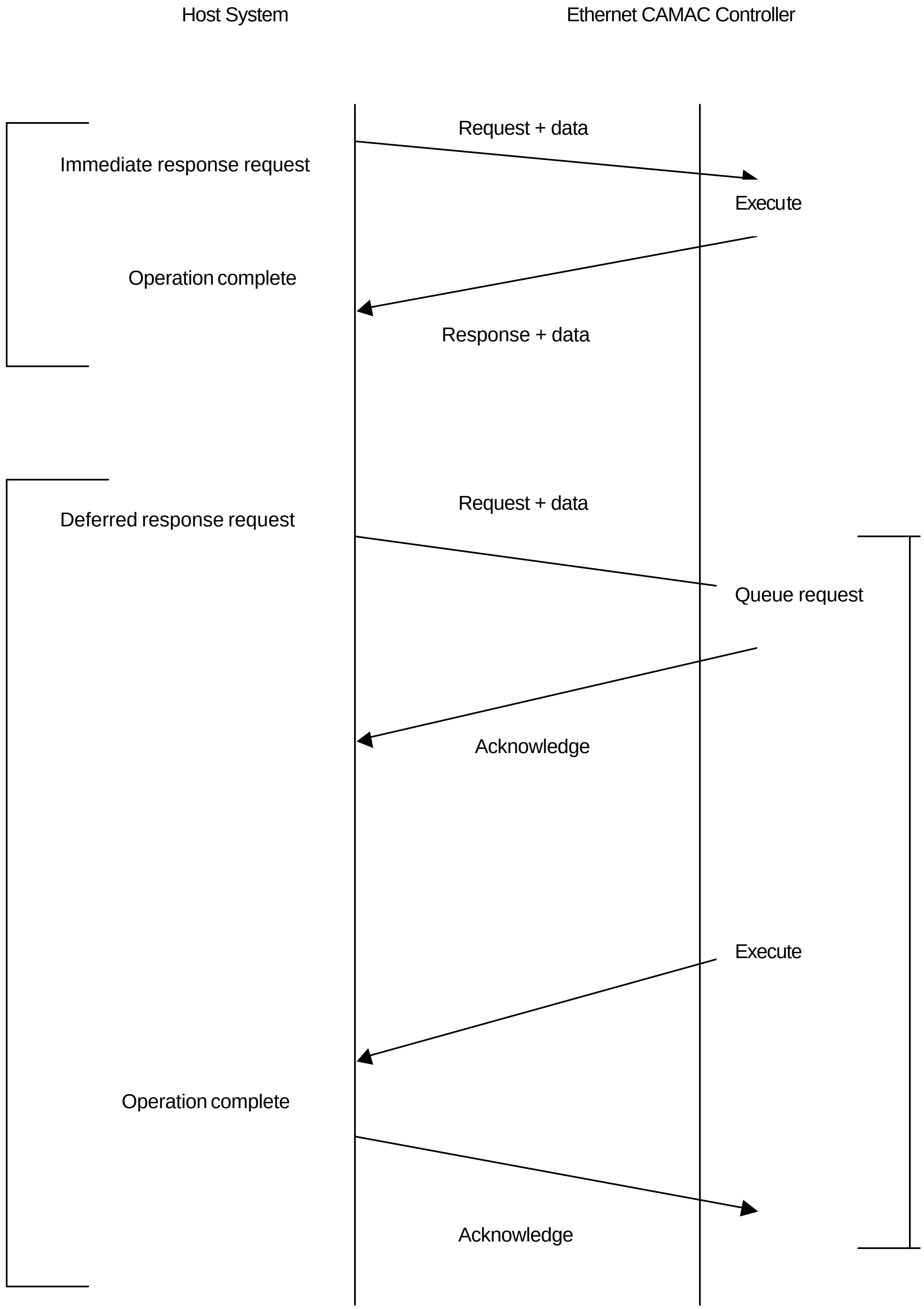


Figure 7 Network Interactions

Because LLC3 procedures are used for the main interaction between host and the ECC 1365, a constraint is placed such that only one LLC3 operation (command-response sequence) can be in progress between a given host and a given ECC 1365 at any time in a given direction.

Some Ethernet drivers, e.g. the current VMS driver, cannot transmit and receive LLC3 frames. For these systems, a "pseudo LLC3 " protocol is available. In this protocol, the LLC3 control and status fields are carried in the first two bytes of the data area of the frame and the frame is converted to an LLC1 UI frame. All the normal LLC3 procedures are operated using these two moved fields.

4.1.2 UDP/IP

The term TCP/IP has come to describe a family of Internet Protocols and not just the specific Transmission Control Protocol and Internet Protocol (see ref 15). The protocol of most immediate use to the ECC 1365 operation is the User Datagram Protocols (UDP). Most UNIX implementations that include TCP/IP support include UDP as well as part of the protocol family. Users should check specifically with the version of UNIX and / or TCP/IP that they intend to use supports the User Datagram Protocol.

In order to achieve a single firmware set that supports both Logical Link Control and UDP/IP, LLC3 procedures are carried in /Internet UDP/IP frames. Each ECC 1365 may be controlled by more than one host using either LLC1 / LLC3 or UDP/IP protocols; the ECC 1365 will decide dynamically which protocol the host is using.

The use of Internet UDP frames allows host systems with standard socket interfaces to communicate easily with the ECC 1365 without the need to program at the Ethernet device driver level. This is achieved by taking the standard "LLC3" frame, excluding the two Ethernet address fields and the MAC length field (i.e. starting from the LCC LSAP field) and placing it as data in a UDP frame. As UDP is a datagram protocol, LLC3 procedures are used to control the flow of data to and from the ECC 1365.

When the Internet Protocols are used, the Find Address Protocol (FAP) is not available and crates are accessed by a crate number to internet address look up table maintained in the IP host (IPADDR.DAT). The ECC 1365 will support the Address Resolution Protocol (ARP ref 19) for mapping Internet addresses to Ethernet addresses and the Internet Control Message Protocol (ICMP ref 18) for error reporting. (Note: the ECC 1365 will also respond to "ping" requests). The UDP/IP implementation does not support Network Time Protocol (NTP), but may read correctly time stamped data as long as at least one VAX/VMS host exists on the network to act as NTP master.

4.2 Application Layer Protocols – Command Block Format

When the immediate response mode is used, all data required by the ECC 1365 to perform the requested operations (The command block and any required data) must be contained within one Ethernet frame and all data to be returned by the ECC 1365 must also fit within one Ethernet frame.

When the deferred response mode is used, data can be larger than one Ethernet frame.

The Ethernet frame is shown in Table 1.

Offset (bytes)	Length (bytes)	Contents
0	6	Destination Ethernet address
6	6	Source Ethernet address
12	2	MAC length field
14	1	LLC destination LSAP
15	1	LLC source LSAP
16	1	LLC control field
17	1	Padding byte (=0) or LLC3 status field
18	1	Padding byte (=0) or pseudo LLC3 control field
19	1	Padding byte (=0) or pseudo LLC3 status field
20	2	Frame type (=7)
22	2	Request number
24	2	CAMAC crate number
26	2	ECC host ID
28	4	Host PID
32	2	Host access ID
34	2	Flags
36	2	Status
38	n	Data area

Table 1 (ECP) Frame Format when carried by LLC

When true LLC3 procedures are being used, the pseudo LLC3 fields become padding bytes and are set to zero. When pseudo LLC3 procedures are being used, the LLC control field is set to “UI frame”, the first padding field is set to zero and the LLC3 control and status bytes are inserted in the pseudo LLC3 fields.

4.2.1 Command Block Format for ECP Frame Carried by UDP

When an Ethernet Command Protocol (ECP) frame is carried by UDP, the two Ethernet address fields and the MAC length field are omitted. The LLC3 command is provided as a “pseudo LLC3 “ frame as described in section 4.1.1Logical Link Control, Page 24.

Offset (bytes)	Length (bytes)	Contents
0	1	LLC destination LSAP
1	1	LLC source LSAP
2	1	LLC control field (set to ‘UI Frame’)
3	1	LLC status field (set to 0)
4	1	Pseudo LLC3 control field
5	1	Pseudo LLC3 status field
6	2	Frame type (=7)
8	2	Request number
10	2	CAMAC crate number
12	2	ECC host ID
14	4	Host PID
18	2	Host Access ID
20	2	Flags
22	2	Status
24	n	Data area

Table 2 ECP Frame format when carried by UDP

4.3 Data Segmentation

When several Ethernet frames are used to transfer user data for one Ethernet CAMAC Protocol (ECP) interaction (deferred response only), the data are considered to be a single stream split into several segments (one per Ethernet frame). These segments are delivered in sequence and can be concatenated to reconstitute the original data stream.

Several ECC 1365 commands can be invoked by a single ECP interaction. The methods for distinguishing the data associated with each command are described in outline below and in more detail in the descriptions of the individual commands.

4.4 Data to the ECC 1365

The data stream to the ECC 1365 consists of a sequence of one or more ECC command blocks. Each command block starts with a command code that is followed by any data required by that command. The length of the command-specific data can be inferred from the command code or can be calculated from a length or count field that follows the command code.

4.5 Data from the ECC 1365

The data stream from the ECC 1365 consists of a sequence of zeroes or one (or more) ECC data blocks. Each block corresponds to an ECC command that requests data from the ECC. Commands that do not request returned data do not generate an ECC data block.

An ECC 1365 data block can be further sub divided into data sections, where each section is preceded by a length field. This field is a 16-bit integer and its absolute value gives the number of 16-bit words that follow i.e. the length count does not include itself. If the length count is negative, this section is NOT the last one in the data block. If the length count is positive, this section IS the last one in the data block. Note that a length count of zero is allowed and it indicates that there are no data in this section but this is the end of the block.

The ECC 1365 and host systems handle the segmentation of the command block by queuing buffers and maintaining a set of pointers locally. It is required that the header fields are all contained within the first segment, so that only the parameter fields can span segments.

4.6 ECC 1365 Commands

Each ECC 1365 command block is formatted as shown in table 3. The command code can be followed by an optional, command-specific data. The ECC commands pre-defined by the ECC 1365 firmware are shown in table 4.

Command (binary)	Definition
1ccc cccc mmmm mmmm	ECC control command ccccccc – command code mmmmmmmm – command modifier
data	Zero or more 16-bit, command specific data words

Table 3 ECC 1365 Command Format

Command Code	Description	Modifier Contents
0	No Operation	
1	CAMAC Operation	COR Number
2	Set Maximum No-Interrupt Count	
3	Set Wait Timer	Wait time value in 10 msec units
4	Book Module	Station number
5	Unbook Module	Station number
6	Book Lam	Station number
7	Unbook Lam	Station number
8	Attach To Lam	Station number
9	Generate Dataway Initialise	
10	Generate Crate Clear	
11	Set / Clear Dataway Inhibit	1 if set, 0 if clear
12	Test Dataway Inhibit	
13	Enable /Disable Crate Demand	1 if enabled, 0 if disabled
14	Test Crate Demand Enabled	
15	Test Crate Demand Present	
16	Set LAM access mode	Mode value
17	Clear LAM	Station number
18	Test LAM	Station number
19	Inform host of LAM	Station number
20	Change security table entry	0-add, 1 -update, 2-delete
21	Read booking table	
22	Read timestamps	
23	Read statistics data	
24	Read trace buffer	
25	Load new ECC command	Command number
26	Load new COR	Routine number
27	Read security table	
28	Store host command block	Stored block number
29	Store system command block	Stored block number
30	Chain to stored host block	Stored block number
31	Chain to stored system block	Stored block number
32	Set /clear module promiscuous flag	Set/clear + Station number
33	Set /clear LAM promiscuous flag	Set/clear + Station number
34	Pre-allocate response buffer space	
35	Enable / disable module LAM	
36	Clear all entries in security table	
37	Attach COR to LAM	Station number

Table 4 ECC 1365 Control Commands

4.7 CAMAC Operation Routines

CAMAC operations are performed by a CAMAC Operation Routine (COR). The particular COR to be used is specified in the modifier field of the “CAMAC operation” ECC 1365 command. There can be up to 255 CORs, some of which are made available by the ECC 1365 software. CORs can also be downloaded from a host.

Each COR is capable of executing a particular CAMAC sequence, e.g. there is a COR for Q repeat operations. Several CORs might be available for the same CAMAC sequence; they differ in the type of optimisation applied to the sequence. For example, for Q-repeat there is a COR that enables CAMAC Look at ME (LAM) interrupts following a specified number of CAMAC operations. In addition, there is a COR that will not enable LAM interrupts until the whole Q-repeat sequence is complete.

Table 5 shows the format of the CAMAC operation command. The operation counter is a 32-bit integer which specifies how many CAMAC operations are to be performed. For a repeat operation, it specifies how many times a successful repeat is to be performed using the following single CAMAC operation. For general CAMAC operations, it specifies how many CAMAC operations follow.

Command List (binary)	Definition
1000 0001 cccc cccc	ECC CAMAC operation command cccc cccc specifies COR to be used
LLLL LLLL LLLL LLLL	Low 16-bits operation counter
HHHH HHHH HHHH HHHH	High 16-bits operation counter
0fff ffnn nnna aaas	CAMAC operation fffff CAMAC function code (5 bits) nnnnn CAMAC station number (5 bits) aaaa CAMAC subaddress (4 bits) s data size indicator s = ‘0’ – 16 bit data s = ‘1’- 24 bit data
xxxx xxxx xxxx xxxx	16 or 24 bits of data (see note) or further CAMAC operations as necessary

Table 5 CAMAC Operation Command

Note:

24-bit CAMAC data are placed in the 24 least-significant bits of a 32-bit data word. The 8 most-significant bits are ignored.

Table 6 shows the CORs that are available to the ECC 1365 software. The action of each COR is described in terms of the block transfer mode descriptors, defined in Reference 6. The counter “max-noint” is set by an ECC 1365 command and specifies how often interrupt shall be enabled by CORs that permit interrupts during their execution. When interrupts are enabled, the ECC attempts to transmit full response buffers back to the host.

The COR routines that do not permit interrupts execute faster but at the expense of interrupt latency. The requirements of a given application can be met by careful use of these routines, with the CORs that enable interrupts with max-noint set to a suitable value. The use of CORs with the delay wait timer (currently only COR 12) allows a slow poll of a module. A wait time of zero is permitted and this can be used to provide round-robin polling of several modules.

COR Number	Action
1	MCA mode. Q-responses are stored in the Q-response area. Interrupts are disabled for the whole operation.
2	MCA mode. As 1 but interrupts are checked every "max-noint" CAMAC operations.
3	ACA mode. Interrupts are disabled for the whole operation.
4	ACA mode. As 3 but interrupts are checked every "max-noint" CAMAC operations.
5	UCS mode. Interrupts are disabled for the whole operation.
6	UCS mode. As 5 but interrupts are checked every "max-noint" CAMAC operations.
7	UCW mode. Interrupts are disabled for the whole operation.
8	UCW mode. As 7 but interrupts are checked every "max-noint" CAMAC operations.
9	ULS mode.
10	UQC mode. Interrupts are disabled for the whole operation.
11	UQC mode. As 10 but interrupts are checked every "max-noint" CAMAC operations.
12	UQC mode. As 11 but after Q=0 response the next execution of the CAMAC operation is delayed by the wait time.

Table 6 CAMAC Operation Routines

4.8 Mapping ESONE / DOE Subroutines to Network Protocols

Tables 7, 8 & 9 show the mapping on the European Standards On Nuclear Equipment (ESONE) subroutines (known in the USA as DOE routines) into command blocks. When one of the ESONE / DOE block routines requires to wait for a LAM before starting execution, a command with code 8 (attach to LAM) is pre-pended to the command list. When short data-word CAMAC operations are required, the least significant bit of each CAMAC command is set to zero rather than one.

ESONE / DOE Subroutine	Command List
Perform single CAMAC operation	1000 0001 0000 0001 0000 0000 0000 0001 0000 0000 0000 0000 0fff ffnn nnna aaal

Table 7 Single Action Command Block

ESONE / DOE Subroutine	Command List	Notes
Generate Dataway Initialise	Generate Dataway Initialise	
Generate Crate Clear	Generate Crate Clear	
Set / Clear Dataway Inhibit	Set / Clear Dataway Inhibit	1
Test Dataway Inhibit	Test Dataway Inhibit	
Enable / Disable Crate Demand	Enable / Disable Crate Demand	2
Test Crate Demand Present	Test Crate Demand Present	
Clear LAM	Set LAM access mode Clear LAM	3
Test LAM	Set LAM access mode Test LAM	3
Link LAM to Service procedure	Set LAM access mode Inform host of LAM	3

Table 8 Mapping ESONE / DOE subroutines to ECC 1365 Commands

Notes:

1. Command modifier determines set or clear
2. Command modifier determines enable or disable.
3. The mode value is a copy of the LAM access specifier provided to the Declare LAM subroutine

ESONE / DOE Subroutines	Command List	Notes
General Multiple action	Set “max-noint” count = 50 1000 0001 0000 0010 Number of operations (low) Number of operations (high) 0fff ffnn nnna aaal Data if write 0fff ffnn nnna aaal Data if write …………….	
Address Scan	Set “max-noint” count = 50 1000 0001 0000 0100 0000 0000 0000 0010 0000 0000 0000 0000 0fff ffnn nnna aaal 0fff ffnn nnna aaal Data if write …………….	1
Controller-Synchronised Block Transfer	Set “max-noint” count = 50 1000 0001 0000 0110 Number of operations (low) Number of operations (high) 0fff ffnn nnna aaal Data if write ……………. Or	2
	Set “max-noint” count = 50 1000 0001 0000 1000 Number of operations (low) Number of operations (high) 0fff ffnn nnna aaal Data if write …………….	3
LAM-Synchronised Block Transfer	Set LAM Access mode 1000 0001 0000 1001 Number of operations (low) Number of operations (high) 0fff ffnn nnna aaal Data if write …………….	
Repeat Mode BlockTransfer	Set “max-noint” count = 50 0000 0001 0000 1011 Number of operations (low) Number of operations (high) 0fff ffnn nnna aaal Data if write …………….	

Table 9 Mapping ESONE / DOE Subroutines to ECC 1365 Commands Block Transfers and Multiple Actions

See notes overleaf

Notes

1. Provides station number and subaddress of the last CAMAC operation.
2. Stop mode.
3. Stop-on-word mode

4.9 Network Protocols

4.9.1 Find Address Protocol

The Find Address Protocol (FAP) enables a host to determine the Ethernet address of an ECC, given the number of the CAMAC crate controlled by that ECC. FAP is not available with UDP protocols.

If a host does not know the Ethernet address of an ECC 1365, it transmits a Find Address Request multicast frame. This frame contains the number of the CAMAC crate being sought. The host waits for 3 seconds, for a Find Address Response multicast frame containing that CAMAC crate number. If a response has not been received after 3 seconds, the request is re-transmitted but the number of retries is limited to three. When a response is received, the source address of the response frame is that of the sought ECC 1365. The FAP multicast frame format is given in Appendix A2, Table A2.2

When an ECC receives a Find Address Request multicast frame with its CAMAC crate number, it transmits a Find Address Response multicast frame with a copy of the CAMAC crate number.

As the Find Address Response frame is transmitted with a multicast address, it is potentially received by all hosts on the Ethernet. Any host receiving such a frame but which has not transmitted a Find Address Request, can use the information within the received frame to maintain a table of known crate and corresponding Ethernet addresses.

4.9.2 ECC 1365 Reset Protocol

The ECC Reset Protocol (ERP) can be used by a host to reset an ECC 1365. The function is not available to UDP hosts.

When a host wishes to reset an ECC 1365, it transmits an ERP request multicast frame (table) containing the CAMAC crate number of the ECC to be reset. The host waits for 60 seconds, for an ERP Response multicast frame or an ERP active multicast frame containing the appropriate CAMAC crate number. If a response has not been received after this time, the request is re-transmitted but the number of retries is limited to three. The ERP frame format is given in Appendix A2, Table A2.3.

When an ERP Response frame is received, the host canassume that the ECC is resetting and, when an ERP Active frame is received, the host can assume that the ECC has completed its reset procedure.

When an ECC 1365 receives an ERP request, it checks that the originating host is allowed to make that request. If permitted, it transmits an ERP Response and initiates a reset. If the host may not make the request, it is ignored.

As the ERP response frame is transmitted with a multicast address, it is potentially received by all hosts on the Ethernet. Any host receiving such a frame but which has not transmitted an ERP Request, can use the information within the received frame.

When an ECC 1365 encounters a fatal internal error, it attempts to transmit an unsolicited ERP response to inform hosts that it is resetti ng.

When an ECC 1365 completes its reset sequence, it transmits an ERP Active multicast frame to inform hosts that it is available. Note that the ERP Active frame is not sent until the Network Time Protocol (NTP) Listening state has been completed.

4.9.3 ECC 1365 Status Protocol

The status protocol returns various parameters from the ECC, such as queue length, free buffer counts, etc. These can be used for performance monitoring.

4.9.4 Ethernet Control Protocol

The Ethernet Control Protocol (ECP) is used for normal operation of the ECC 1365. It instructs the ECC to perform CAMAC operations, transfers CAMAC data and enables control over the use of the CAMAC modules controlled by the ECC. An overview description of ECPs is covered in Chapters 4.6 ,ECC 1365 Commands, Page 29 & 4.7 ,CAMAC Operation Routines, Page 30. The ECP frame format is given in Appendix A2, Table A2.4

CHAPTER 5

5 NETWORK TIME

The network time protocol (NTP) maintains a uniform time across the network, by all systems periodically generating NTP multicast frames. These frames contain a timestamp from the originator and an estimate of the transmission delay.

Note: UDP protocol hosts (UNIX) cannot issue NTP multicast frames so, therefore, cannot become network time masters. If networks contain at least one LLC protocol host (VMS) then normal network time service will be available to UDP hosts.

5.1 Theory

The NTP is based on the work of Lamport, see Reference 12. The aim is to ensure all ECC 1365 modules and all cooperating host processes on an Ethernet are synchronised with respect their record of time.

For any event, 'a' can be said to occur before 'b' if the clock value of 'a' is less than the clock of 'b'. Events 'a' and 'b' might be events within a process or could be transmission and receipt, respectively, of a message across a network. To guarantee that this system synchronises Network Time, two rules must be applied.

> Where 'a' and 'b' are events within a process, the clock for the process must be incremented between successive events.
>
> Where 'a' and 'b' are transmission and receipt, respectively, of a message, the message must contain a timestamp of the transmitter, and upon receipt, the receiver must advance its clock to at least the value of the timestamp.

In real time, there is some total delay between transmission and receipt but this delay is unknown to the receiver. However, it is possible to calculate the minimum delay in the system such that the minimum delay is greater than zero and it is less than or equal to the total delay.

A process sends a message with its clock value as the timestamp. On reception, the receiving process must set its clock equal to the maximum of its existing clock value or the timestamp value plus the minimum delay.

Following this simple procedure, the Network Time is synchronised for all co-operating processes attached to the network.

5.2 Practice

The working of the algorithm depends upon the successful estimation of the minimum transfer delay of a message between processes. The delay occurs in three places.

1. the transmission delay
2. the transit delay
3. the reception delay:

Of these, the transit delay on an Ethernet is usually insignificant. The other two depend on the functioning of the host system (the transmitter) and the ECC 1365 module (the receiver). The latter can be minimized and accurately estimated. The former is host dependent and extremely variable, depending on the processor and its loading. A separate program is provided which estimates this value. If the transit delay on the Ethernet becomes significant over an extended period of time (due to congestion or a fault condition), the accuracy of the network time across the total system decreases (due to inaccuracies in the individual clocks). The accuracy of the network time is, to a first order, equal to the transit delay being experienced.

5.3 Network Time Algorithm

This algorithm is executed on receipt of every NTP multicast. Network time is defined as the number of 10msec units since midnight, i.e. it provides a time-of –day clock.

Time, Tn is calculated as the sum of the timestamp value in the NTP multicast frame, the originator's estimate of its transmission delay and the receiver's estimate of its receipt delay. If the value of Tn is greater than the receiver's current estimate of network time, the receiver replaces its value of network time with Tn.

5.4 Network Time Protocol

All systems on the network generate NTP multicast frames every 10 seconds. Generated frames contain the originator's current value of the network time and an estimate of the transmission delay in the originating system. All systems –host(s) and Ethernet Crate Controller (ECC 1365) modules – receive these frames and run the Network Time algorithm, taking into account the minimum delay computed from the information provided in the frame. The NTP frame format is given in Appendix A2, Table A2.1.

If the Network time held locally is required to advance, this is done immediately, by modification to the Network Time Bias variable for host systems or directly, by altering the time-of-day count in the ECC 1365 modules.

NTP multicast frames also act as a heartbeat for all systems and the loss of six consecutive NTP multicast frames can cause the software to reset any reference to the particular system.

All systems enter a Listening state on start up, this enables them to synchronise their clocks before generating NTP frames. The listening time is 35 seconds. If no NTP multicasts are received during this period, a host system sets its value for the network time to its own time-of-day and commences sending NTP multicasts. An ECC 1365 module remains in the Listening state until it receives at least one NTP multicast.

CHAPTER 6

6 ETHERNET CAMAC CONTROLLER FIRMWARE DETAILS

The ECC 1365 CAMAC controller is designed to be driven from one or more hosts across an Ethernet local area network. An overview of the network protocols used and the software provided in the Ethernet Crate Controller (ECC 1365) and for host systems is described in Chapter 4,SYSTEM PROTOCOLS, Page 23.

This chapter gives a more detailed description of the firmware structure, its functions and processing priorities.

6.1 Priorities & Main Control Loop

The software in the ECC 1365 assigns event priority in the following order:

- The timer interrupt
- The QSPAN/82559 interrupt
- LAM interrupts.
- Received frames. Immediate response frames are actioned during LLC3 frame input processing
- Deferred response requests.

The requests contained in Logical Link Control (LLC1) frames are actioned within the QSPAN/82559 interrupt routines. Note that this includes the reset command and ensures that the ECC 1365 can be reset despite the presence of a permanent CAMAC LAM interrupt condition or runaway command execution:

Figure 8 illustrates these processing priorities and figures 9 & 10 show the flow of command lists through the ECC 1365 software.

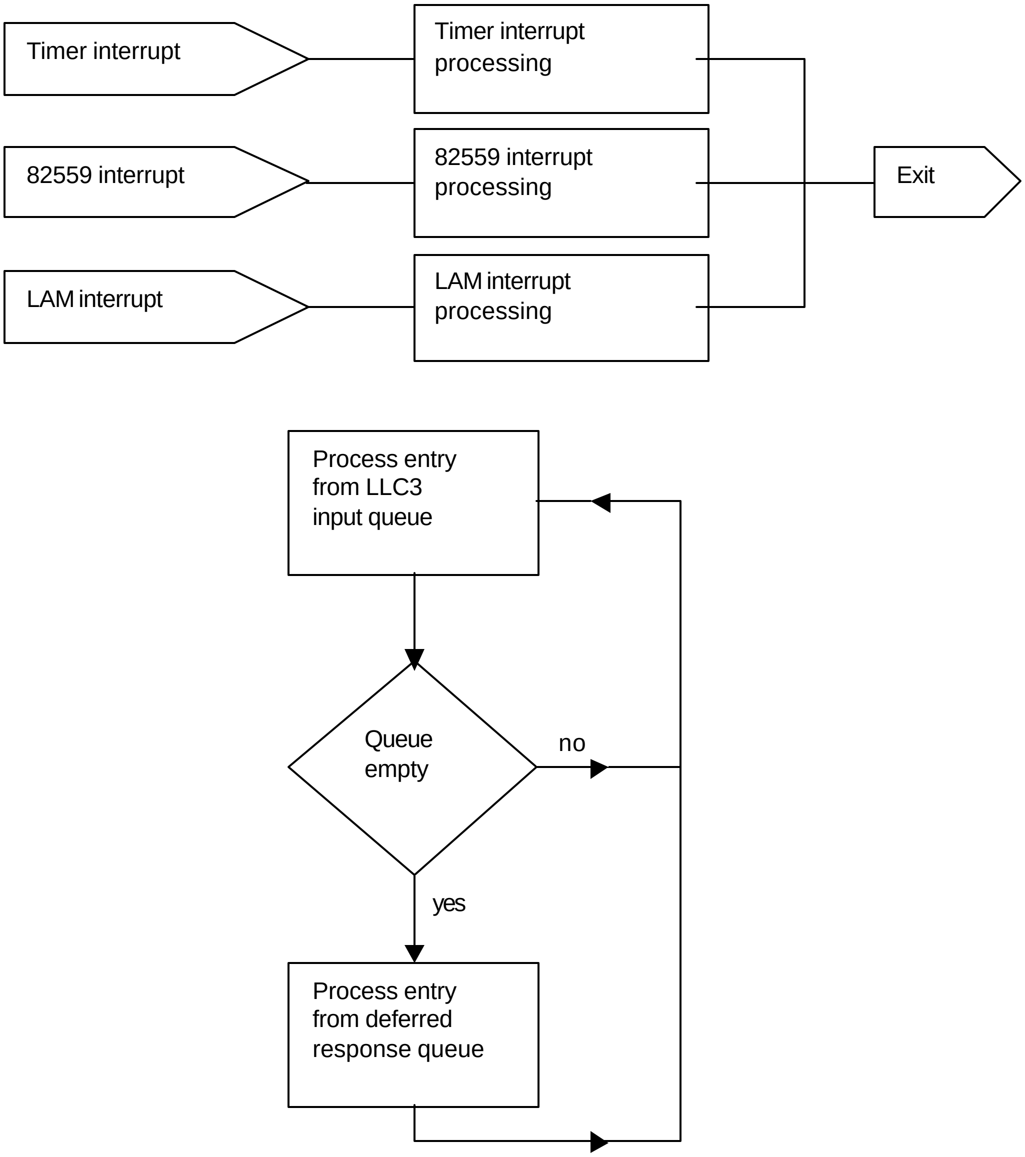

Timer interrupt
Timer interrupt processing
82559 interrupt
82559 interrupt processing
LAM interrupt
LAM interrupt processing
Exit
Process entry from LLC3 input queue
Queue empty
no
yes
Process entry from deferred response queue

Figure 8 Processing Priorities

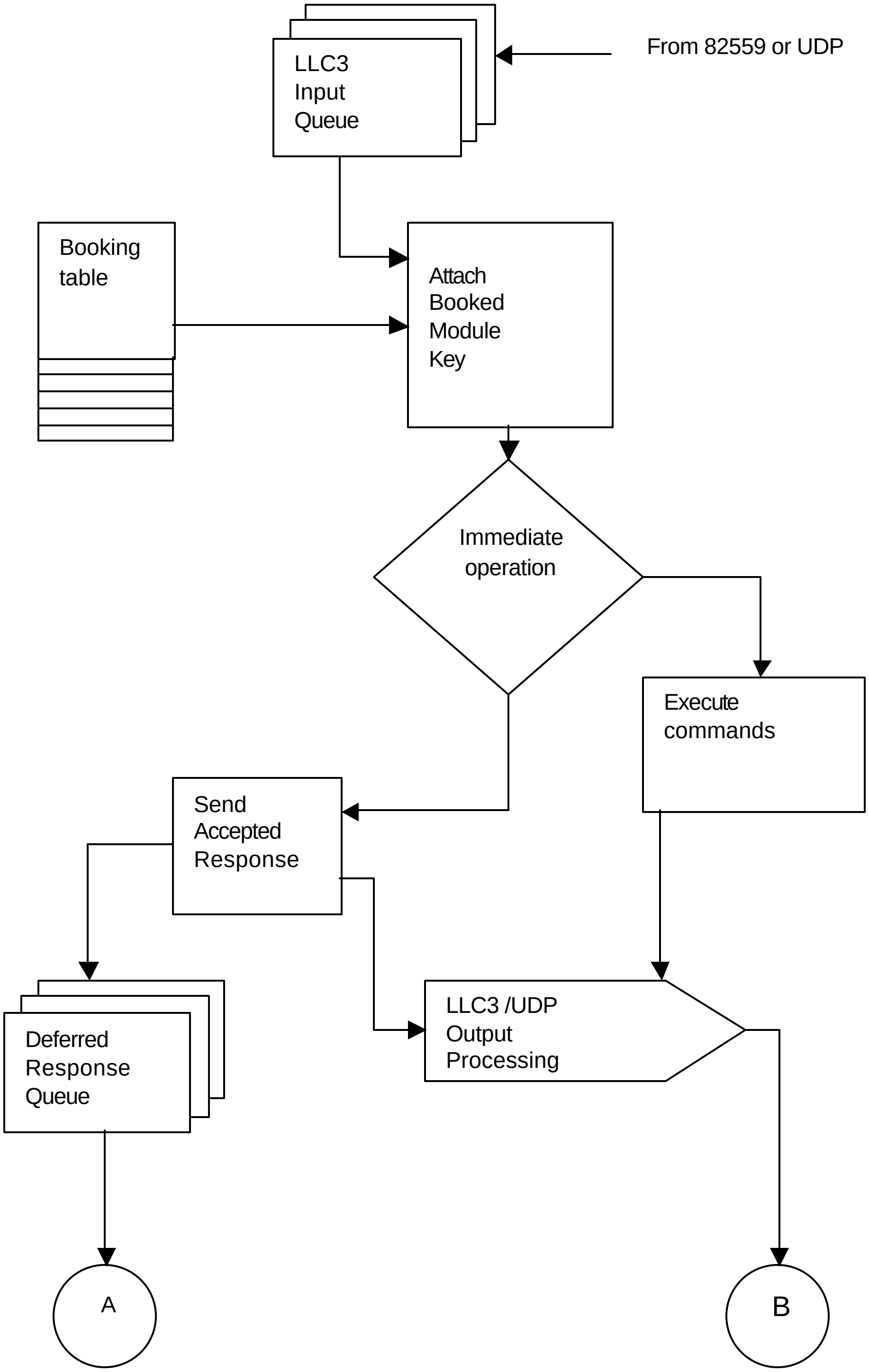


Figure 9 Command List Data Flow- Immediate Operations

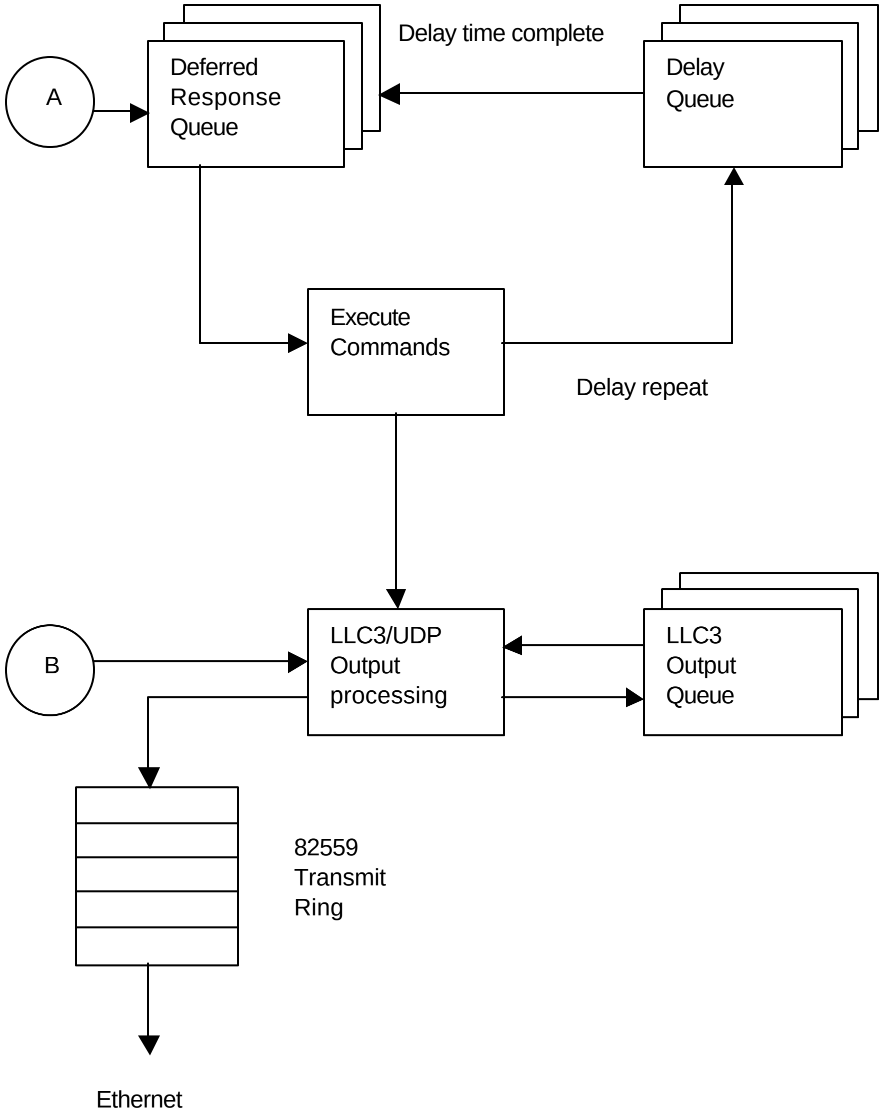


Figure 10 Command List Data Flow

6.2 Timer Interrupt Actions

The timer interrupt routine performs the following actions on each interrupt:

Increment the real time clock.

Cycle through the queue of command blocks for which a delay timer is in effect. For each one, decrement the timer and, if it is now zero, stop the timer and re-queue the associated command block on to the deferred response queue.

Cycle down a list of outstanding LLC3 transmit timers. When it finds one, decrement the timer, and if it is now zero, invoke the appropriate LLC3 error handler.

6.3 82559 Interrupt Actions

The action of the software when receiving an 82559 interrupt is shown in Figure 11.

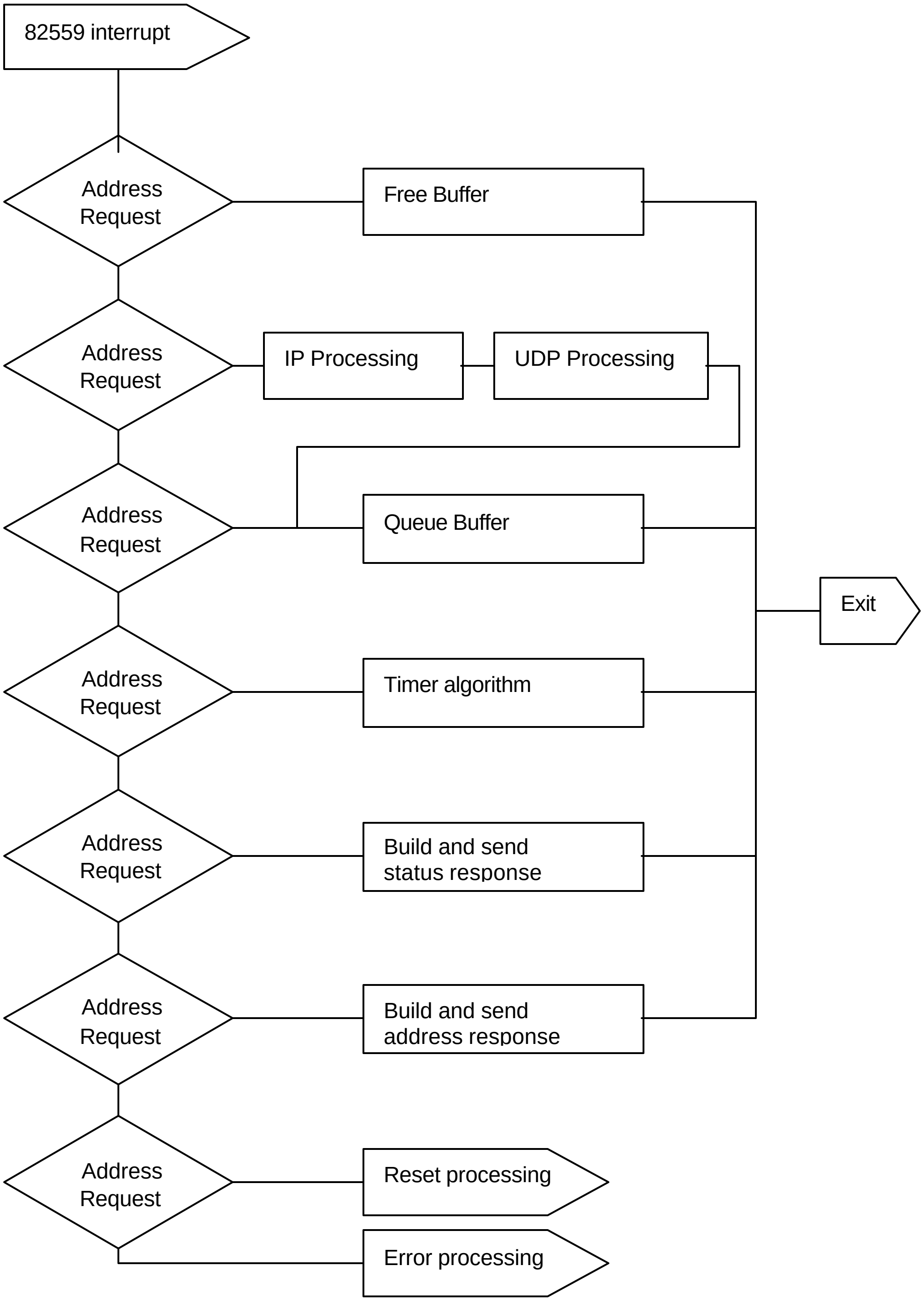


Figure 11 Command List Data Flow- Deferred Operations

6.4 LAM Interrupt Actions

The LAM interrupt handler checks the associated CAMAC module control block to determine the action to be taken. This action is one of:

Send notification of the LAM to a host

Restart execution of a LAM-synchronised CAMAC operation

Start execution of an attached command block

Record an unexpected LAM message in the trace buffer and

Disable the appropriate LAM mask bit

6.5 Module booking

The software in the ECC 1365 maintains a booking table. Each entry in the field contains two fields; a 48-bit Ethernet address and a 24-bit booked module mask.

The Ethernet address field is used when starting processing a command and it identifies the entry for the host. If no entry is found, a new one is created with a booked module mask of all zeros.

The booked module mask contains a record of all modules booked by the host, where a 1 in bit position 2^N indicates that the module in station number N is booked. The booked module mask is attached to the command block when processing the command begins.

Each CAMAC module has an associated control block that contains four fields of interest to the module booking software:

A 24-bit module identification field contains one single bit set in position in position 2^N and can be “bit-wise ANDed” with the booked module mask attached to the command block to see if this module is booked to the issuing host.

A flag field contains a ‘module booked bit’-used to indicate that the module has been booked, and a ‘module promiscuous bit’ – which indicates that the module can not be booked. The initial state of the module promiscuous bit is read from permanent RAM if this is enabled; otherwise, all modules are marked as non-promiscuous. The state of this bit can be altered by ECC command code 32 or the relevant ECCOP command.

A ‘booking host ID’ field contains a pointer to the relevant entry in the booking table.

A ‘booking PID field’ contains the PID of the booking process.

Modules may be booked by host Ethernet address alone or by host Ethernet address and Process ID. The PID booking mode is selected by switch SW1-2 on the side of the controller (on = enabled). Once selected, this mode cannot be changed without switching the controller off and resetting the switch.

Note: Unix users should be wary of the PID mode being enabled.

If PID booking is enabled by the switch and an initialisation [!INIT] command is performed, auto module booking is disabled.

An auto-booking scheme may b e enabled by the appropriate ECC command code or the relevant ECCOP command. If enabled, the auto-booking is invoked during command block processing whenever a module is referenced which is; not booked to the host, is not promiscuous and is not booked to a ny other host (or PID if PID booking enabled). There is no corresponding auto-unbooking mechanism and all modules must be unbooked explicitly. Notification of host reset (whether caused by network or host failure) un-books all modules booked to that host. Dataway Clear and Dataway Initialise do not un-book modules.

The ECCOP routine CLRBOOK will clear all booking on all modules; this routine can be protected against by using “clear booking table allowed” flag in the security tables.

6.6 LAM Booking

The software in the ECC 1365 operates a LAM booking scheme. This scheme allows a LAM from a CAMAC module to be booked to a specific host or PID. Once a LAM is booked, the host can specify what is to be done on receipt of a LAM from the module (see also Chapter 6.4 ,LAM Interrupt Actions , Page44). Operation of the booking procedures is similar to that for module booking, including auto-booking and promiscuous operation– Command Codes 6,7,8 & 33 (see Chapter 6.5 ,Module booking, Page 44)

Note that booking a LAM requires that the host or PID has already booked the corresponding module.

6.7 Operating Statistics

The ECC 1365 software maintains a table of statistics that can be read by host systems (Command Code 23) or displayed by a terminal connected to the ECC 1365 front panel port. These statistics provide cumulative counts of the number of times that selected conditions are encountered in the ECC. The content of the statistics table is shown in Table 10

Major Topic	Counter	Bit Length
82559	Packets transmitted successfully	32
	Packets having to defer on transmit	32
	Number of excessive collisions	32
	Number of illegal collisions	32
	Number of excessive deferrals	32
	Number of bad packets monitored	32
	Packets received successfully	32
	Number of receive FIFO overruns	32
	Number of receive buffer overflows	32
	Number of receive descriptor exhausted	32
	Number of receive buffer exhausted	32
	Number of collisions during reception	32
	Number of heartbeat failures	32
	Number of missed packets	32
	Number of CRC errors	32
	Number of frame alignment errors	32
Module counters	Number of LAMs	32
(one block per module)	Number of unexpected LAMs	32
	Number of double booking attempts	32
	Number of security violations	32
	Number of Dataway timeouts	32
Memory allocation	Kbytes currently allocated	16
	Maximum Kbytes allocated	16
Command block counters	Number available	16
	Number currently allocated	16
Host table entry counters	Number available	16
	Number currently allocated	16
	Maximum number allocated	16
Security table entry	Number available	16
counters	Number currently allocated	16
	Maximum number allocated	16
Crash table entries	Up time to crash in seconds	32
(5 copies, see note)	Crash code	16
Current up time	Time since last restart in seconds	32
Download memory	Size available in bytes	32
	Current usage in bytes	32

Note: The crash table entries are time-ordered, with the last entry corresponding to the most recent crash. Unused entries have a crash code of SUCCESS

Table 10 Statistics Table Format

6.8 Tracing

The ECC 1365 software records significant events (mostly errors) in a circular trace buffer. The trace buffer is 1 Kbyte and maintains a record of the last 64 events. The format of a trace table entry is shown in table 11.

Field	Length (bytes)
Timestamp	4
Event code	2
Host Ethernet address	6
Module number	1
Interrupt level	1
Event-related data	2

Table 11 Table Trace Entry Form

Trace Table data can be read by a host (Command code 24).

6.9 Downloading New Software

It is possible for a host to load new software into the ECC 1365 (Command codes 25 & 26). This software can replace an existing ECC command (or CAMAC operation routine – COR) or it may add a new ECC command (or COR) by using an unused command code or routine number. An area of ECC memory can be reserved for downloaded code; when this area is full, further download requests will fail. The ECC must bereset to recover the space in the reserved memory.

A COR routine can be attached directly to a LAM so that when the LAM is present, the routine is invoked. This allows downloaded code to handle LAMs.

A separate manual, entitled 'Downloading Software' describes this facility in more detail and is normally shipped as part of the distribution.

6.10 Initialisation

Switches on the ECC 1365 are read to determine the initial operating parameters of the ECC 1365 software. These switches are used as follows:

The front panel Normal Mode / Diagnostic Mode switch determines whether the ECC enters normal operating mode or diagnostic mode.

Jumper JP4 enables or disables the use of a security table. In the disabled state, the software defaults to no security features applied.

Four switches (5 to 8 on SW5) are used to specify the LSAP address pair to be used.

Details of these switch settings are in Chapter 8.1.6,Configuring the Links & Switches, Page 73

6.11 The Tick Timer

A 10 msec tick timer is implemented by one of the timers in the hardware. This is used to maintain a time-of-day counter “cur-time” (in 10 msec units) and a time-since-last-restart counter “up_time” (in seconds).

6.12 Time Tagging

The time when a command was received by the ECC 1365, the time when its execution commenced and the time when its execution completed are recorded by the module firmware. A data block containing these times for the most recently executed command can be read by a host on request (command 22)

6.13 The Clock System

Since the time taken for the “Set time” message to be formed, transmitted by the host, received and decoded by the controller and acted upon is indeterminate, the relationship between Controller Time and Real Time is always in error up to 0.2 seconds either way.

The “Read Time” message is used to estimate the transmission delay of the message and determine the error, if any, in the time held by the controller. The “Read Time” and “Set Time” processes operate IN ADDITION to the NTP scheme that “trims” the RTC on each device.

In applications where very precise time tagging is required, a separate CAMAC Real Time Clock module should be used, accessed by the host in the course of data collection.

6.14 The Crash Table

The firmware maintains a circular crash table in the battery-backed RAM, which contains the reason for the last five system crashes together with the value of the “time up” variable at the time of the crash. The index number at the start of the crash table indicates the next table entry to be written.

The error codes are shown in the table overleaf.

Value	Name	Description
0	FAILURE OR FAIL	General Failure
1	SUCCESS	Function Performed Successfully
2	QWASCLR	Queue Was Empty
3	ERP_ACCEPTED	ERP Request Accepted
4	NOBUFS	Not Enough Buffers On Queue To Satisfy Request
6	NO_CMND_BLOCKS	No Command Blocks Left
8	BAD_PARAM	Error Found When Encoding/Decoding A Parameter
10	BAD_SEG	Bad Segment Request
12	PROMISCUOUS	Booking Request Failed, The Module/LAM Is Promiscuous
13	UPDATE_PROM	Trace Table Entry Only, Promiscuous Flag Updated
20	BAD_CMND	Error Decoding ECC Command Or Undef. ECC Command
22	DUP_CRATE	Duplicate CAMAC Crate Number Seen On Ethernet
24	ERP_REQUEST	Reset Request By ERP
26	HOST_FULL	Host Table Full
28	FAIL_SECURITY	Host Request Failed Security Checks
30	LAM_ATTACHED	LAM Already Attached
32	MOD_BOOKED	Module Booked To Another Host
34	TRAP_68901	Bad 68901 Interrupt
36	TRAP_POWER	Power Fail Interrupt
38	TRAP_BUS	Bus Error Interrupt
40	TRAP_ADDRESS	Address Error Interrupt
42	TRAP_ILLEGAL	Illegal Instruction Interrupt
44	TRAP_DIVIDE	Zero Divide Interrupt
46	TRAP_CHK	CHK Instruction Interrupt
48	TRAP_TRAPV	TRAPV Instruction Interrupt
50	TRAP_PRIV	Privileged Instruction Interrupt
52	TRAP_TRACE	Trace Interrupt
54	TRAP_BAD	General Bad Interrupt
56	TRAP_TRAP	TRAP Instruction Interrupt
58	MEMORY_ERROR	Failed RAM Diagnostics
60	SEC_BADREQ	Bad Change Security Table Entry Request
62	SEC_FULL	Security Table Full
64	NO_SBLOCK	No Stored Command Block To Supply To
66	BAD_COR	Non Existent CAMAC Operation Routine Requested
68	USER_RESET	User Has Requested A Reset
70	DIAG_9519	Failed AMD9519 (UIC) Diagnostics
72	NO_DTM4	No DTM4 Module Has Been Defined For Test
74	DIAG_CAMAC	Failed CAMAC Diagnostics
76	INV_IMMEDIATE	Command Invalid In Immediate Response Request
78	BAD_CAMAC	Bad CAMAC Operation Requested
80	DOWNLOAD_LOCK	Download Already In Progress
82	DOWNLOAD_DATA	Error In The Download Data
84	DOWNLOAD_FULL	Not Enough Memory For Download Data
86	NO_MEMORY	Not Enough Memory For Getmem() Request
90	CAMAC_NOTX	Not X During CAMAC Operation. Note: Warning Only
92	CAMAC_NOTQ	Not Q During CAMAC Operation.
94	CAMAC_NOTQX	No Q Or X During CAMAC Operation.
96	IPTIMER_LOOP	Loop In IP Timer Queue
98	PUSHDOWN_FAIL	Buffer too small for pushdown
100	MOD_BOOKED_PID	Module booked to another PID
102	BAD_VERSION	Firmware / host software version mismatch
104	DIAG_82559	Failed 82559 diagnostics
110	82559_TXERR	82559 hard TX error
112	TRAP_1101	Line 1101 exception interrupt
114	TRAP_1111	Line 1111 exception interrupt
118	REG_82559	Unable to read / write 82559 registers

Table 12 ECC 1365 MK 4 Firmware Error Codes (Crash Codes).

6.15 Command Processing

The command block in a received frame is decoded and executed within module “cmndexec.c”

A 128-element lookup table is used to determine the ECC 1365 command routine to be executed.

The lookup table is set during ECC initialisation, to point to routines to execute the pre-defined ECC commands shown in table 3. Undefined entries in the lookup table are initialised to point to an error routine.

6.16 COR Processing

CAMAC operations requested by the “CAMAC operation” ECC 1365 command are handled by module “cor.c” (Command Code 1).

A 256-element lookup table is used to determine the CAMAC operation to be executed.

The lookup table is set during ECC initialisation, to point to routines to execute the pre-defined CORs shown in Table 5. Undefined entries in the lookup table are initialised to point to an error routine.

6.17 Security Processing

A set of routines for handling the security table are present in module “security.c”. The security state of the ECC 1365 is maintained in the global variable “security_state”. If this variable is zero, the ECC is unsecure. If this variable is non-zero, the ECC is secure and the variable value indicates the number of active entries in the security table. The check and link routines can be called independently of the current security state, see also Chapter 9,SECURITY FEATURES, Page 83.

The security table can be read by all hosts (Command code 27) and can be changed by permitted hosts (Command Code 20)

NOTE: as a precaution against locking out access to an ECC 1365 by entering an erroneous Ethernet address, when the entry is the first entry, (making a first entry changes controller state from OPEN to SECURITY CHECK) a consistency check is carried out by the ECC 1365 firmware. The very first security table update from a remote host must specify an Ethernet address equal to the source address in the Ethernet frame and it will be forced to have security table update enabled for it.

6.18 Power Fail

The ECC 1365 MK 4 contains a CAMAC power-fail monitor. The power-fail monitor detects a sharp drop in the incoming +6 volt rail and interrupts the processor through NMI (non maskable interrupt) when this happens giving rise to Crash Code 36 and reports to all known hosts where possible.

6.19 Error Codes

A common set of error codes is used within the firmware. These are defined in module “structs.h” and are reproduced in Table 12. Some of these codes are internal to the software and some can be observed at the user level, e.g. in a system crash table entry.

CHAPTER 7

7 ECC 1365 FRONT PANEL DIAGNOSTICS TERMINAL SUPPORT

This section describes the command interface to the ECC 1365 firmware, available through the front-panel RS232 connector. It defines the commands available and the output from those commands.

7.1 Overview

A simple command interface is available to a terminal connected to the front-panel RS232 connector of the ECC 1365 module, see Chapter 8.1.5,Connecting the Front Panel RS232 Port to a terminal, Page73. The commands are divided into three groups:

The first group contains the commands available for normal operation of the system.

The second group contains commands for configuration of the module.

The third group contains diagnostic commands.

The operating mode of the system determines which commands are available:

Normal mode makes available only normal commands.

Battery-backed RAM mode makes available the normal commands plus command for setting the module configuration.

Diagnostic mode makes available the normal commands plus diagnostic commands. Note that the diagnostic command $RUN is available only if the front panel switch is in the diagnostic position at power up. Exit from this special startup mode is via a diagnostic command but there is no entry to th is special state from an operating system.

Note that whenever an error is made at the keyboard, e.g. the wrong command or a keying error, the response is always:

```
Bad command
```

Only in some instances will an explanation be given.

If a typing error is noticed immediately, use the Back Space key to move the cursor to the left and then overtype.

The last five commands can be recalled by use of the VT200/VT300 terminal up-arrow key (similar to the VM5/DCL method). For terminals without arrow keys, Ctrl/r can be used.

The available commands are shown in Table 13.

Command	Action
Normal Mode	
DISPLAY SECURITY	Displays entrie s from the security table
DISPLAY DTM4	Displays the CAMAC station number of a DTM4 module
DISPLAY STATISTICS	Displays the contents of the statistics table
DISPLAY ADDRESS	Displays the modules addresses
DISPLAY CRASH	Displays the contents of the crash table
DISPLAY MODE	Displays the current operating mode
DISPLAY ARP	Displays ARP protocol details
DISPLAY AUTO	Displays the current booking methods
DISPLAY NL	Displays station numbers of the N/L line test modules
CHANGE SECURITY	Change entries in the security table
CHANGE DTM4	Changes the CAMAC station number of a DTM4 module
CHANGE MODE	Changes the operating mode
CHANGE PR2401	Change station number of PR2401 module (N line test)
CHANGE OD2407	Change station number of OD2407 module (L line test)
RESET	Resets the module and restarts the firmware
CLRBOOK	Clear all booking entries from the controller
CAMAC N A F [DATA]	Performs the specified CAMAC operation
HELP	Displays a list of available commands
Battery-backed RAM Mode	
!INIT	Initialises the contents of the battery-backed RAM
!EPA	Sets the module’s Ethernet physical address
!EMA	Sets the module’s Ethernet multicast address
!CLRSEC	Clears all entries in the security table
!DLMEM	Specifies the size of the download memory region
!IPA	Sets module IP address
!IPS	Sets module “well known” socket number
!AUTO	Enables or disables autobooking
Diagnostic mode	
$DM	Displays a block of memory
$DL	Displays a longword of memory
$DW	Displays a word of memory
$DB	Displays a byte of memory
$CL	Changes a longword of memory
$CW	Changes a word in memory
$CB	Changes a byte in memory
$DMOD	Displays a module control block
$DHOSTI	Displays a host control block
$DHOSTE	Displays a host control block
$RUN	Runs a diagnostic routine
$NORMAL	Exits the special diagnostic startup mode
$CAMAC n a f [data] [+]	Loop on the specified CAMAC routine

Table 13 ECC 1365 Front Panel Terminal Commands

This list is displayed whenever ‘help’ is typed (upper or lower case). The list is presented in four sections, the first three stopping with the message:

```
--more–
```

The next section is then shown when <Return> is pressed. The help list can be aborted by pressing Ctrl-C at any time.

Abbreviations are allowed for some of the commands, as shown below.

Command Word	Abbreviation
DISPLAY	D
CHANGE	C
STATISTICS	STATS

Table 14 Command Word Abbreviations

Command details are given below.

Some commands cause the firmware to ask further questions, to define the operation to be performed. If a default answer is relevant, it is shown in square brackets after the question,
`e.g. [U(pdate)] or [D(elete)?]`

Enter <Return> to accept the default displayed.

7.1.1 Trap Details

When the 68060 processor generates an unusual trap condition (e.g. Bus error) the firmware will attempt to display diagnostic information on the terminal screen before completing crash/restart processing. This information will include the contents of the 68060 registers at the trap and the top of the stack (at the very top of the stack will be the 68060 exception frame).

7.2 Normal Mode Commands

7.2.1 Display Security

Enter either a 12-digit (hexadecimal) Ethernet or an n.n.n.n style Internet Protocol address. Alternatively press<return> to see a list of all entries in the table. If there are no entries, the message:

‘Security Table empty’ is displayed.

If a known Ethernet address is entered, a display is generated. A typical one is shown below

```
Address              SU Z  C  I  DL PR  E  ST          Module mask
                                                                 111111111122222
                                                       123456789012345678901234

EEEE 0000 0000       X  .  .  X  X  .   X  X           XXXXX.....XXXXXXXXXXXXXX

Completed OK
```

Note: an ‘X’ denotes a bit set and a ‘.’ denotes a bit clear.

7.2.2 Display DTM4

DTM4 is the Hytec CAMAC Dataway Test Module, type 4 –used for diagnostic tests.

The command displays:

```
DTM4 is in station 2
```

7.2.3 Display Statistics

The firmware displays the statistics shown in Table 15. The output is paginated; press <return> to see the next page or <Ctrl-C> to stop.

The statistics listing is initiated by the command;

display statistics

or

d stats

and a typical printout would be:

Table 15 ECC 1365 Statistics Printout

82559 Statistics

```
Packets transmitted successfully              133
Packets having to defer on transmit           2
Number of excessive collisions                0
Number of max collisions                      0
Number of normal collisions                   0
Number of transmit under-runs                 0

Packets received successfully                 191
Number of receive overruns                    0
Number of receive resource errors             0
Number of Frame Alignment errors              0
Number of CRC errors                          0

Individual address register 1-6  0 80 3 14 3 9
```

IP statistics

```
Total 0 runt 0 len err 0 vers err 0 checksum err 0 badproto 0
```

ICMP statistics

```
Chksum err 0 no space 0 icmp 0 bdsts 0
Type   rcvd   sent
```

UDP statistics

```
Sent 0 rcvd 0 bdcsts 0 chksum err 0 unknown socket 0
```

General statistics

```
Current up time  54:00
Missed timer interrupts   0
       (corrected for)
```

Memory Statistics

```
Heap pool size                          1940800 bytes
Memory currently allocated                50816 bytes in 33 blocks
Allocation high water mark                50816 bytes in 35 blocks
Current average block size                 1588 bytes

Number command control blocks                 50
Number currently allocated                    0
Allocation high water mark                    0

Number of host control blocks                 30
Number currently allocated                    0
Allocation high water mark                    0

Number of security table entries              150
Number currently allocated                    0
Allocation high water mark                    0

Download memory size (bytes)                  00000000
Current allocation (bytes)                    00000000
```

CAMAC Module statistics

```
Station       Good          Unexpected    Booking       Security      Dataway
              LAMs          LAMs          failures      violations    timeouts
1             0             0             0             0             0
2             0             0             0             0             0
3             0             0             0             0             0
4             0             0             0             0             0
5             0             0             0             0             0
6             0             0             0             0             0
7             0             0             0             0             0
8             0             0             0             0             0
9             0             0             0             0             0
10            0             0             0             0             0
11            0             0             0             0             0
12            0             0             0             0             0

Enter <RETURN> to continue, <CTRL-C> to stop press <return>

Station       Good          Unexpected    Booking       Security      Dataway
              LAMs          LAMs          failures      violations    timeouts
13            0             0             0             0             0
14            0             0             0             0             0
15            0             0             0             0             0
16            0             0             0             0             0
17            0             0             0             0             0
18            0             0             0             0             0
19            0             0             0             0             0
20            0             0             0             0             0
21            0             0             0             0             0
21            0             0             0             0             0
22            0             0             0             0             0
23            0             0             0             0             0
24            0             0             0             0             0
```

7.2.4 Display Address

Typing this command causes the following display;

```
CAMAC crate number                  1
Controller Ethernet address         0080 0314 0302
Multicast Ethernet address          0180 0300 0000
Host LSAP                           60
Controller LSAP                     64
Controller IP address               192.10.4.0
Controller Socket                   240
```

7.2.5 Display Crash

The firmware displays information for up to the last five firmware crashes. For each crash, the reason code for that crash is displayed along with the previous uptime of the firmware (in seconds). For example:

```
D crash


 ------Restart History------
uptime 2:10:48 restart code 68
uptime 1:06:21 restart code 31
uptime 3:28:19 restart code 25
```

7.2.6 Display Mode

The current operating mode of the module is shown:

```
Current mode is – normal
```

7.2.7 Display ARP

The firmware displays the Address Resolution Protocol (ARP) operating statistics and the current contents of the ARP table, for example:

```
D ARP

Received 0 badtype 0 badlen 0 bogus addr 0 reqst in 0 replies 0 regst out 0
```

Type   IP addr Time Q addr

7.2.8 Display Auto

This command displays the current state of auto-booking and the booking type whether it be host only or host and PID.

A typical display shows:

```
Auto booking is currently enabled
```

The booking is by host_id and PID

7.2.9 Change Security

The display shows:

```
Enter Ethernet address or IP address:
```

Enter either a 12-digit (hexadecimal) Ethernet address as 3 groups of 4 digits, i.e. C0C0 0000 0000, or as a decimal format IP address (e.g. 192.1.2.3).

The display might show:

```
No space for new entry
```

If no table space is available to add a new address (max.150).

If a table entry already exists, the question:

```
U(pdate) or D(elete)?[U]
```

Is displayed.
Enter "U" to update the entry or "D" to delete it. If the entry is not to be deleted, several questions are asked to determine the contents of the table entry.

When updating an existing entry, the default values shown reflect the existing value and the display is:

```
Enter a 24-bit mask with not-blank and not-dot giving access to module

         111111111122222
123456789012345678901234
……………………………………..
```

The dots indicate that access is not allowed to the module at the indicated CAMAC station for that host address. The 24 numbers shown correspond to the CAMAC Station numbers (read vertically)

Enter a mask pattern. To do this, enter any character (except a blank or a dot) to permit access to chosen modules, e.g.

```
11111   11111111111111
```

This allows access to all modules, except station numbers 6 to 10 inclusive, for that address.

When <Return> has concluded the above selection, the following messages are displayed in turn– each waits for a response, which can be acceptance of the offered default or the entry of another option.

Note that responses must be made in UPPER CASE

```
Security table update allowed: Y(es),N(o):
Crate Initialise allowed: Y(es),N(o):
Crate Clear allowed: Y(es),N(o):
Set/Clear Dataway Inhibit allowed: Y(es),N(o):
Download new command or COR allowed: Y(es),N(o):
Alter module/LAM promiscuous flag allowed: Y(es),N(o):
ECC reset allowed: Y(es),N(o):
Store system command block allowed: Y(es),N(o):
Enable /disable autobooking allowed: Y(es),N(o):
Clear all booking entries allowed: Y(es),N(o):
Completed OK
```

Follow this sequence for all host addresses to be set up. Upon completion, run 'display security'.

WARNING:

Extreme caution should be taken when entering security data. If the security table was previously empty (module was OPEN), you must ensure that the host address you enter is correct for the host you are entering data for. Otherwise, all access to the module is prohibited until the error is corrected or the security table disabled. Correctly entered Ethernet or IP addresses for existing hosts do not cause a problem.

7.2.10 Change DTM4 [n]

Typing this command causes the message:

```
Enter (decimal) station number of DTM4 module (0=none) [0]:
```

To be displayed. The new station number then entered can be checked by using the display dtm4 command.

7.2.11 Change MODE [n]

When the command:

```
change mode
```

Is typed, the message:

```
WARNING- setting mode non-zero allows operations which may make the
controller function incorrectly. If in doubt, issue a RESET command.

Enter mode -        0(normal)
                    1(B-RAM setup)
                    2(Diagnostic)
                    3(B-RAM + Diagnostic)[2]:
```

is displayed. This warns that damage might result from misuse of commands not available in normal mode.

The firmware then asks for the new mode to be entered. Type the required mode number, when the response is:

```
Change complete.
```

7.2.12 Reset

Using this command causes the message:

```
WARNING – Reset will destroy all current controller operations and all
settings will be re-read from the switches and the battery-backed RAM.

Are you sure you wish to continue [no]:
```

If ‘yes’ is returned, the following message will be displayed.:

```
SYSTEM CRASH – Code 68 *************

       HYTEC ELECTRONICS Ltd. ETHERNET CRATE CONTROLLER ECC1365 MK IV

Serial number 769
Firmware version 8.0 (Sept 2000)
1988 Kbytes memory installed
Co-processor not fitted
Main initialisation complete

-----------Restart History-------------

Uptime 2:10:48, restart code 68

Starting QSPAN diagnostics
PCI Ethernet initialised OK
I82559 diagnostics complete – start normal operation

I82559 Autonegotiation complete 100Mbit Half Duplex
```

7.2.13 HELP

The firmware displays the available commands together with a short description of their purpose. The output is paginated; press <Return> to see the next page or <Ctrl-C> to stop. Sample output is shown in table13.

7.2.14 CAMAC

This command executes a single CAMAC command in the crate. The format is:-

CAMAC N A F [data]

Where: -

N	=	CAMAC station number in range 0..24
A	=	CAMAC sub-address in range 0..15
F	=	CAMAC Function Code in range 0..34

If the Function Code is a write (range 16-23), then the data argument must be supplied:-

Data = CAMAC data in decimal

The CAMAC command responds with:-

```
       CAMAC operation Fn Am at station p
```

Where n, m and p are N A F respectively.

If the Function Code was a read (0-7) then the read data is displayed:-

```
Data = xxx (decimal) yyy (hex).
```

The Q and X responses are always shown thus: -

```
       X – response =0      Q – response =0
```

Where response can be either 0 or 1 for false and true respectively.

7.3 Battery-backed RAM Mode Commands

If the firmware is not operating in battery-backed RAM mode, the following message is displayed and the command is ignored.

```
                          Not in Battery-backed RAM setup mode
```

7.3.1 !INIT

Typing this command causes the message:

```
WARNING- This command will destroy all data in the battery-backed RAM
```

```
Are you sure you wish to continue [no]:
```

If the answer is “yes”, the battery-backed RAM is initialised to the following state:

The crash table is emptied.

The Ethernet physical and multicast addresses are set up from the data in the internal EPROM

The security table is emptied

The statistics data are cleared

Note: If the battery-backed RAM becomes corrupted, due to battery discharge, this command MUST be issued before normal operation is possible.

7.3.2 !AUTO

Typing this command causes the message:

```
WARNING – Enabling and disabling the autobook function should only be
performed if all current users are made aware of the change to the
controller.

Enter –0(Autobook disabled)
        1(Autobook enabled)
```

7.3.3 !EPA[n]

Set up the Ethernet Physical Address.

Syntax: !EPA xxxx xxxx xxxx

Where xxxx is a 4-digit hexadecimal number. The three numbers are the Ethernet Physical address. The second digit of the first set of four must be even for a physical address.

If an error is made, the message:

```
Bad input –3 4-digit hex numbers required
```

Is shown. For example;

```
!EPA C0C0 0000 0001
```

This command allows you to set up a physical address different to the one stored in the internal EPROM, if desired.

7.3.4 !EMA [n]

Set up th e Ethernet Multicast Address.

Syntax: !EMA xxxx xxxx xxxx

Where xxxx is a 4-digit hexadecimal number. The three sets of four digits provide the Ethernet Multicast address. The second digit of the first set of four must be odd for a multicast address.

The broadcast address of FFFF FFFF FFFF is not allowed. Example;

```
!EMA 8500 0000 0000
```

This command allows you to set up a multicast address different to the one stored in the internal EPROM, if desired.

7.3.5 !CLRSEC

Clear the security table

Syntax: !CLRSEC

The command issues a warning message explaining that all the data in the security table are lost if execution is continued.

Enter “Yes” to proceed, any other response is taken as no. *Note: you must enter the full word ‘yes’ for this command to operate.*

7.3.6 !DLMEM

Declare downline load memory region, in bytes.

Syntax: !IDLMEM xxxxxxxx

Where xxxxxxxx is a hexadecimal number specifying the number of bytes to allocate to the download memory region after the next ECC restart. The value is stored in the battery-backed RAM.

If an odd number of bytes is specified, the message:

```
Even length in hex required
```

Is shown.

If too much memory is specified, the message:

```
Can’t allocate more than ½ free memory to download region
```

is given. The rest of the memory is required for system buffers.

7.3.7 !IPA[n]

Syntax: !IPA nnn.nnn.nnn.nnn

where nnn.nnn.nnn.nnn is the decimal form of the module's IP address. The value will be stored in the battery-backed RAM. See Chapter 8.2.4,Setting Up The Internet Protocol And Socket ID Addresses., Page 78 for details of IP addresses.

7.3.8 !IPS[n]

Syntax: !IPS nnn

where nnn is the decimal number specifying the module's "well known" socket number. The value will be stored in the battery-backed RAM. See Chapter 8.2.4,Setting Up The Internet Protocol And Socket ID Addresses., Page 81 for details of socket numbers.

7.4 Diagnostic Mode Commands

If the firmware is not operating in diagnostic mode, the following message is displayed, and the command is ignored.

```
Not in Diagnostic mode
```

Note that the $RUN commands are available in this mode.

7.4.1 $CL

Syntax: $CL hexaddr hexvalue

Changes the longword of memory at hexaddr to hexvalue. Hexaddr must be even.

7.4.2 $DL

Syntax: $DL hexaddr

Displays the longword of memory at hexaddr. Hexaddr must be even.

7.4.3 $DM

Syntax: $DM hexaddr hexlength

Displays hexlength bytes of memory starting at hexaddr. Hexaddr must be even.

If hexlength is not specified, a length of 128 bytes is used.

The display is paged in 128-byte pages; press <Return> to see the next page or <Ctrl-C> to stop.

7.4.4 $DW

Syntax: $DW hexaddr

Displays the word of memory at hexaddr. Hexaddr must be even.

7.4.5 $DB

Syntax: $DB hexaddr

Displays the byte of memory at hexaddr. Hexaddr can be odd.

7.4.6 $CW

Syntax: $CW hexaddr hexvalue

Changes the word of memory at hexaddr to hexvalue. Hexaddr must be even.

7.4.7 $CB

Syntax: $CB hexaddr hexvalue

Changes the byte of memory at hexaddr to hexvalue. Hexaddr can be odd.

7.4.8 $DMOD

Syntax: $DMOD index

Displays the module control block specified by index. Index is a decimal number and corresponds to a CAMAC station number.

7.4.9 $DHOSTI

Syntax: $DHOSTI index

Displays the module control block specified by index. Index is a decimal number between zero and the maximum number of simultaneous hosts supported by the system, minus one, i.e. 29.

7.4.10 $DHOSTE

Syntax: $DHOSTE xxxx xxxx xxxx

Displays the host control block corresponding to an Ethernet address, where xxxx is a 4 digit hexadecimal number. The three sets of four digits provide the Ethernet physical address. The second digit of the first set of four must be even for a physical address.

7.4.11 $RUN

Syntax $RUN testname

If the firmware is not operating in startup diagnostic mode, the following message is displayed.

```
$RUN is available only at system startup and requires the start in
diagnostic mode switch to be set
```

Runs the diagnostics test specified by 'testname'. Table 16 lists the available diagnostic tests. The individual tests are described in more detail below.

Diagnostic test name	Action
MEMORY	Extended test of the buffer memory
CAMAC	CAMAC access and highway tests (requires DTM4)
TIMER	68901 tick timer test
LEDS	Front panel LEDs, 8-bit DIP switch and CAMAC crate address switch test
NL	Station number and LAM line test using special modules– Hytec use only

Table 16 Available Diagnostic Tests

7.4.11.1 $RUN MEMORY

A moving bit pattern is written to the buffer memory, then read, and checked. Nine complete passes are made through the memory. A typical message is

```
    Memory test of buffer area C17C20 to DF1000
```

This test takes less than one minute to complete.

Only buffer memory is checked with this test as the remainder of the RAM is required for system operation.

The test displays a rotating windmill whilst running and can be aborted by pressing <CTRL-C>. If the test fails, the appropriate memory address and data are displayed.

7.4.11.2 $RUN CAMAC

This test runs a 24-bit read/write data check at the DTM4, followed by Function code, Sub-address, Q and X response checks.

Dataway Z, C and I are checked for correct operation.

The message:

```
No DTM4 module defined
```

Might be displayed. Enter the command 'change dtm4' and then the required station number (see above) before re-attempting $RUN CAMAC

If successful, the message;

```
Test 1 – 16-bit write/read
Test 2 – 8-bit data high register test
Test 3 – FA control lines set
Test 4 – Crate initialise test
Test 5 – Crate clear test
Test 6 – Crate inhibit test
Test 7 – Q & X test
Completed OK
```

is shown.

NOTE! This test will only run correctly with a Hytec Electronics Ltd. Dataway test module type DTM4.

7.4.11.3 $RUN TIMER

This test checks the operation of the timer (Timer A) on the 68901 MFP chip. A 1-second tick timer is initialised and the message "Tick" is output to the terminal on every timer interrupt. The ticks can be timed to check clock accuracy.

Terminate the test by pressing <CTRL-C>.

7.4.11.4 $RUN LEDS

This test consists of four parts and each is terminated by pressing <CTRL-C>

A bouncing, single bit pattern is written to the LEDs 'NOQ' to 'FAST CAMAC' inclusive.
The 8-way DIP switch SW1 (emulation) is copied to the LEDs
The 8-way DIP switch SW2 (emulation) is copied to the LEDs
The CAMAC Crate number switches are copied to the LEDs

The display is:

```
LED test – check for a bouncing pattern
Press Ctrl-C to abort
8-way DIP switch SW1 test – switch value copied to LEDs
Press Ctrl-C to abort
8-way DIP switch SW2 test – switch value copied to LEDs
Press Ctrl-C to abort
CAMAC Crate switch test – switch value copied to LEDs
Press Ctrl-C to abort
Test terminated
```

Important notes:
The SW1 and SW2 tests relate to the switches in the Mk3 controller and only parts of these are controlled by switch SW5. SW5 elements 5-8 (LSAP) appear in the lower 4 LEDs (DIAG to FAST CAMAC) during the SW1 test, and elements 1 and 3 control LEDs NOQ and INH during the SW2 test. Jumpers JP3 and JP4 appear in the SW1 test on NOQ and NOX respectively (JP IN = ON).

7.4.12 $NORMAL

The firmware is switched out of the special startup diagnostic mode and normal system operation is initiated. The action is the same as starting the system with the NORMAL/DIAGNOSTIC switch in the normal position.

After this command has been actioned, the $RUN command is no longer available.

7.4.13 $CAMAC

CAMAC command loop. This command is similar to the normal mode CAMAC command (7.2.14) where N, A, F and data are supplied. The command is executed in a continuous loop until <CTRL-C> is entered. If the command line is terminated with a + after the data (for CAMAC writes only) then the data is auto incremented on each cycle of the loop.

This command is only available in diagnostic mode.

Command format:-

```
$CAMAC N A F [data]
```

or if F is a write command (16..23) then:-

```
$CAMAC N A F data +
```

where:-

N	=	CAMAC station in range 1..24
A	=	CAMAC sub-address in range 0..15
F	=	CAMAC function code in range 0..31
Data	=	data for write command (decimal)
+	=	auto increment data

Once the command is entered (RETURN key enters the command) the CAMAC command loop is entered. The message: -

```
Type Ctrl-c to stop
```

is displayed.

CHAPTER 8

8 USING THE ECC 1365

The following sections describe how to configure the ECC 1365 hardware and software and how to verify correct installation. It includes some tips on troubleshooting, should problems with the ECC 1365 arise. See the relevant Installation guides for VMS, UNIX or other host software installations.

8.1 Installing the ECC 1365

The normal delivery configuration of an ECC 1365 will be as Master ACB controller; the front panel RS232 port set for 9600 Baud and the LSAP address set to 60 hex.

It is recommended that you check all configuration details, the links and the switches of all delivered units prior to initial operation.

8.1.1 Configuring as Master ACB

The ECC 1365 is configured as a Master ACB controller as follows:

1 To configure the unit as a master ACB controller the configuration of both the left hand and right hand boards must be as follows:

To access the right-hand board, open the unit by removing the top rail screws of the right hand station and loosening those at the bottom. There is one screw on the rear panel and one on the front panel. The right hand board should now be fitted in place using the four M2 pan-head screws. Now re-assemble the unit, by carefully closing the unit and re-securing the two screws (front & back panels).

2 Install the rear panel ACB connector cable between the two ACB IDC headers.

3 Install the six SIL (8 x 470R) (RN1-6) and two DIL (13 x 470R) (RN7, RN8) “pull-up” resistor packs in their sockets on the rear (close to the CAMAC connector) of the left hand controller board. The resistor packs are installed as shown in Figure 12 and access necessitates removal of the left hand side panel. Be careful to orientate the resistor networks correctly. Note that the common end of the SIL networks is at the bottom.

IMPORTANT: Ensure that the correct values are located in the sockets, and in the correct orientation.

4 Install the single pole LEMO cable between the front panel “Request” and “Grant in” sockets.

The unit is now configured for Master ACB operation.

8.1.2 Configuring as Slave ACB

The ECC 1365 is configured as Slave ACB controller as follows:

1 To configure the unit as a slave ACB controller the pull up resistor packs must be removed from the left-hand board and the right-hand board should be removed as follows:-

To access the right-hand board, first, remove the interconnecting ACB cable, if fitted from the rear panel ACB connectors of the unit. The unit must then be opened, by removing the top rail screws of the right hand station and loosening the bottom rail screws. There is one screw on the rear panel and one on the front panel. Open the unit and remove the four M2 pan-head screws securing the short right-hand card to the rails. Re-assemble, by carefully closing the unit and re-securing the two screws (front & back panels).

Note: the supplied rear panel ACB ribbon interconnect is not fitted in slave ACB mode. A special rear ACB cable is required (available from Hytec on request) with the appropriate number of connectors for the configuration you are using.

2 Remove the six “pull up” SIL resistor packs, RN1 - 6 from their sockets on the rear (close to the CAMAC connector) of the left hand controller board and the two DIL resistor packs, RN7 and RN8. The resistor packs are located as shown in Figure 12 and access necessitates removal of the left hand panel.

The unit is now configured for Slave ACB operation. Remember to re-configure the front panel “Request/Grant” daisy chain, as appropriate, when the unit is installed as a Slave controller in a CAMAC system.

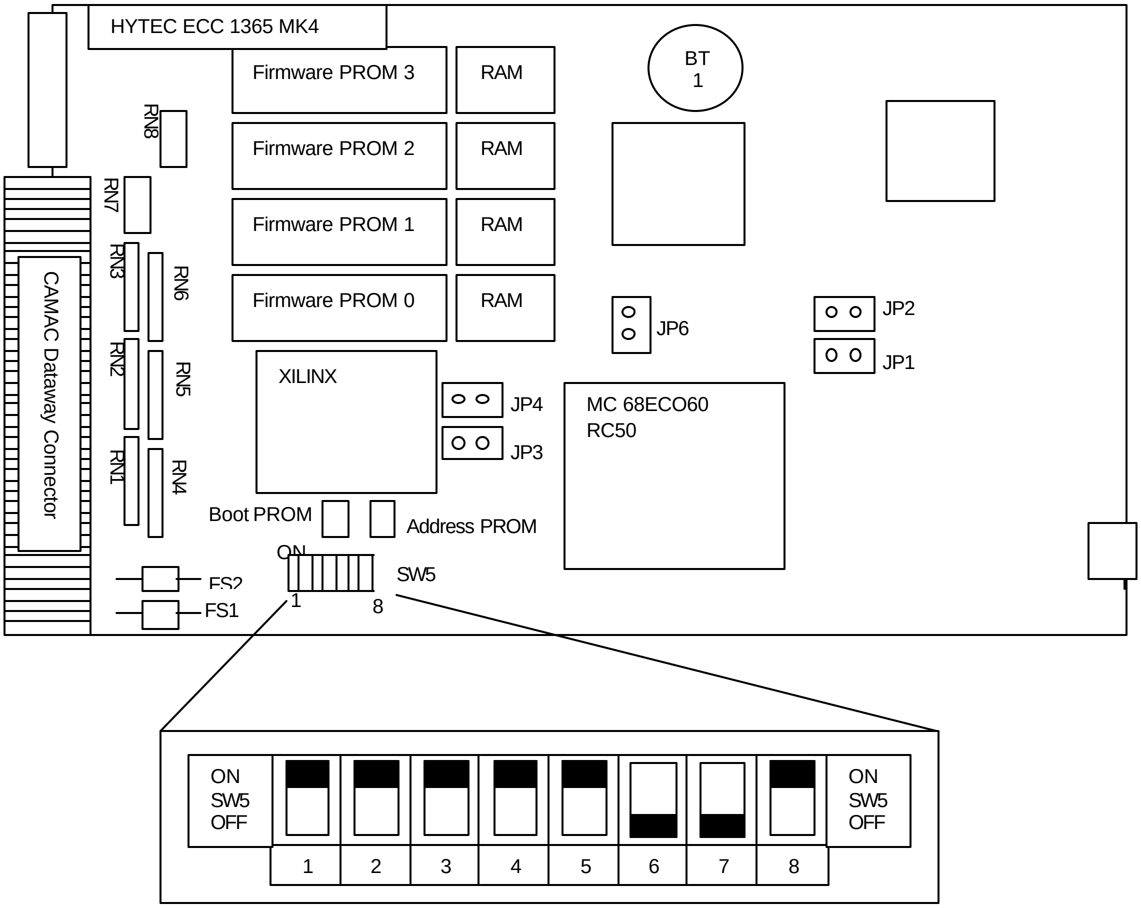
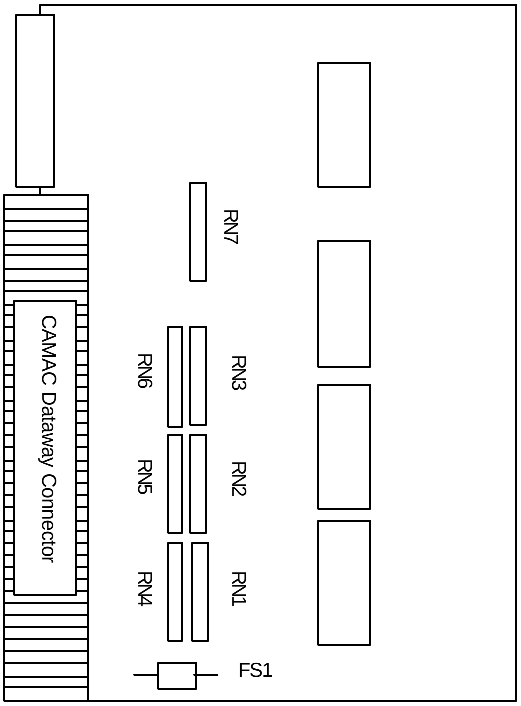


Figure 12 ECC 1365 MK 4 view of left hand side board



FUSE VALUES

Fuses are PICOFUSE Type 275

LHB FS1	3 AMP
LHB FS2	1 AMP
RHB FS1	1 AMP

RESISTOR NETWORKS

RN1 to RN6 on left hand board:
SIL 8 x 470R

And RN7, RN8:
DIL 13 x 470R packs

Figure 13 ECC 1365 MK 4 view of right hand side board

8.1.3 Connecting to UTP Ethernet

The front panel 8-way connector, “UTP”, is for 10/100 UTP Ethernet connection. The connector pin-out and wiring assignment is standard, and is fully covered in the Ethernet specification, see reference 3.

To check for LINK configuration, observe the front panel LINK LED above the UTP connector. If, when powered up, this LED is illuminated (after a short initial delay), the controller has correctly detected a valid link for UTP Ethernet operation. The Ethernet controller will auto-negotiate with the link partner and establish the best available connection. This will normally be either 10Mbit or 100Mbit, Half Duplex. If 100 Mbits is selected, the ‘SPEED’ LED will be illuminated. A message is sent to the diagnostic terminal during initialisation in Normal mode, indicating the result of the negotiation.

If the cable connection is subsequently lost (cable unplugged or broken) this is detected, notified to the terminal and re-connection attempted at regular intervals.

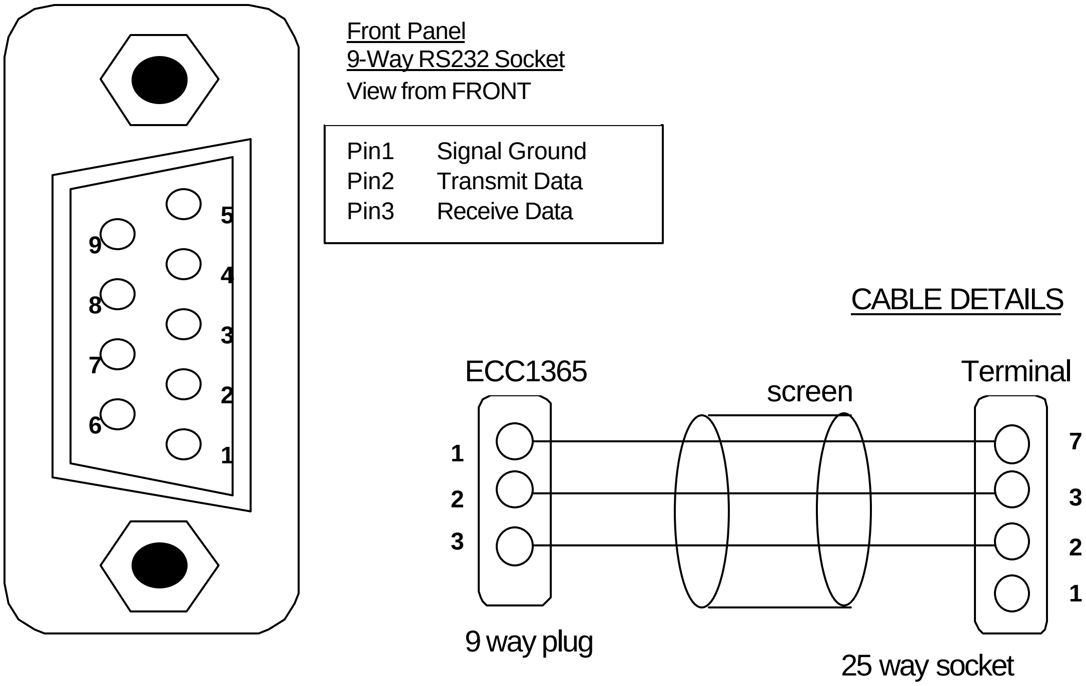
8.1.4 Connecting the Front Panel RS232 Port to a terminal

The front panel diagnostic terminal is connected via the 9-way D-type socket. This is an RS232 connection whose pin allocation is given in Fig 14. Both the transmit and receive paths operate at the selected Baud rate with the following serial settings:

8 data bits
1 stop bit
no parity

The line speed is set in firmware at 9600 Baud. Line data flow control is via the ASCII characters XON, XOFF. A VT100 or compatible type of terminal is suitable.

The diagnostic terminal prints messages at module power-up and is used for initialisation of the module, various types of status displays, setting up of security features and for running diagnostics. Full details are given in Chapter 7.



Pin1	Signal Ground
Pin2	Transmit Data
Pin3	Receive Data

Figure 14: Diagnostic terminal 9-way D-type connector

8.1.5 Configuring the Links & Switches

The ECC 1365 has a number of links and switches that must be set up before using the module. The switches that need to be configured are those which select the operating mode of the controller. Other links on the controller board are factory configured but may need to be modified for special configurations. Normal operation also requires that the rear panel ACB link cable (Master mode only) and the front panel single-pole LEMO cable link from “Request” to “Grant In” must be installed.

Details of links and switch settings that may need attention are given in the following sections. Links and switches not documented should NOT be changed.

8.1.5.1 CAMAC Crate Number Switches

To identify the CAMAC crate from a host computer, the Ethernet Crate Controller is addressed by its CAMAC crate number (this is normal CAMAC philosophy). Each ECC 1365 on the same Ethernet must have a unique CAMAC crate number.

The controller's CAMAC crate number is set up on the two front panel rotary switches located above the UTP connector. Set the switches by inserting a small screwdriver into their centre slot and rotating, when the arrow on the switch shows the setting. The switches can be set from '0' to 'F' in normal hexadecimal fashion. This gives a maximum crate number of 255 decimal. (FF hex).

To set the switches, convert the required crate number to a hexadecimal value and then set the switches accordingly. For example, to set up for crate 42, convert 42 to hexadecimal, which is 2A hex. Set the MSD switch to 2 and the LSD switch to A. Note that these switches are only read at RESET or power-up.

8.1.5.2 Diagnostic Mode/Normal /Reset Switch

The front panel Diagnostic /Normal /Reset mode switch is a three-position toggle with a non-latching position for Reset mode and a latching position for Diagnostics mode.

Operating the switch to the RESET position, forces either a soft or hard reset to the controller. The soft or hard reset mode is selected by JP6 on the left-hand board, see Chapter 8.1.5.5, Left Hand Controller Board Jumpers, Page 76. After a 2-second pause, this causes the controller to re-initialise and enter the appropriate operating mode.

The switch centre position is the NORMAL operating position for the controller.

The upper switch position is for DIAGNOSTIC mode. To select this, move the switch to RESET and immediately move it to DIAGNOSTIC. The controller then initialises into the Diagnostic mode, making available the $RUN and $CAMAC commands form the front panel diagnostic terminal.

To terminate Diagnostic mode, RESET the controller, leaving the switch in the NORMAL position.

8.1.5.3 Z Switch

The front panel Z switch is a push button that issues a CAMAC dataway ZED. The action of depressing the switch interrupts the processor and causes a CAMAC Dataway cycle issuing a CAMAC ZED (CAMAC initialise) to be executed. The switch is deliberately mounted flush with the front panel to avoid accidental operation.

Note: Issuing a CAMAC ZED to a CAMAC crate causes a total crate re-initialisation and should therefore be used with extreme caution. It should never be done to a running system unless full authorization for such action has been obtained.

8.1.5.4 Left Hand Controller Board Switches

The left hand controller board has one bank of switches, accessible through a cut out in the bottom rear of the left hand side panel. These switches are shown in Figure 12

The switches have the following functions and should be set up at installation time.

Switches SW5 – left hand board

Switch SW5-1 CAMAC ZED on reset. When enabled (SW2-1 is up) the firmware will issue a CAMAC ZED when the module is reset. When disabled (Switch SW2-1 is down) no CAMAC ZED is issued at module reset.

Switch SW5-2 is not used. [Spare]

Switch SW5-3 sets the accuracy for the internal tick counter. If the switch is down (OFF) the normal 10ms tick is maintained, if the switch is up (ON) the tick rate is increased to 1ms. This may be used for more accurate timing of operations or more frequent timer routines.

Switch SW5-4 is not used. [Spare]

Switches SW5-5 to Switch SW5-8 are used to configure top four bits of the Link Service Access Point (LSAP) address. The LLC protocols require two LSAP addresses, the second of which always has the value of the switch setting plus 4. This MUST be set up even when used with UDP protocol only systems.

For example: for LSAP address of 60hex, set switches SW5-7 and switch SW5-6 down (OFF) and Switch SW5-5 and SW5-8 up (ON). This gives the first LSAP address as 60hex and the second LSAP address is automatically set to 64.

8.1.5.5 Left Hand Controller Board Jumpers

The left hand board jumper locations are shown in figure 12. Their functions are as follows:-

JUMPERS JP1 and JP2 – factory use only, **DO NOT CHANGE DELIVERED SETTINGS.**

Jumper JP3 is a security override setting. With the jumper fitted, the security feature is enabled and any security data in the battery-backed RAM is active. With the jumper OUT, all security features are disabled and battery-backed RAM security data are ignored.

Jumper JP4 is used to enable or disable PID mode booking. When the jumper is IN, modules are booked according to the host Ethernet address and the PID of the process. If the jumper is OUT, then modules are booked by host Ethernet address only.

JUMPER JP6 – HARDWARE RESET ENABLED – this jumper selects the soft / hard reset action of the front panel reset switch. With JP6 installed, a hardware reset is enabled (reset pin of processor is toggled). With JP6 removed, a soft reset is enabled whereupon the firmware initiates the reset action.

A soft reset allows the firmware to fully execute the ECC 1365 reset protocol enabling all hosts to be informed of the reset. A hard reset occurs instantaneously and therefore precludes reset protocol notifications.

8.2 Initial Setup Of Battery-Backed RAM

To enable operation of the ECC 1365, the battery-backed RAM must be initialised. This process must also be carried out whenever the battery-backed RAM has been corrupted, or when you suspect that the battery has become discharged. The NiCad battery (BT1 in figure 12) is permanently on trickle charge whenever the ECC 1365 is powered and once fully charged, should maintain the state of the battery-backed RAM for many months.

It is also possible that you will need to change the settings loaded at factory test time. Note that if the battery-backed RAM has lost its data or you suspect it is corrupted, the controller will not initialise in normal mode. In this case, you must first initialise the module in diagnostic mode and follow the procedure defined below before normal operation can commence.

8.2.1 Entering Battery-Backed Ram Setup Mode

This can be done only with a terminal connected to the front panel. At this terminal, enter the change mode command by typing:

```
CHANGE MODE <RETURN>
```

Enter ‘3’ <RETURN>, to enter diagnostic plus battery-backed RAM setup.

8.2.2 Clearing All Data From The Battery-Backed RAM

Initialise the battery-backed RAM by entering

!INIT <RETURN>

Answer 'yes' to the prompt.

8.2.3 Setting Up The Ethernet Address

The unit requires two Ethernet addresses for normal operation. These are its physical address (its unique address on the Ethernet) and its multicast address that all 1365 controllers and hosts use.

Each unit is supplied with its own unique Ethernet address in an internal PROM. This is read and loaded into battery-backed RAM when the !INIT command is issued. This setting can be overridden using the !EPA command (see Chapter 7.3, Battery-backed RAM Mode Commands, Page 61.

Each unit is also shipped with an identical multicast address, unique to ECC 1365 controllers. This is also loaded by the !INIT command. The setting can be overridden by the !EMA command (see chapter 7.3 Battery-backed RAM Mode Commands, Page 61)

The default physical Ethernet address of each unit is as follows:

0080 0314 0302. The first six HEX digits are defined by Hytec's company ID. Digit seven, a '1', defines the unit as an ECC1365 variant, and the eighth digit, a '4', shows it is a Mark 4 unit. The final four HEX digits are the serial number of the unit.

The default multicast address for all ECC units and hosts is:

0180 0300 0000.

The multicast address specified must be unique for CAMAC controller multicasting, i.e. it must:

- ~ Not conflict with multicasts used by other non-CAMAC interfaces on the same Ethernet.
- ~ Conform to the IEEE 8802.3 Ethernet multicast addressing requirements
- ~ Be the same multicast address used for all ECC 1365 controllers in the same group, i.e. a group of controllers and host machines will share the controllers on the same multicast. Another group of hosts and controllers on the same Ethernet with a different multicast exist separately and will be invisible to each other.
- ~ Be the same multicast address stated in the ECC 1365 host software configuration files.

All host configuration files must have the same Ethernet multicast address when connected to the same Ethernet.

8.2.4 Setting Up The Internet Protocol And Socket ID Addresses.

For operation with UDP/IP protocols, the unit requires that an Internet Protocol address and UDP socket address be set up. These addresses are NOT installed in the internal PROM and therefore MUST be set up for UDP/IP operation.

It is not necessary to initialise these fields if you intend to work in an LLC3 only environment (ALPHA or VAX hosts).The values you enter will be stored in the unit's battery-backed RAM and thus be saved when the unit is powered down.

8.2.4.1 Internet Addresses

The Internet Address is a 32-bit number that encodes both a network address and a host ID. Every host and IP internet must have a unique 32-bit address. There are three formats that determine how the 32-bit field is divided up between network address and host ID. The relevance of this in this discussion is that if your network does not contain an Internet router then your ECC 1365 Internet address must have the same network address field as your host otherwise the host will not see the target. The three types of Internet Address formats are shown in Figure 15.

		7 bits	24 bits
Class A	0	Net id	Host id

			14 bits	16 bits
Class B	1	0	Net id	Host id

				21 bits	8 bits
Class C	1	1	0	Net id	Host id

Figure 15 Internet Address Formats

The other vital information is to understand how internet addresses are written. They are written as four decimal numbers separated by decimal points. Each decimal number encodes one byte of the 32-bit Internet Address. For example, the 32-bit hexadecimal value 0X 0102FF04 is written 1.2.255.4

The number range of the first decimal number identifies the class of the address. Numbers in the range 0 to 127 are class A, numbers in the range 128 to 191 are class B and numbers greater than or equal to 192 are class C.

In order to determine the IP address to assign to your ECC 1365 first give it the same network id field as your machine and then give it a unique host id value.

I.e. if your host IP address is
192.4.6.0

then assign
192.4.6.1
to your ECC 1365 (assuming 192.4.6.1 is not used by any other host).

To determine your host IP address, examine the hosts field in the /etc directory
e.g cat /etc/hosts

To set up the IP address use the !IPA command (section 7.6) whilst in battery-backed RAM setup mode.

NOTE: The IP address, socket number and CAMAC crate number assigned to the controller must be entered in the IPADDR.dat file in /ecc_dir (see section 11.3).

8.2.4.2 PING Command

The controller will respond to the Internet Control Message Protocol "PING" command.

To ping the controller, assuming that the internet address has been set up correctly as described in 8.2.4.1,Internet Addresses, Page 79 above, type the UNIX command:

```
Ping 192.4.6.1
```

The response will be

```
192.4.6.1 is alive
```

Or if it fails, typically:

```
192.4.6.1 is unknown
```

The ping command is a test of basic IP communications and PING must be working before you go on to get the UDP/host code working.

Check the syntax of the PING command for your version of UNIX before you enter the command.

8.2.4.3 Socket Address (port number)

The socket address (also known as the port number) is a 16-bit integer that associates the host process, the data and the target process. The value you choose must not be one of the other "well known port numbers" on the system, indeed some port number values are internet specific and must not be used. The value you choose to use must be well known to all TCP and UDP protocol users on your network and be unique to ECC 1365 controller use. All controllers on your network should use this same number. We have used the value 240 and have not found any problems on our network.

The socket address (or port number) is set up in the controller using the !IPS command described in section 7.3,Battery-backed RAM Mode Commands, Page 60The controller must be in battery-backed RAM set up mode to use the !IPS.

8.2.5 Starting the ECC 1365 in Normal Mode

Once the battery-backed RAM is initialised and the Ethernet address is set up, the controller can operate normally. If you wish to initialise the security table and/or set up the download command RAM area, this can be done whilst still in battery-backed RAM mode, using the commands given in Chapter 7.3,Battery-backed RAM Mode Commands, Page 60

To enter normal operation at this point, operate the front panel switch, leaving it in its normal position after toggling to RESET.

8.3 Trouble Shooting

The following is a list of faults or problems that you may encounter along with a few possible causes and suggested solutions. This is not an exhaustive list but may help with overcoming initial “teething” problems for u nfamiliar users.

If the problem persists or the solution cannot be found, please contact Hytec Electronics Ltd, U.K. or our agents worldwide for advice

IF IN DOUBT – ASK!

The list is divided into two sections. The first deals solely with the ECC 1365 controller unit and its installation in a CAMAC crate. The second list considers VAX/VMS host problems and system problems arising from the host / ECC 1365 combination.

ECC 1365 Trouble shooting

PROBLEM	POSSIBLE CAUSES AND FIXES
1. Front panel LEDs do not light	▪ Check CAMAC crate power supplies are Ok (+6V, -6V, +24V, -24V) ▪ Check ECC 1365 internal fuses are OK – see figures 12 & 13 (3 fuses). If fuses have blown, check for causes before replacing and re-trying.
2. Module will not initialise	▪ Battery-backed RAM corrupted (possibly due to the battery being discharged) Need to initialise, see chapter 8.2, Initial Setup Of Battery-Backed RAM. Page 77 ▪ Ethernet not connected correctly. Check UTP connection. See section 8.1.3, Connecting to UTP Ethernet, Page 72. ▪ Ethernet crossover problem – check that the hub port is not a crossover type. ▪ CAMAC self test fails, see 4 below ▪ Check ACB cable between left hand and right hand CAMAC PCBs is correctly inserted.
3. Front panel port does not communicate with terminal	▪ Check interconnection cable. See figure 14 for wiring details. ▪ Check terminal Baud rate setting is 9600. ▪ Check for 8 data bits, 1 stop bit, no parity. ▪ Check for receive/transmit polarity in cable (pin2/ pin3 problem) ▪ Issue XON to ECC 1365 by typing <CTRL-Q> (ECC 1365 uses XON/XOFF for flow control).
4.CAMAC self test fails ($RUN CAMAC in diagnostic mode)	▪ Check LEMO cable is fitted between REQUEST and GRANT IN on the front panel. (ACB Master only). ▪ Check ACB ribbon cable is fitted at rear of unit (ACB Master only) ▪ Check module is in control station (rightmost CAMAC station). ▪ Check LEMO cables between GRANT OUT and GRANT IN fitted between Master and other slave ACB controllers. ▪ Check that test module is a HYTEC Dataway Display type DTM4 ▪ Check that DTM4 station number has been defined (see CHANGE DTM4 command, section 7.2 ,Normal Mode Commands , Page 53
	▪

CHAPTER 9

9 SECURITY FEATURES

The software in the Ethernet Crate Controller (ECC 1365) maintains a table containing the address of host systems that are allowed to access the ECC (the use of this table is enabled by switch SW1-1 on the ECC – see Chapter 8.1.5.5, Left Hand Controller Board Switches, page75.

For each address, a mask defines which modules the host system can access and a set of capabilities define which ECC-wide operations the host can perform.

The table is kept in battery-backed RAM so that it is maintained when power is removed from the ECC 1365.

All security features are optional. If the table is empty, the ECC is "open" and any host is allowed to perform any operation. If there is at least one entry in the table, the ECC is "closed" and only the hosts in the table can access the ECC.

Note! Changing data in the security table requires care. Errors in data entry can cause confusing results. In order to protect hosts who attempt to make the first entry to an 'open' module the following conditions are enforced:-

> When a host system sends a security table update command, and the security table in the ECC 1365 is currently empty (i.e. OPEN), then the host address in the command message must match the source address of the message and the security table update enable bit is forced to be SET.

The table can be updated by one of two methods:

> A terminal can be connected to the front panel RS232 connector and a simple command interface then used to display and change table entries. See section 7.2 ,Normal Mode Commands, Page 53
>
> A host can make changes to the table across the Ethernet, provided that the table is initially empty or the host has the required capability specified in its existing table entry. (Command code 20).

The security table can contain approximately 150 entries and the format of an entry in the table is shown in Table 18.

Ethernet IP Address	Capabilities	Flags	Module mask
48 bits	16 bits	8 bits	24 bits

Figure 16 Security Table Entry Format

Where :
Capabilities is a 16-bit field defining the capability of this host to perform ECC-wide operations

Module mask is a 24-bit field and contains a 1 in bit position 2^N if the host is allowed access to the module in station number N.

Value (binary)	Meaning
`.... .... .... ...0`	Security table update not allowed
`.... .... .... ...1`	Security table update allowed
`.... .... .... ..0.`	Crate Initialise not allowed
`.... .... .... ..1.`	Crate Initialise allowed
`.... .... .... .0..`	Crate Clear not allowed
`.... .... .... .1..`	Crate Clear allowed
`.... .... .... 0...`	Set/Clear Dataway Inhibit not allowed
`.... .... .... 1...`	Set/Clear Dataway Inhibit allowed
`.... .... ...0 ....`	Download new command or COR not allowed
`.... .... ...1 ....`	Download new command or COR allowed
`.... .... ..0. ....`	Alter module/LAM promiscuous flag not allowed
`.... .... ..1. ....`	Alter module/LAM promiscuous flag allowed
`.... .... .0.. ....`	ECC reset not allowed
`.... .... .1.. ....`	ECC reset allowed
`.... .... 0... ....`	Store system command block not allowed
`.... .... 1... ....`	Store system command block allowed
`.... ...0 .... ....`	Enable / disable autobooking not allowed
`.... ...1 .... ....`	Enable / disable autobooking allowed
`.... ..0. .... ....`	Purge booking entries not allowed
`.... ..1. .... ....`	Purge booking entries allowed

Table 17 Security Table Capabilities Field Format

ECC 1365 MK 4 SPECIFICATION

Mechanical

Dual-width CAMAC Crate Controller module to ANSI/IEEE Std 583-1982 (EUR4100).

Height	120mm
Width	35mm
Depth	330 mm (including rear connectors & front panel switch)
Weight	1.3kg

Electrical

Power Supplies:

+6V	2.0 A max
+24V	400mA max

Fuses – see fig12.

Operating temperature: 0 to +50°C. Forced air-cooling **mandatory.**

Connectors

Rear Panel ACB connector

40-way 3M low-profile box header (centre bump polarization)

Front Panel

Request/Grant In/Grant Out
Single Pole LEMO “00 size” socket

UTP Ethernet

8-way MMJ socket.

RS232

9-way sub-miniature D-type socket, with screw locks.
(see figure 14 for connections)

GLOSSARY

ARP Address Resolution Protocol

Dataway Q Single bit response to CAMAC status interrogation, i.e. True or False.

Dataway X Single bit response. Returned after each CAMAC cycle

0= either no module or the module does not support the command

1= the module responds to the command.

Enable demand Enable CAMAC interrupts (LAMs).

Ethernet A local area network technology originally developed by DEC, Intel and Xerox. A new version of the technology is specified by ISO and is more accurately described as Carrier Sense Multiple Access with Collision Detection (see reference 3 for full details). The term “Ethernet” still commonly refers to this type of technology.

Ethernet address a 48-bit address which uniquely identifies a system on an Ethernet local are network

Event Flags Status posting bits maintained by VMS, which are used to perform a variety of signalling functions

Global Section A section of memory, which may be shared by more than one VMS process

IP Internet Protocol

ICMP Internet Control Message Protocol

LSAP the Link Service Access Point is the interface between the Link Layer (layer2) of the ISO 7-Layer model) and the user of that service. In the ISO model, the user is the Network Layer (layer3). However, in this document, the application interfaces directly to the Link Layer

LSAP Address. An 8-bit address, used by the Link layer within a particular system, to identify an LSAP.

Logical Link Control Procedures

These concern the data-link layer and support medium-independent data link functions and use the service of the Medium Access Control sub-layer. Type 1 operations describe a connectionless mode of operation [Reference 2]. Type 3 operations describe a connectionless acknowledged mode of operation [Reference 4]

Multicast Address An Ethernet address that is accepted by a group of systems on an Ethernet local area network.

TCP/IP Transmission Control Protocol/Internet Protocol.

UDP User Datagram Protocol

REFERENCES

1 ESONE SR/01, 1978, Subroutines for CAMAC.

2 ISO/IEC IS8802-2 Logical Link Control for Local Area Networks

3 ISO/IEC IS8802-3 Carrier Sense, Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specification.

4 ISO/IEC JTC1/SC6 N5231 Local area Networks, Part 2 Logical Link Control Addendum 2: Acknowledged Connectionless Service, Type 3 operation.

5 IEEE Std 583-1975, Modular instrumentation and digital interface system (CAMAC).

6 IEEE Std 683-1976, IEEE recommended practices for block transfers in CAMAC systems

7 System Oriented Network Interface Controller (SONIC) National Semiconductor Local Area Network Data Book

8 Vax/VMS vol.7B Program Development: Message Utility Reference Manual.

9 Vax/VMS vol.8C System Routines: Run-time Library Reference Manual

10 Vax/VMS vol.8D System Routines: System Services Reference Manual

11 Vax/VMS vol.10A System Programming: I/O Part II

12 L.Lamport (1978) comm. ACM 21 (7), pp558-565.

13 The HYTEC 1365 Ethernet Crate Controller – User Guide To The Extended ESONE Routines (FORTRAN and C editions available)

14 Introduction to Internet Protocols. Computer Science Facilities Group, Rutgers, The State University of New Jersey, USA 1987

15 RFC 791, Internet Protocol

16 RFC 768, User Datagram Protocol

17 RFC 792, Internet Control Message Protocol

18 RFC 826, Address Resolution Protocol

19 RFC 1010, Assigned numbers.

APPENDICES

APPENDIX A1

A1 ECC 1365 HARDWARE DETAILS

The CAMAC Port

The processor accesses CAMAC through a memory-mapped interface. The Base address of the CAMAC Port and Control and Status Registers start at HEX 800000. The CAMAC Station Number, Subaddress and Function Code are encoded into the “memory” address used by the processor, to access CAMAC as follows:

1 0 0 0 0 0 0 0 0	F8 F4 F2 F1	N16 N8 N4 N2 N1	A8 A4 A2 A1	0 0
Base address	F Code	Station number	Subaddress	Must be zero

Note that F16 is derived directly from R/W

When the processor accesses CAMAC, a Read or Write memory cycle occurs, whose length depends on the time taken to gain ACB Mastership and then complete the CAMAC cycle. To guard against ACB lockup, for example, a Timeout protection system is incorporated, which also prevents non-existent memory accesses. Whilst the CAMAC address access takes place, 24 bits of data can be transferred in either direction.

A separate Status Register tells the processor whether Q and X were received in the last CAMAC cycle, (see below).

Internal Controller Functions.

These are implemented in a way similar to a standard set of “Type A” Controller Commands, with the inclusion of most of those relevant to a Programmable LAM Grader, addressed through Station 28 or 30.

A(12) F(1)	Read LAM status (Actual L line states)	Q=0
A(13) F(1)	Read LAM mask (Host specific)	Q=0
A(14) F(1)	Read LAM request Register (Host Specific)	Q=0
A(0) F(8)	Test Controller LAM	Q=LAM
A(0) F(10)	Clear Controller LAM	Q=0
A(13) F(11)	Clear all LAM Mask bits (Host specific)	Q=0
A(0) F(14)	Set Controller LAM	Q=0
A(13) F(20)	Bit set LAM Mask	Q=0
A(13) F(22)	Bit clear LAM Mask	Q=0
A(1) or A(10) F(24)	Disable Demands +	Q=0
A(1) or A(10) F(26)	Enable Demands +	Q=0
A(8) F(26)	Generate Z	Q=0
A(9) F(24)	Remove I	Q=0
A(9) F(26)	Set I	Q=0
A(9) F(27)	Test Dataway I	Q=I
A(10) F(27)	Test Demands Enabled +	Q=DE
A(11) F(27)	Test Demands Present +	Q=DP

+ means Demand relevant to a specific host, i.e. the controller can send Demand Messages to some hosts but not to others.

NOTE: These commands are provided through the firmware and are intended for compatibility only. Their use is strongly discouraged. Use the appropriate ESONE / DOE routine instead.

Single Action Messages result in the controller doing the appropriate CAMAC command and then returning a message with any read data collected, followed by a Statusbyte (showing Q and X for the cycle). An error occurring during the cycle results in an error reply message being sent (see below).

Block command messages result in a number of CAMAC cycles taking place in the selected Q mode (provided that none of the stations referred to by the block command are booked to another host). The number of CAMAC cycles are defined by the message and they are all performed unless some error arises to curtail the sequence. The various sources of error all result in a “Block Mode Incomplete” type reply message being sent, for the following reasons:

a) No X (except in Q scan)
b) No Q (except in Q ignore or Q scan)
c) Timeout failure (see Errors and Interrupts, below)
d) Cycle Count complete before End Address in Q scan
e) Q Scan End Address before Cycle Count complete in Q Scan

Note that the “incomplete” message can still contain data

CAMAC Port Control and Status Register.

The CAMAC Port is equipped with an 8-bit Control and Status register. By writing to this Register, the processor can over-write the Dataway Q and X stores, assert or remove the controller's Dataway Inhibit signal & the "Software LAM" and control the generation of Power-Fail Interrupts. The status Register shows the state of:

Q and X during the last CAMAC cycle

Dataway Inhibit

Controller LAM

Power-Fail Interrupt Disable

Power-fail Flag

The NORMAL / DIAGNOSTIC Switch

Control Register Format

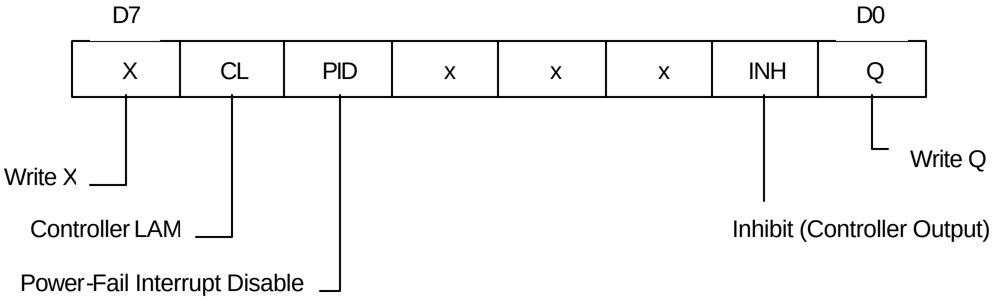


Figure 17 Control Register Format

The controller LAM enables the processor to generate a LAM for Test Purposes.

The Power-Fail Interrupt Disable gates the output of the power monitoring circuit before it causes an interrupt.

Status Register Format

The Status Register is an 8-bit register, which contains the following information:

a) The state of Dataway Q from the last CAMAC cycle
b) The state of Dataway I (a logical OR of controller INH and others)
c) spare
d) The state of the DIAGNOSTIC/NORMAL mode switch
e) spare
f) The power-fail interrupt disable bit state.
g) The state of the Controller LAM
h) The state of Dataway X from the last CAMAC cycle

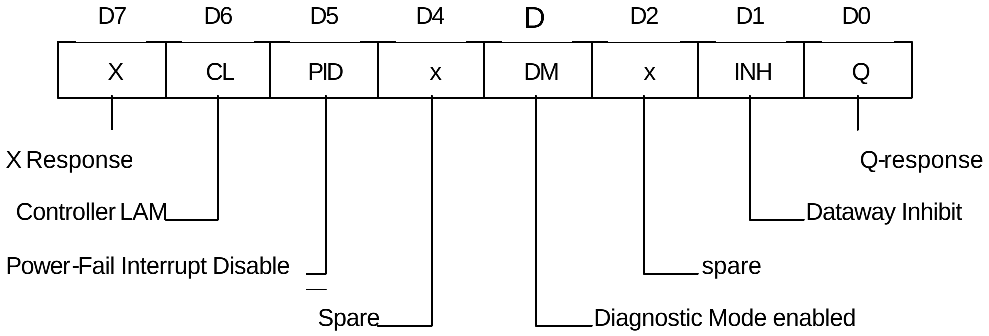


Figure 18 Status Register Format

Errors and Interrupts

After a CAMAC Cycle has been initiated by the processor (by asserting Transfer Start with the bus address within the CAMAC area), The "memory" cycle is completed (even if it has to be cut short by the Timeout Monitor circuit). This monitor protects against ACB failures plus any attempted access to non-existent memory. It works as follows:

Some external cause could prevent the successful completion of a CAMAC cycle e.g. someone holding the ACB or an attempt made to access a memory location which does not physically exist (determined by the transfer acknowledge (TA) Response Programmed Logic Device). Then, a preset time (nominally 10 microseconds) after the Cycle was initiated, the Timeout Circuit causes BUS ERROR to be asserted into the processor. The processor issues a RESET to clear the fault and sends a "Processor Timeout" message to the host.

LAM Handling
LAM signals are received on the left hand board via the ACB Auxiliary 'L' Lines. If the controller is a Master in Stations 24 and 25, these will be terminated on the right hand board and fed through the ACB cable to the left-hand board.

The 24 LAM lines are connected to the Xilinx chip on the left-hand board. This provides full masking and/or prioritising of the LAMs under software control. This logic produces its own interrupt signal and this is fed into the processor's Prioritised Interrupt Handler as IRQ4.

Power Fail

This circuit monitors the CAMAC +6 volt power rail inside the Ethernet Crate Controller. The circuit output is connected to the processor's Non-Maskable Interrupt line through a gate, which can be controlled by the processor via o ne of the Control Register Output lines (bit 5). The processor response to the power-fail interrupt is to attempt to notify all known hosts.

Serial Port

A front panel 9-way D type connector is provided for an external RS232 or RS423 device to communicate with the processor, see Chapters 2.6 and 8.1.5.4, Left Hand Controller Board Switches, Page 76.

A VDU can be connected and two principal uses are envisaged:

During commissioning, to select test routines from the firmware, to check out sections of the controller.

In operation, to allow "privileged access" to the Security Tables, held in the battery-backed RAM.

Bit and Byte Order

The bit numbering in this document has bit 0 as the least significant bit.

All data defined in this document, except the MAC and LLC headers, is in Vax byte order. Thus processors such as the 68060 need to re-order the data as follows:

8-bit values are correctly ordered;

16-bit values need to have the two bytes swapped;

32-bit values need to apply the 16-bit swap to the two halves.
The first 16 bits are then the low 16 bits of the 32-bit value and the second 16 bits are the high 16 bits of the 32-bit value.

RAM Memory

The standard controller is equipped with 2 Mbytes of Static RAM memory provided by four 512K byte devices.

RAM addresses are:

2 Mbyte	Hex C00000	to	DFFFFC	4 x 512K

APPENDIX A2

A2 ECC 1365 PROTOCOLS FRAME FORMATS

Offset (bytes)	Length (bytes)	Contents
0	6	Multicast Ethernet Address
6	6	Source Ethernet Address
12	2	MAC Length Field
14	1	LLC Destination LSAP
15	1	LLC Source LSAP
16	1	LLC Control Field (=UI Frame)
17	1	Padding Byte (=0)
18	2	Frame Type (=1)
20	4	Originator's Network Time (10msec since midnight)
24	2	Originator's transmission delay (10 msec units)

Note: see Chapter 5.4, Network Time Protocol, Page 37.

Table A2 -1 NTP Multicast Frame Format

Offset (bytes)	Length (bytes)	Contents
0	6	Multicast Ethernet Address
6	6	Source Ethernet Address
12	2	MAC Length Field
14	1	LLC Destination LSAP
15	1	LLC Source LSAP
16	1	LLC Control Field (=UI Frame)
17	1	Padding Byte (=0)
18	2	Frame Type (=2 for Request, =3 for Response)
20	2	CAMAC crate number

Note: see Chapter 4.9.1,Find Address Protocol, Page **Error! Bookmark not defined.**.

Table A2 -2 FAP Multicast Frame Format

Offset (bytes)	Length (bytes)	Contents
0	6	Multicast Ethernet Address
6	6	Source Ethernet Address
12	2	MAC Length Field
14	1	LLC Destination LSAP
15	1	LLC Source LSAP
16	1	LLC Control Field (=UI Frame)
17	1	Padding Byte (=0)
18	2	Frame Type (=4 for Request, =TODO ? for Response =TODO ? for Active)
20	2	CAMAC crate number

Note: see Chapter 4.9.2, ECC 1365 Reset Protocol, Page **Error! Bookmark not defined.**

Table A2-3 ERP Multicast Frame Format

Offset (bytes)	Length (bytes)	Contents
0	6	Destination Ethernet Address
6	6	Source Ethernet Address
12	2	MAC Length Field
14	1	LLC Destination LSAP
15	1	LLC Source LSAP
16	1	LLC Control Field
17	1	Padding Byte (=0) or LLC3 status field
18	2	Padding Byte (=0) or pseudo LLC3 control field
20	2	Frame Type (=7)
22	2	Request number
24	2	CAMAC crate number
26	2	ECC Host ID
28	4	Host PID
32	2	Host access ID
34	2	Flags
36	2	Software Version number from host / Status to host
38	n	Data area

Table A2-4 ECP Frame Format (LLC and Pseudo LLC3 only).

The fields in the frames are defined as follows (LLC and MAC fields are defined in the appropriate standards):

When true LLC3 procedures are used, the pseudo LLC3 fields become padding bytes and are set to zero.
When pseudo LLC3 procedures are used, the LLC control field is set to “UI frame”, the first padding field is zero and the LLC3 control and status bytes are inserted into the pseudo LLC3 fields.

Frame type identifies an ECP frame. Set to 7.

Request number is unique to each request from the host to the ECC. A sequence number can be used.

CAMAC Crate Number is the number of the CAMAC crate controlled by the ECC. It is used to cross check the request / response.

ECC host number is copied by the host from responses to subsequent requests. It is used by the ECC to speed table lookup. A value of –1 indicates “not known”.

Host Process Identifier (PID) is copied by the ECC from a request to its response. It is used by the host to identify the originating user process.

Host access ID is copied by the ECC from a request to a response. It is used by the host to speed table lookup.

Flags a 16 bit flag field is formatted as follows.

[.... .... xxxx xxxx] Local to host or ECC. Always zero during transfer.
[1... ....] Immediate response required
[0... ....] Deferred response required.
[.... ...1 ....] First segment of sequence of frames.
[.... ..1. ....] Last segment of sequence of frames.

Note that an immediate response request and its response must have both the first and last segment flags set to 1.

Version The version number of the host software (allows version compatibility checking)

Status The completion status of a requested operation (see Appendix 3.)

Data The user data

APPENDIX A3

A3 VAX/VMS HOST SOFTWARE DETAILS

This appendix describes the host system software, which is written for VAX machines running Version 5.n of VMS (VAX and VMS are trademarks of Digital Equipment Corporation) It describes the internals of this software together with its data structures and the interface with its user processes and with the controller.

A3.1 User-based Software

A3.1.1Overview

A user process is able to communicate via the ESONE / DOE CAMAC subroutines (which do not return until the specified operation is complete) or via a set of extended ESONE / DOE CAMAC subroutines, which return immediately. The latter require a user call to a generalized wait routine, to receive the command completion status when it is available. The routines also exist as a set of function calls.

The ESONE / DOE CAMAC subroutines make use of the CTSTAT subroutine to provide status information to the user-based software. The ESONE / DOE CAMAC functions return status directly to the user based software, making the call to CTSTAT redundant.

An additional set of routines is provided to allow the user to access the full functionality of the ECC 1365.

All routine calls cause a parameter block to be built, based on the parameters passed as arguments together with an internal identification code, which uniquely identifies which routine has been called. First-order error checking is carried out at this stage and errors are available when control passes back to the user-level software.

The extended ESONE / DOE CAMAC routines have, as additional parameters, a variable identifying a local event flag (set on completion) and the address of an I/O status block which contains, on completion, the final status of the command.

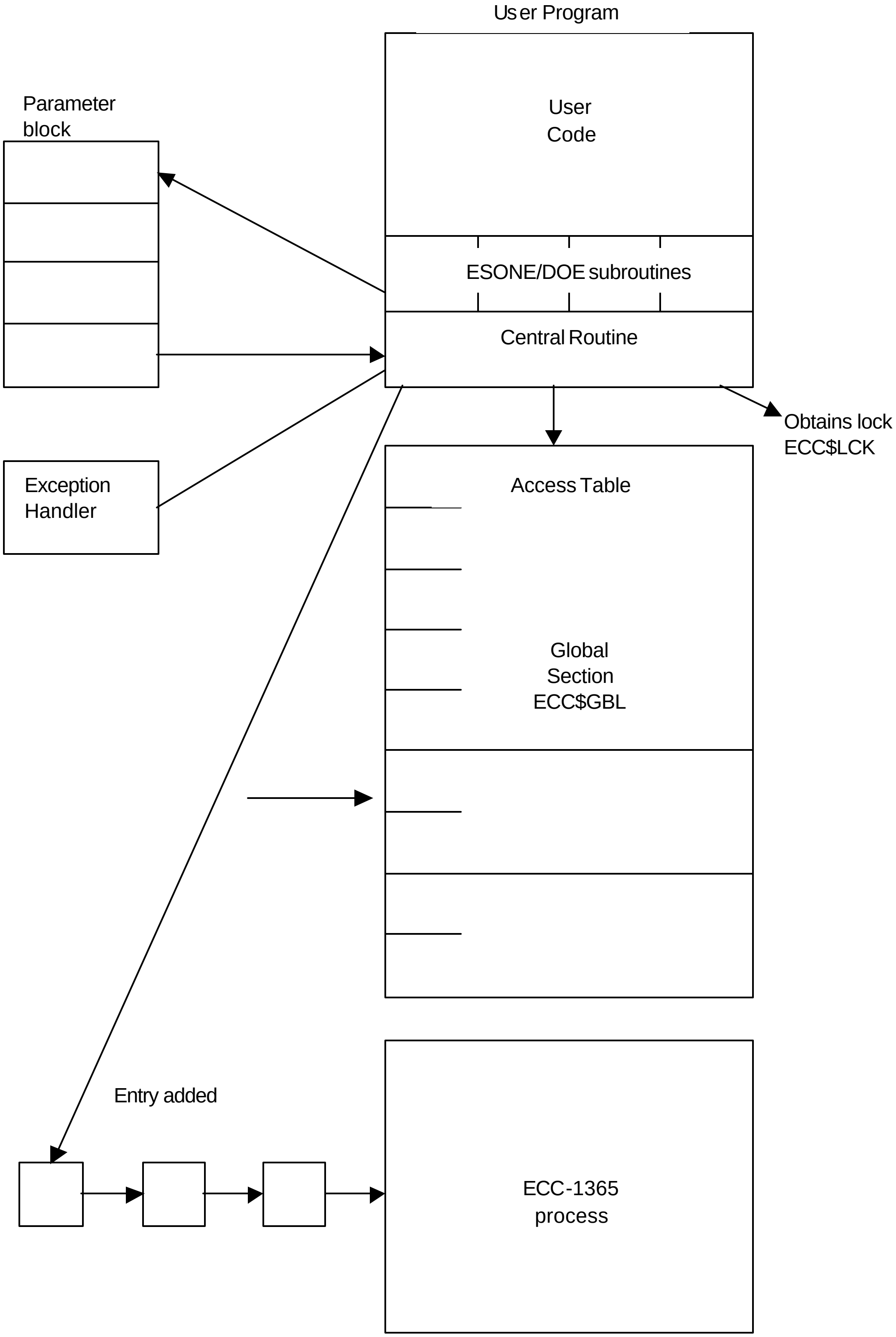


Figure A3-1 User Process to ECC 1365 Host Process communication

A3.1.2User Based Software Central Routine

Once the parameter block has been constructed, it is passed to a central routine that acts as the focus for all user-callable routines. This routine is responsible for the communications between the user's process and the system process (called ECC_1365). This involves establishing the linkage to the ECC_1365 process, constructing and transferring user CAMAC commands to the ECC_1365 process for transmission onwards and tidying up on completion.

The central routine establishes a VMS exception handler that is called if any exception condition is generated by the user code. The exception handler tidies up the association with the ECC_1365 process and releases all resources held by the user process. The process of tidying up includes signalling to the ECC_1365 process to clear all references to this user process andfree up any resources held on its behalf.

Establishment of the linkage with the ECC_1365 process should be read in conjunction with the description of the interface between the ECC_1365 process and all user processes.

The user process identifier, (the PID) is obtained via a call to a VAX/VMS System Service and is stored in the Access Table and used in all communications with the ECC_1365 process.

An attempt is made to obtain the exclusive lock ECC$LCK and any failure is reported back to the user level code by the mechanism described above.

The global section ECC$GBL which has been established by the ECC_1365 process is mapped.

An Access Table (in the global section) is searched to find an available entry. If the search is successful, the entry is marked "in use" by adding the PID to this table. If no entry is available, an error is returned to the user-level code. In either case, the lock is released at this point.

The table entry contains the address of a queue origin (which is used to receive information from the ECC_1365 process) and the value of a common event flag on which this process awaits communications from the ECC_1365 process.

The ECC_1365 process has a single input queue and an associated common event flag which is known to the user process. These are used to transmit information to the ECC_1365 process.

The received parameter block is decoded and the equivalent ECC 1365 command block constructed in memory, the details of which are described inChapter 4.6 System Protocols. This command block is transferred to the ECC_1365 process in a set of one or more buffers. The header field of the buffers is completed, to include the index to the Access Table and the PID of this process. These are used uniquely to identify the buffers to the system.

The command block is copied to the data area of the set of buffers and the parameters block is set up to ease the extraction of data from the set of buffers when they have been received by an ECC 1365 module.

A3.1.3User Based Software Completion Processing

If the transferred command resulted from a call to a standard ESONE / DOE CAMAC routine, the process at this point waits on its common event flag for completion of the command. This wait operation is guarded by a safety timer to ensure that a deadlock is avoided.

If the command resulted from a call to an extended ESONE / DOE CAMAC routine, a summary of the command is written and added to the "awaiting completion " queue and control passed back to the user-level code. The status indicating successful queuing ofthe command is available to the user-level code.

On completion from the wait state, the complete command block is extracted from the set of returning buffers and a parameter block is encoded. This is passed back to the specific ESONE / DOE routine which extracts the data and passes them back in the arguments of the original call. The final completion status is available at this time.

If, while awaiting completion of a standard ESONE / DOE CAMAC routine command an extended command completes, it is saved on the "completed" queue to be handled later, when the user-level code calls the wait-on-completion routine, as defined in the extended ESONE / DOE CAMAC routine set.

If the safety timer expires, all association with the ECC_1365 process is removed and control is passed back to the user-level code. The error status is available to the user-level code.

If the user –level code has made calls to the ESONE / DOE CAMAC routines, a call must at some time be made to the wait-on-completion routine to receive back the results of the CAMAC command. The routine is called with the logical OR of the set of local event flags passed as arguments in previous calls.

This routine either waits on completion from the ECC_1365 process or uses entries on the "completed" queue to satisfy the command completions specified by the set of local event flags. The relevant I/O status blocks are identified, together with any user data areas. These are loaded with information from the completing request and control is passed back to the user-level code.

In this mode of operation, it is essential that all data structures passed to the extended ESONE / DOE CAMAC subroutines are unmodified until completion occurs, indicated by the returning I/O status block.

When the user code terminates, control passes through the exception handler, which ensures that the linkage with the ECC_1365 process is broken and any resources held by the user's process are returned correctly.

A set of routines is provided to allow access to the ECC 1365 modules to perform management operations. This includes reading statistics, tracing buffers, perform download requests and accessing the security features. Suitable authorisation checking is included in this software.

A3.2 Interface Between User- and System- based Software

The ECC_1365 process runs as system process distinct from any user process. Inter-process communication is by the use of a mapped global section, with the logical name ECC$GBL. This is created by the ECC_1365 process to hold tables, queue origins and buffers.

The ECC_1365 process is able to support a configurable number of user processes and generates the required table space at initialisation. For each user process that is supported, one of the common event flag numbers is allocated from the set of common event flags defined by VMS for inter-process communications. This sets the limits of user processes to 60.

A single queue origin and common event flag number is defined for the ECC_1365 process which is known to all user processes and represents the mechanism of communication between a user process and the ECC_1365 process.

An Access Table is defined to allow user processes to connect to the system process. This table contains the queue origin, to be used by the user process to obtain information from the ECC_1365 process, together with the value of the common event flag on which it waits.

To access this table, a locking mechanism is defined using the Lock Management Service of VMS. This lock is known by the logical name ECC$LCK. This exclusive lock ensures there can be no interaction between user processes when an attempt is made to connect to the ECC_1365 process. The user process adds its PID to its Access Table entry to provide unique identification and all communications from a user process contain the PID of that process to ensure consistency

The remaining space in the global section is allocated to buffers, which are each 1536 bytes long. Two general routines are available to the user process.

The first allocates a buffer from the free chain.

The second releases a buffer or a chain of buffers.

Each buffer is able to hold one maximum-sized Ethernet frame but buffers can be linked together so that only one queue operation is required to transfer a set to the ECC_1365 process. The way in which buffers are chained together are:

Individually, for attaching to a queue

Jointly to enable one queue operation to pass several buffers

All queuing operations, including buffer allocation / de-allocation, use the VMS Run Time Library routines which provide indivisible operation on interlocked queues. Once a queuing operation has been completed, the correct event flag is set to signal the operation to the appropriate process.

A3.3 System-based Software ECC_1365 process

The ECC_1365 system process is responsible for the co-ordination of all host activities and the management of communication across the Ethernet. It achieves this by the use of two tables:

The Access Table

The LLC3 Control Table

The Access Table holds specific information about user processes within the host system and the LLC3 Control Table holds information on the state of communication between this host system and all ECC 1365 modules on the Ethernet. The communications are controlled by the use of procedures defined in the LLC3 protocol, see Reference 4

As a supplementary activity, the ECC_1365 process ensures that the Network Time Protocol runs to maintain the Network Time.

The ECC_1365 process has the following functions

Initialise the global section

Initialise the Ethernet interface

Run the Network Time Protocol (NTP)

Process host user requests

Process received network requests

Handle error conditions

A3.3.1Initialisation

On start up, the process declares and holds the exclusive lock ECC$LCK and creates and maps to the global section ECC$GBL. A configuration file is read, and based on that, the Access Table is initialised such that all configured entries are available to all user processes.

The LLC3 Control Table is set up with a configured number of entries, to a maximum of 256entries – one for each CAMAC crate attached to the Ethernet. The table is maintained dynamically, to contain the Ethernet addresses of the ECC 1365 by a process described below. The configuration data defines which host Ethernet controller is to be used and the access to this interface is initialised.

The Network Time Bias variable used by the NTP is initialised and the process enters the Listening state for the period specified by a timeout period.

At this point, the process waits on network events or the expiry of the timeout period. During this period, the process receives NTP frames from any other host systems on the network. Using the information from the frames, the Network Time Bias is adjusted to synchronise the host system time with the Network Time. This action is important because synchronisation is necessary to reduce perturbations to the Network Time when this host begins generation of NTP frames. Once the Listening state time expires, the process releases the ECC$LCK lock, enters the Active state and waits on one of the following events:

A host event

A network event

A timer event

A3.3.2Normal Operations

A3.3.2.1 Host Event

An event completing from a host user process is authorized by comparison of the PID in the received buffer with the PID from the relevant Access Table entry. If there is an inconsistency, the received buffer(s) are released, the entry marked “out of order” and the fact logged, to allow manual corrective action. A correctly authorised request is queued to the relevant LLC3 Control Table entry, based on the Crate information in the request.

If the table entry has no crate Ethernet address, a Find Crate Address multicast frame is generated on the Ethernet and a timer started against this entry. If such information s available and no other requests are outstanding, this request can be transmitted via calls to LLC3 transmission procedures. This generates the appropriate LLC3 request and starts a timer against receipt of the required response. If a request is already outstanding, the user request is queued to this entry until the outstanding request completes or times out. Once it reaches the head of the queue, it is transmitted in the usual manner.

Where the request spans several buffers, these are queued serially on the transmission queue such that, with correct operation, the set is sent to the target system for reconstruction to the command block.

The exception handler of a user process can generate an abort request for the specified host process, which is identified by the Access Table entry number and by the PID. This is validated and, if accurate, acted upon. All knowledge of the host process is destroyed and all resources held on behalf of the host process are returned. If the validation fails, the request is ignored.

A3.3.2.2 Network Event

When a network event completes, it is identified as one of an LLC3 frame, a response to a Find Crate Address multicast or a NTP frame.

A received LLC3 frame is identified as an acknowledgement to an outstanding request or a request to which response is required, by accessing the relevant entry in the LLC3 Control Table.

If it is an acknowledgement, a check is made to validate it and the timer against receipt of this frame stopped. An unsolicited acknowledgement is ignored. Using information in the frame header, the appropriate entry in the Access Table is found and the returning frame is validated against the user PID from the table. It is queued to the user process and the common event flag of that process is set. Finally, the LLC3 Control Table transmission queue is read and the entry from the top of the queue is transmitted.

If the LLC3 frame is a request, i.e. a deferred return of data to a user process, it is acknowledged by the LLC3 module and queued to the user process as above. The LLC3 transmission queue is not accessed.

The buffer being completed to the user process must be checked to see if it is one of a set making up one command response. If it is, completion does not occur until the full set of buffers has been received and linked, so that the single queue operation returns all data related to the initial request.

A response to the Find Crate Address request contains a crate number and, from the source address field of the frame, the Ethernet address of the crate. The LLC3 Control Table is updated. If this results in a change to the Ethernet address (other than from “not known”) and there is a request waiting an acknowledgement, the request must be completed to the user process indicating the error. Requests on the transmission queue can remain unaltered. The response is a multicast and, as such, is received by all host system processes.

This mechanism reduces the total of Find Crate Address requests on the network and allows an individual host to maintain its LLC3 Control Table

The reception of a NTP frame results in the Network Time algorithm being run. This results in the Network Time Bias being adjusted to correct the clock time of this host or the frame being ignored for timing purposes. All frames are used to act as a heartbeat for the originating system and this is noted in the LLC3 Control Table against each system. If, over a sustained period, the heartbeat is missing, the Ethernet addressing information in the Control Table is removed.

A3.3.2.3 Timer Event

This process runs with a tick-timer always active.

On expiry of the timer, the LLC3 Control Table is scanned and any timer counts decremented. If, as a result, a timeout has occurred, the appropriate action is taken in tidying up the table entry, freeing resources held and making the error available to the user-level code in the usual manner.

The NTP timeout is decremented and, on expiry, a NTP frame is generated. This contains the Network Time as perceived by the system, together with an estimate of the transmission delay imposed by this system.

A3.3.3Received Ethernet Frame

A3.3.3.1 Normal Processing

A received frame results in an AST being delivered by the VMS Ethernet device driver to complete the Ethernet read request. This validates the receive status and, if successful, re-issue the read request on the correct I/O channel and queue the received frame to this process for later processing.

A3.3.3.2 Received Events

Two separate types of frames can be received:
An LLC1 frame or an LLC3 frame.

The receipt of these frames is dealt with separately below.

LLC1 Frames
An LLC1 frame carries one of the NTP, the FAP or the ERP frames. These can be distinguished by the type field in the frame that uniquely identifies the protocol being carried.

An NTP frame is passed to the NTP processor. The receive time is computed by summing the time value, the minimum transmission delay from the frame and the estimate of reception delay. This system's time is computed by summing the system time with the network time bias value. The two are compared and if the system time is less that the received time, the network time bias is adjusted to bring them to equality. If the received time is the lower of the two, no action is taken. The buffer holding the frame is finally freed

A received FAP request is ignored and the buffer holding the frame is released.

All FAP responses are examined to keep the address record of the ECCs on the network up to date.

If the LLC3 Control table was empty, the address is recorded and no further action takes place.

If the FAP exchange was initiated by this process in response to a received User Command, the first frame from the sequence comprising the User Command is subsequently transmitted as an LLC3 command.

If the FAP response indicates that the Ethernet address of the specified ECC 1365 has changed and the LLC3 Control Table has a User Command on the active chain, an error status is generated.

The User Command on the active chain is completed to the user process with an error indicating the circumstances and the LLC3 link is re-synchronised. When successfully completed, the top User Command from the passive chain is moved to the active chain. The first frame from the sequence comprising the User Command on the active chain is transmitted as an LLC3 command

A received ERP request is ignored and the buffer holding the frame is released.

A received ERP response frame is noted in the relevant entry in the LLC3 Control Table.
If there is a User Command active, it is completed to the User with an error status and no other Commands are acted upon until the ERP active frame is received.

A received ERP active frame clears the ERP flag from the LLC3 Control Table and allows processing on this entry to continue.

LLC3 Frames

A received LLC3 frame can take one of two formats:

An LLC3 command
An LLC3 response

The distinction between these formats can be drawn by the LSAPs on which they are received.

This process maintains two LSAP addresses so that full duplex communication might exist between any ECC 1365 and this process. LLC3 imposes a constraint that, on any communication path, only one command can be outstanding at any instant and this must be acknowledged before any other traffic can use the path. The communication is defined in terms of the Ethernet and LSAP addresses of the source and destination process. By defining two LSAP addresses in the host, it is possible to have two distinct communication paths between an ECC and a host process.

A received LLC3 command returns data, in response to a User Command or re-synchronises the communications path. This is determined by the presence or absence of an LSDU in the received frame and the setting of the Poll bit in the LLC3 control field.

If the Poll bit is clear and there is a null LSDU, a response with the Final bit clear and a null LSDU must be returned. The communication path is then re-synchronised. The reception of a command with the Poll bit clear and valid user data is, for this implementation, considered to be invalid. Any such frames are ignored and an error status reported in the error logfile.

If the Poll bit is set and the command contains valid user data, this must be completed back to the appropriate user process. The frame is validated by comparing the PID in the frame with the PID in the appropriate entry in the Access Table. If there is a discrepancy, the frame is ignored.

Further validation compares the source Ethernet address of the received frame with the address held in the LLC3 Control Table entry. If there is a difference, the received frame is used to report the error condition to the user and, at that time, any other frames waiting on the active chain are completed to the user process.

The User Command at the head of the passive chain is moved to the active chain and normal processing continues. On successful validation, the received frame is completed to the user process and an LLC3 response with the Final bit set returned to the initiator.

A received LLC3 response should be acknowledging an outstanding LLC3 command. Address violation and PID validation are performed as described above and, where necessary, an error is reported to the user process. The received response has the Final bit set or cleared. This distinguishes a returning acknowledgement to a command containing user data or a command attempting to re-synchronise the communications path.

Final bit clear
If the Final bit is clear and the LSDU is null, the frame acknowledges a re-synchronisation command and user data transfer can recommence. If the LSDU is non-null, the frame is ignored although an error report is added to the error log file

Final bit set
If the Final bit is ser, the response is acknowledging an outstanding LLC3 command that sent user data to an ECC 1365. The response might or might not return user data, depending on the activity of the ECC. An immediate response from an ECC returns user data, while a deferred response acknowledges receipt of the user data. The returning user data is encoded in an LLC3 command at some later time.

User data returned

If user data is returned, it must be completed tothe user process. In either case, successful receipt of the response indicates that the buffer containing the original command might be freed by this process and, in so doing, returned to the originating user process on its secondary input queue. The next frame in the sequence from the active chain should then be transmitted as an LLC3 command. If the active chain is null, the command from the head of the passive chain is moved to the active chain and the first frame from that sequence is transmitted.

A3.4 Data Structures

A3.4.1Global Memory Allocation

The global section has three pages reserved at its head, to hold control structures for this process and user processes. The remainder of the global section is divide into buffers each of 1536 bytes:

Page 1 of the global section holds the User bitmap, this process's input queue origin, the Access Table and the buffer management structures.

Page 2 holds the secondary queue origins of user processes located at a fixed offset from their primary queue origins.

Page 3 holds the pre-allocated buffers used by user processes to communicate a serious error to this process. They are fixed length and their location is calculated by each user process based on their index to the Access Table

Layout of Page 1 of the Global Section ETH$GBL

Use	Size (longwords)	Offset in Page_1
User Bit Map	2	0-1
Process UIC	1	2
Process PID	1	3
Ethernet address	2	4
Process Input Queue	2	6
Reserved	2	8
Access Table	4each entry	10-20
Buffers:		
Buffer Free Chain	2	124
Total Buffer Count 1		126
Free Buffer Count 1		127

Table A3 -1

Each entry in the LLC3 Control Table has the following definition and is used to control the data exchange between this host process and an ECC 1365. The exchange is based on the combination of this process's source Ethernet address and LSAP and the ECC Ethernet address and LSAP value. The LSAP value used depends upon the LLC3 exchange.

A3.4.2LLC Control Table

Integer	*active	*current User Command being transferred
Integer	*passive	*chain of User Commands awaiting transfer
Short	known	*set if ECC active and address known
Short	crate	*CAMAC crate number
Short	flags	*flags field
Short	retry	*retry count for ERP/FAP
Integer	timer	*timer on outstanding ERP/FAP request
Short	addr[3]	*ECC Ethernet address
Unsigned char	tx_sap	*LSAP to initiate LLC3 commands
Unsigned char	v_si	*transmit sequence state variable
Short	cmnd try	*LSAP to respond to LLC3 commands
Unsigned char	v_ri	*Receive sequence state variable
Unsigned char	v_rb	*reception status state variable

Table A3 -2

Each entry in the Access Table has the following layout and its location in the global section is calculated by a host user process using the bit number allocated from the User bitmap. The PID field is set by the User process to mark the entry in use and to provide validation of communications between the User process and this process.

A3.4.3Status Codes

The ECC 1365 uses a global set of status codes to describe the progress of internal operations. Those values which might be returned in the status field of an ECP frame or the reason field of an ERP frame are defined below.

Code (decimal)	Definition
0	General failure
1	Operation performed successfully
3	ERP request accepted
8	Error found when encoding / decoding a parameter description
12	Booking request failed. The module / LAM is marked as promiscuous
22	Duplicate CAMAC crate number seen on the network
24	ECC reset requested by ERP

Table A3 -3

A3.4.4Access Table

Long	Queue[2]	*input queue origin User process
Unsigned	Long PID	*User (process) PID
long	Spare	*reserved to Hytec

Table A3 -4

A3.4.5ECC_HOST Control Table

The ECC 1365 Control Table has the following layout and controls the generation of NTP multicast frames and holds the NTP time bias variable. The state variable is held here and the current state of the process is controlled by the state timer variable.

Integer	*eccq	*process input queue origin
Integer	state	*state of this process
Integer	state_timer	*timer for state transitions
Integer	ntp_bias	*NTP time bias variable
Integer	ntp_timer	*timer to transmit NTP multicast

Table A3 -5

A3.4.6Configuration Data File

The following is an example of the configuration data file. It can be modified to suit a particular installation but such modifications should follow the guidelines outlined in the main body of the text.

```
XQA0:                   *DEQNA driver
1                       *reads issued by the driver
60                      *LSAP1 (in hexadecimal), used by LLC1 and LLC3
64                      *LSAP2 (in hexadecimal), used by LLC3
10                      *number of buffers in system
1                       * logging is enabled
5300 0000 0000          *LLC1 multicast address
1                       *User.txt  logging enabled / disabled
```

APPENDIX A4

A4 AUXILIARY CONTROLLER LOCKOUT MODE (ACL MODE)

A4.1 Overview

The ECC 1365 MK4 controller has been designed ONLY to operate in Request / Grant mode. The unit operates in Request/Grant mode and will respond to the ACL signal described below. A discussion of Request / Grant mode and ACL mode follows:

A4.2 Multiple Controllers on the Auxiliary Control Bus (ACB)

When more than one controller will share control of a CAMAC crate using the ACB, the arbitration scheme used and the assignment of priorities must be carefully considered.

There are two arbitration schemes available:
A) All controllers in Request/Grant Mode
B) One controller in Auxiliary Controller Lockout Mode, all others in Request Grant Mode

A4.3 Request Grant Mode

Control of the crate is shared by assertion of REQUEST and propagation of a GRANT signal from highest to lowest priority by a daisy-chain connection. When all controllers require relatively infrequent access, this scheme works well, but if one or more very high-speed controllers are placed higher in priority then a low speed device then it is possible that this low priority controller can get “shut out” by the other controllers grabbing control and not passing on the GRANT signal. If the low priority controller is connected to a processor then this will cause TIMEOUTS. It is recommended that high-speed controllers can be placed lower in priority than this type of “time critical” device. The disadvantage of this is that the REQUEST–GRANT propagation time of the “slow” device is added to the cycle time of the fast controllers, reducing their speed somewhat.

A4.4 ACL Mode

Perhaps a better way of ensuring that a “time critical” controller does get in when it needs to is to place it in ACL mode while leaving all others in Request/Grant mode. In this case, the ACL device simply asserts a signal called ACL (Auxiliary Controller Lockout) and waits for everyone else to relinquish the bus, whereupon it does its cycle. This guarantees access and leads to the briefest possible interruption to the high speed controllers’ operations. The only drawback of this scheme is that an auxiliary can be forced to abort a cycle, wait for the other controller to do its cycle, then restart its cycle in order to complete its operation.

A4.5 Operating the ECC Mk4 with a device in ACL Mode

The ECC1365 Mk4 is designed to work correctly with all other ACB devices, whether they are in ACL or R/G mode. It arbitrates with them and responds correctly to the ACL signal from, for example, a type L2 serial crate controller. As long as the interruption to the CAMAC cycle caused does not last more then 10 microseconds, then the unit will not experience a timeout.

APPENDIX 5

A5 ERROR PROCESSING AND ERROR MESSAGES

When an executable file is run, a file will be created in the current directory that will contain any error messages that may be generated during execution. This file is called user.txt. The convention for the format of the error string is as follows:

%ECU-severity-reason, message-error generated at user level
%ECU-severity-reason, message-error generated at host manage level
%ECU-severity-reason, message-error generated by remote ECC 1365

These error messages are also written to the user's terminal

A5.1 VAX/VMS Error Processing

All error handling uses the signalling utilities of VMS, in particular the RTL routine lib$signal. This is used in conjunction with the VMS Message utility so that meaningful text messages can be produced. The messages defined here tend to be of an informational or error nature and only when a severe (fatal) error is reported from VMS does this process top. The error log file contains all the information available about the failure to allow remedial action to be performed. See the section, below, for a list of all messages that this process can generate.

Logging to a file is also available by setting the configuration data file to record activity. This provides a file (ecc$dir:ecc.log), which shows the activity of the process for the logging period. It is recommended that under normal operation, this activity should be disabled. When diagnostic information is required, this facility should be used.

A5.2 UNIX Error Processing

All efforts have been made to make the UNIX environment functionally equivalent to the VMS environment. Routines have been written so that near identical error handling is available. All errors described in Section 4.3 , Data Segmentation, Page28 below are available and are also reported to the user.txt file as described above. A diagnostic logging environment is also provided by setting the appropriate field in the configuration file (/ecc_dir/config.dat) It is strongly recommended that in normal operation, this feature be disabled.

A5.3 Error messages

The following list of error messages can be generated by the host process and the severity of each message is indicated. Very often, such error messages are accompanied by extract error messages from the operating system, which provide system-level details of a p articular failure.

A5.3.1 User Process Errors

The following list of error messages can be generated by the user process and the severity of each message is indicated.

SEVERITY = SUCCESS

MORETOCOME	<not all specified events have been completed>
SUCCESS	<operation successfully complete>

SEVERITY = ERROR

ACTIVE	<crate controller has successfully reset>
ADDR	<Ethernet address of crate controller has changed>
ALLOC	<failed to allocate memory for operation>
ASRQS-FAILURE	<unable to assign queues for processing>
BADFRAME	<inconsistency in chain of buffers detected>
BADPARAM	<bad parameter value specified in data exchange>
CTRL-Y-ASS	<failed to assign channel for CTRL-Y trapping>
CTRL-Y-FAIL	<failed to disable CTRL-Y trapping>
CTRL-Y-AIO	<QIO failed; unable to catch CTRL-Y>
DEAD	<crate controller not responding>
FILE	<unable to access specified file>
GETPID-FAILURE	<unable to get PID to reserve Access Table>
HOST-BUSY	<ECC host process busy>
INVARG	<invalid argument passed in routine call>
LLC3-FAILURE	<connection to the ECC has failed>
LOCK-FAILURE	<failed to get lock ECC$LCK>
NO-EF-ALLOC	<no event flags available>
NO-GBL-SEC	<global section ECC$GBL does not exist>
NOSUCH	<specified event identifier is unknown>
NOTINIT	<user process not initialised via CCINIT()>
RESET	<crate controller is resetting>
TIMEOUT	<timeout during I/O with CAMAC device>
UNKNOWN-CMD	<ECC command is unknown>
UNKNOWN-CRATE	<specified crate is unknown on the ether>
UNLOCK-FAILURE	<failed to release lock ECC$LCK>

A5.3.2Manager Process Errors

The following list of error messages can be generated by the host manager process and the severity of each message is indicated.

SEVERITY	=	INFORMATIONAL
NOLOCK		<the lock ECC$LOCK has not been granted>
SEVERITY	=	WARNING
ETHERR		<the Ethernet device reported a (non-fatal) error>
ETHREAD		<failed to issue Ethernet read request>
ETHSTRT		<failed on ether startup>
ETHWRIT		<failed to issue Ethernet write request>
INITIAL		<failed to initialise ECC host process>
SEVERITY	=	ERROR
ASCEFC		<unable to associate to CEF cluster>
BUFFERS		<failed to initialise buffers>
CRMPSC		<failed to create global section>
EFCLEAR		<failed to clear event flag>
EFREAD		<failed to read event flags>
EFSET		<failed to set event flags>
ETHER		<failed to initialise Ethernet>
ETHASS		<assign fail on ether startup>
ETHFATAL		<the Ethernet device driver reported fatal error>
ETHGDVI		<getdvi failure on ether startup>
ETHIDEV		<invalid device for ether startup>
ETHIOS		<iosense mode failure>
ETHLEN		<invalid length of frame specified>
DGBLSC		<unable to delete global section>
LLCRPV		<LLC type 3 receive protocol violation>
LLCTPV		<LLC type 3 transmit protocol violation>
NOBUFFER		<no buffers available>
PID		<unable to get UIC/PID>
QUEUE		<queuing operation failed>
READQ		<failed to read input queue>
RTIMER		<failed to restart timer>
TIMER		<failed to start timer>
UNLOCK		<error unlocking ECC$LCK resource>
WAIT		<failed in system service wait>

SEVERITY	=	SEVERE (all relate to the configuration data file)
DREADS		<the driver read are incorrectly specified>
DRIVER		<the driver name is incorrectly specified>
FAPMAULT		<FAP multicast incorrectly specified>
NBUFFS		<the number of buffers is incorrectly specified>
NLOG		<the logging switch is incorrectly specified>
NTPMULT		<NTP multicast incorrectly specified>
SAP1		<LSAP value not read or incorrectly specified>
SAP2		<LSAP value not read or incorrectly specified>

A5.3.3ECC 1365 Controller Errors

The following list of errors can be generated by the Hytec ECC 1365 module and the severity of each message is indicated.

SEVERITY	=	SUCCESS
SUCCESS		<Function performed OK>
SEVERITY	=	INFORMATIONAL
NOTQ		<Q missing during operation>
NOTX		<X missing during operation>
NOTQX		<Q and X missing during operation>
SEVERITY	=	ERROR
FAILURE		<general failure>
QWASCLR		<Queue was empty>
ERP-ACCEPTED		<ERP request accepted>
NOBUFFS		<Not enough buffers on queue to satisfy request>
BADPARAM		<error found when encoding / decoding a parameter>
BADSEG		<bad segment construction>
SEG COMPLETE		<buffer segment building complete>
PROMISCUOUS		<booking request failed - marked as promiscuous>
UPDATE-PROM		<promiscuous flag set>
BAD-CMND		<error decoding ECC command>
DUP-CRATE		<duplicate crate address seen on Ethernet>
ERP-REQUEST		<reset requested via ERP>
HOST-FULL		<Host table full>
FAIL SECURITY		<Host request failed security>
LAM ATTACHED		<LAM already attached>
MOD-BOOKED		<Module booked to another host>
TRAP_68901		<bad 68901 interrupt>
TRAP_POWER		<power fail interrupt>
TRAP_BUS		<bus error interrupt>
TRAP_ADDRESS		<address error interrupt>
TRAP_DIVIDE		<zero divide interrupt>
TRAP_CHK		<CHK instruction interrupt>
TRAP_TRAPV		<TRAPV instruction interrupt>
TRAP_PRIV		<Privileged instruction interrupt>
TRAP_TRACE		<Trace interrupt>
TRAP_BAD		<General bad interrupt>
TRAP_TRAP		<TRAP instruction interrupt>

SEC_BADREQ	<bad security table update request>
SEC_FULL	<Security table full>
NO_SBLOCK	<no stored block to which to chain>
BAD_COR	<bad COR requested>
USER_RESET	<User requested reset>
INV_IMMEDIATE	<command invalid in immediate response mode>
BAD_CAMAC	<bad CAMAC operation requested>
DOWNLOAD_LOCK	<download already in progress for another user>
DOWNLOAD_DATA	<error in download data>
DOWNLOAD_FULL	<Not enough memory for download request>
NO_MEMORY	<Not enough memory for getmem() request>
CAMAC_NOTX	NOT X seen during CAMAC operations (warning)
CAMAC_NOTQ	NOT Q during CAMAC operation
CAMAC_NOTQX	NOT QX during CAMAC operation
BAD_VERSION	Firmware/host version mismatch
UNKNOWN	<unknown error code returned>

Note: Error codes produced by the firmware that are displayed on the front panel (e.g. crash codes) are listed in table12 on page 51.