NEW EXECUTIVE FEATURES (SERIES E)

The Series E operating system is to be released soon. There are
several new features and changes in the EXEC. There are three
catagories of features: those for all users, those for account
supervisors, and those strictly for Tymshare people. Before
releasing any of the new features in the first two catagories
to any of your customers, please check with your manager to see
if the specific feature has been announced by Corporate Marketing.
You should, of course, make it a point to tell your customers
about the changes that affect their current knowledge and use of
the system. The third catagory of features are for your own use
only.

FEATURES FOR ALL USERS

1. Large File Directories

The number of files that can be put in a given directory is no
longer limited. The EXEC message, TOO MANY FILES DELETE SOME
BEFORE LOGGING OUT is really dead and buried. Amen! Hallelujah!

When a user logs in, he is automatically given the ability to
add approximately 20 files to his directory. After these files
are added, he will get the following message when trying to create
the next new file:

NO. OF FILES QUOTA EXCEEDED
ERROR. TYPE TO

The new file he was attempting to create will not be saved if he
logs out at this point. However, he is given a chance to write
the information on an old file. (This is an excellent reason for
keeping a scratch file in your directory.) If he logs out and
logs back in he will be able to add another 20 files to his direc-
tory.

2. Writing On Shared Files

It is now possible for users to write on files in other directo-
ries if the owner of the file gives permission. He can do this
with a new option at the end of the DECLARE command, under the
PUBLIC heading. The option is called, WRITE ACCESS. As in pre-
vious systems, a Y answer to PUBLIC? allows all users within the
same account who know the owner's user name and the file name to

read this file. If no further declaration is done, the file still cannot be written upon by other users. However, if under the PUBLIC options, the WRITE ACCESS? question is answered with a Y, the file can be written upon by other users within the account. Any user in the account who knows the owner's user name and the file name can write on this file. A user with access to the directory (such as the Account Supervisor) can also delete such a file.

It is illegal to use the account number to refer to a shared file that can be read or written upon within the account only. The reference must contain only the user name.

Example:

-COPY TELETYPE TO (A4HARRY) /DATA/

is illegal if /DATA/ can be shared only within the account.
The correct form is:

-COPY TELETYPE TO (HARRY) /DATA/.

Harry would have declared the file PUBLIC with WRITE ACCESS. In Harry's directory this declaration will be indicated as follows:

R/W YES, WT SYM /2/25 1 1536 /DATA/

So that a file can be written on by those outside the account, they first must be able to read the file. This is done in the usual manner with @ or control characters.

Please refer to the enclosed FILE ACCESS CHART for information on the ability of the different types of users to access files with various attributes.

3. Moving Shared Files From One Directory To Another

With the Series E system, it is possible to move a shared file from one directory to another without incurring system overhead. The result of moving a file in this manner is the same as copying it into the new directory and deleting it from the old directory. The EXEC command RENAME can now be used to move shared files as follows:

(a) Any file which the user can read can be moved to his own directory with the following command:

   -RENAME (JONES)ABC AS MYFILE (cr)

(b) Any file owned by the user can be moved to any directory
     that is set to accept new files. Use the following command:

     -RENAME MYFILE AS (Z9HARRY)ABC

(c) Any file which the user can read can be moved to any directory
     that is set to accept new files. For example;

     -RENAME (Z9HARRY) @ABC AS (A1GEORGE)DEF

4. Private Files

The owner of a file directory has more privacy for his files than
in previous systems. Unless declared otherwise, all files are
protected from everyone else on the system, including users with
Account Supervisor, Subsystem, System, Operator, or Executive
status. This protection is accomplished by restricting the
following EXEC commands and functions to only the owner of the
directory; that is, only to the user who can log in to the direc-
tory as follows:

Any write access to an old file.

DECLARE

DELETE

INIT

REMOVE

In other words, a file is now write protected, by default, against
anyone but its legal owner.

5. Initialized Files

Existing initialized files are turned off by the Series E systems
upon transfer from a Series D system. The files must be re-
initialized in the new system.

6. EXECUTIVE Command Name Changes

EXEC command and subsystem names must not be abbreviated shorter
than the first three characters. The exceptions are FI and the
two-letter commands like GO. This change increases the speed
and efficiency of the Tymshare EXECUTIVE.

7. File Names

The new file name conventions, documented in Technical Notes number 3, are in effect in the Series E systems.
(NOTE: several examples in Technical Notes number 3 showed commands abbreviated shorter than three characters. This is no longer permitted.)

8. File Numbers

An additional column at the left of the DIRECTORY listing contains the file number. These numbers can be called by the REMOVE command and the new options on the files and DIRECTORY commands (see 10 below).

9. New Command

A new EXECUTIVE command, LAST, gives the number of the last file in the directory.

10. New Options On FILES And DIRECTORY Commands.

To aid searching large file directories, a new option has been added to the FILES and DIRECTORY commands. The option allows listing a directory from a given file number to the end of the directory. With the FILES command the option may be used with any of the normal Line Feed options.

Example:

-LAST (cr)
28

-FILES, 25 (cr)

will list the last four files in the directory.

11. File Directory Controls

A new EXEC command, FDC, allows the owner of a directory to place certain controls on his file directory. Normally, the directory is:

(a) SHAREABLE

This means anyone with GFD status can obtain a copy of the directory.

(b)   LISTABLE

This means that anyone who can obtain a copy of the directory can use the FILES and DIRECTORY commands.

(c)   NEW FILES

This means that anyone who knows the Account Number/User Name identification of the directory can add new files.   GFD status is not required.

The FDC command lets the owner change any of the above states.

Examples:

(1)   -FDC
      SHAREABLE?Y
      LISTABLE?Y
      NEW FILES?N
      -

(2)   - FDC
      SHAREABLE?Y
      LISTABLE?N
      NEW FILES?Y
      -

(3)   -FDC
      SHAREABLE?N
      NEW FILES?Y

NOTE: If a directory is not SHAREABLE it cannot be LISTABLE, but it can still be set to accept NEW FILES.

Another new EXEC command, PFDC, will print the state of the file directory controls.

Example (Refer to example 1 above):

      -PFDC
      SHAREABLE LISTABLE
      -

FEATURES FOR ACCOUNT SUPERVISORS

1. User File Security

The following EXECUTIVE commands cannot be used by the Account
Supervisor if he uses GFD to access a user's directory:

DECLARE

DELETE

INIT

REMOVE

Also, he cannot write on an old file in the directory if it has
not been declared PUBLIC, WRITE ACCESS by the owner.

2. Multi-User Directories

More than one user can use the same file directory at the same
time in the Series E system. An Account Supervisor can use GFD
to obtain the directory of one of his users whether that user is
logged in or not. If the user is logged in, the Account Super-
visor will no longer get the message ALREADY ENTERED when he does
GFD. The Account Supervisor will gain access to the directory
while the user retains his access to it. Assuming that the
Account Supervisor has WRITE ACCESS to a file, the user and the
Account Superviosr will <u>not</u> both be able to write on the same
file at the same time.

The printout from the WHO command is now different after a GFD.
The first line will show the terminal number, account number,
and user name that was logged into. A second line has been added
to show the account number/user name identification of the file
directory obtained by GFD.

Example:

-WHO

15   Z9JONES

20*   Z9 BIG SHOT

 Z9   JONES

-

FEATURES FOR TYMSHARE USERS ONLY

1. Status Controls

For improved system security, a new set of status controls has been implemented.

(a) User status types

These status types are assigned to account number/user name identifiers. They are called:

(i)   User status

(ii)   Account supervisor status

(iii)   Peripheral status

(iv)   CBl status

Every user automatically gets User Status. The others can be assigned independently in any combination to a user name.

(b) Fork status types

These status types are assigned to programs. They allow the programs to obtain higher status than the user status types for the duration of execution.

See the enclosed charts on EXEC commands for information on what can be done with various levels of status.

2. Machine, System, And Version Numbers

The EXEC command, SYSNO now prints the machine number in addition to the Monitor and EXECUTIVE version numbers. To obtain version numbers of current subsystems, type:

-1V (cr)

3. File BRS Additions

Six new file BRS's have been added. They are:

BRS 62 Replaces 15 and 16
BRS 63 Replaces 18 and 19
BRS 64 Replaces 48 and 16
BRS 65 Replaces 60 and 19
BRS 68 Returns file name string pointer and file parameter
BRS 69 Delete file

These BRS's are documented in a recent supplement to the BRS
Reference Manual, and are included in the most recent printing
of this Manual as Pages 2-2A and 2-2B.

Tom Manuel

FILE ACCESS CHART

File Attributes	ACCOUNT				GLOBAL								
	Owner	User Status	Account Supervisor		User Status	CB1 Status	Subsystem Status	System Status		Operator Status		Executive Status	
			Normal	GFD				Normal	GFD	Normal	GFD	Normal	GFD
DECLARABLE	Y	·	·	·	·	·	·	·	·	·	·	·	·
DELETEABLE	Y1	·	·	·	·	·	·	·	·	·	·	·	·
REMOVABLE	Y	·	·	·	·	·	·	·	·	·	·	·	·
RENAMEABLE	Y	·	·	Y	·	·	·	·	Y	·	Y	·	Y
INITIABLE 2	Y	·	·	·	·	·	·	·	·	·	·	·	·
PRIVATE Writable 2	Y1	·	·	·	·	·	·	·	·	·	·	·	·
PRIVATE Readable	Y	·	·	Y	·	·	·	Y	Y	Y	Y	Y	Y
PUBLIC Readable 3	Y	Y	Y	Y	·	·	·	Y	Y	Y	Y	Y	Y
PUBLIC Executable	Y	Y	Y	Y	·	·	·	Y	Y	Y	Y	Y	Y
PUBLIC Writable	Y	Y	Y	Y	·	·	·	Y	Y	Y	Y	Y	Y
GLOBAL Readable 3	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
GLOBAL Executable	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
GLOBAL Writable	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

NOTES

1. A file must have private writability to be deleteable by the owner.

2. A file that is initialized is not writable. It is deleteable.

3. To make a global file globally writable it must be declared public writable.

EXEC COMMANDS REQUIRING STATUS

Status / Executive Commands	Account Supervisor Status	CB1 Status	Peripheral Status	Subsystem Status	System Status	Operator Status	Executive
ANSWER 1	.	Y	.	.	Y	Y	Y
CRASH	.	.	.	.	.	Y	Y
DISABLE	.	.	.	.	.	Y	Y
ENABLE	.	.	.	.	.	Y	Y
GFD 2	Y a				Y g	Y g	Y g
HANG 1	.	.	.	.	Y	Y	Y
LETTER	.	.	.	.	.	Y	Y
LOOK	.	.	.	.	Y	.	Y
PSP	.	Y	.	.	.	Y	Y
SHUT 1	.	.	.	.	.	Y	Y
SMT	.	.	.	Y	.	.	Y
SDP	.	.	.	.	.	.	Y
SLD	.	.	.	.	Y	Y	Y
SYSND	.	Y	.	.	Y	.	Y
TIME 3	Yr	Yr	Yr	Yr	Yr,c	Yr	Yr,c
UP	.	.	.	.	.	Y	Y
USERS	.	Y	.	.	Y	Y	Y
WHERE	.	Y	.	.	Y	Y	Y
WHO 2	Ya	Yg	.	Yg	Yg	Yg	Yg

NOTES

1. Execution of these commands requires setting breakpoint switch 1.

2. a = account only
    g = global

3. r = real terminal time
    c = compute time

EXECUTIVE COMMANDS THAT ALL USERS CAN EXECUTE

1. BRANCH   Branches into a program.

2. COMMANDS   Commands from specified file.

3. CONTINUE   Continues running a subsystem.

4. COPY   Copies file to file.

5. DATE   Types date and time.

6. DECLARE   Sets file controls.

7. DELETE   Deletes file.

8. DIRECTORY   Types file directory with all parameters.

9. DUMP   Dumps all program, saves status.

10. EXIT   Allows logout without writing file directory.

11. FDC   Sets file directory controls.

12. FILES OR FI   Types file directory.

13. GO   Goes to a GOTO type program.

14. INIT   Sets up initial start-up file.

15. KILL   Kills program relabeling only.

16. LAST   Types position of last file in directory.

17. LOAD   Types loading factor.

18. LOGOUT   Logs user out.

19. MAIL   Types all mail in a user's mailbox.

20.	MEMORY	Types unused portion of user's memory.
21.	OPERATOR	Sets operator status.
22.	PLACE	Places a SAVE type program in user's memory.
23.	PFDC	Prints file directory controls.
24.	PMT	Prints a user's pseudo-memory table.
25.	PROJECT	Writes accounting, changes project code.
26.	RECOVER	Recovers from a dump file.
27.	RELEASE	Releases a subsystem.
28.	REMOVE	Removes a file from the directory.
29.	RENAME	Renames a file.
30.	RESET	Returns all of user's memory.
31.	RUN	Does RECOVER followed by CONTINUE.
32.	SAVE	Saves program, creates GO type file.
33.	SEND	Allows user to send a letter.
34.	SETEXEC	Sets job status.
35.	STATUS	Types user's memory status.
36.	TIME	Types real time used.
37.	WHO	Types terminal number and user name.