CC-209

COMPUTATION CENTER
Massachusetts Institute of Technology
Cambridge 39, Massachusetts

May 14, 1963

TO: Limited Distribution

FROM: R. C. Daley and F. J. Corbató

SUBJECT: Use of the Memory Protection and Relocation Mode within the MOD.10 Time-Sharing System.

INTRODUCTION

This memo will discuss the usage of the Memory Protection and Relocation devices (RPQ no. E07291) as implemented in the MOD.10 Time-Sharing System. This Time-Sharing System must be able to process jobs inititated from one or more typewriters as well as jobs inititated through a restricted version of the Fortran-Fap-Mad Monitor System (FMS).

This type of processing requires that a supervisory program, TSS (Time-Sharing Supervisor), be in core at all times to handle such problems as Scheduling, Time Accounting, Input-output, etc. TSS utilizes the memory protection and relocation devices to protect itself from outside interference and to facilitate the moving of a typewriter-initiated program currently working in one block of core memory to another block of core memory where it may continue to run without adverse effect. Since several typewriter-initiated programs may be in core memory at once, memory protection also serves to eliminate the possibility of one program interfering with another. TSS is considered to be the only completely debugged program in the system and therefore is the only program that does not run in the protection mode. TSS for MOD.10 occupies the lowest 6144 registers of core memory and maintains complete control over both FMS and typewriter-initiated jobs.

SUBROUTINE LINKAGE

Typewriter-inititated programs are always run with a relocation greater than zero and which is equal to the setting of the lower bound of the protection indicators. Since no program can be 32,768 words long, this means that a memory reference to -1 when relocated will always produce a lower bound violation and a memory protection trap. With this rule in mind a standard calling sequence has been arrived at by which typewriter-inititated programs can reference system subroutines located in TSS. The following example demonstrates a typical calling sequence:

```
          TSX SUBR, 4
          ...          parameters if any where SUBR is located
```

within the user's program in the form:

```
          SUBR TXI  -1,, LSUBR.
```

LSUBR is the location of a word containing the BCD name of the desired subroutine, left adjusted, such as:

```
LSUBR BCI 1,READ
```

After execution of the TSX instruction the TXI instruction will cause a protection trap to TSS. TSS will locate the subroutine name in its subroutine table and transfer control to the appropriate location. Since TSS and its subroutines must operate out of the protection and relocation modes, the subroutines must first relocate the addresses of any parameters and check for memory protect violations. If a typewriter-inititated program causes a memory protection trap which is not found to be a subroutine call, it is treated as an error and the job is terminated with a diagnostic. A BSS loader can be made to insert the correct subroutine linkage to TSS.

PROTECTION TRAP INTERPRETER

Due to the need for using FMS (and other standard systems) to run with the Time-Sharing System, an interpreter has been written to process FMS instructions which violate the protection mode rather than rewrite FMS to use TSS subroutines. FMS runs in the protection mode, but unlike typewriter-inititated programs it has a relocation of zero making it effectively absolute. The interpreter can analyze and effectively execute all of the violating instructions with the exception of LPI, LRI, LCH, ECTM, ESNT, ESTM. In its present state the interpreter will not execute ETM, RCT, or ENB but at a later date these may be added.

In addition to interpreting operation codes that violate the protection mode, the interpreter must also allow FMS to make use of the floating point and STR traps. Since references to the location associated with these traps (locations 0, 2 and 8) produce a lower bound violation, the interpreter must process all attempts to reference these locations. Since any trap will inhibit I/O traps and cause the computer to leave the protection and relocation modes, FMS can not be allowed to use traps directly, as this would leave TSS unprotected after a trap had occurred. For this reason all trap locations are permanently set to transfers to locations within TSS. When FMS attempts to set a trap location, the address is merely saved internally to TSS, and when the trap does occur the address will be used as the return location after TSS has reentered the protection and relocation modes. FMS is allowed however to reference location 0 directly, but of course still through the interpreter. At present the interpreter will allow only the following instructions to reference the trap locations, but it may soon be expanded to handle all possible combinations:

```
STZ  0
CLA  0       or 2 or 8
CAL  0       or 2 or 8
STO 2        or 8
SLW  2       or 8
STA  2       or 8
```

The remainder of the interpreter concerns the interpreting of all instructions which reference the input-output equipment or the associated indicators (redundancy, EOF, etc.). These instructions must be processed by the interpreter to insure that TSS is not affected by their execution. The following is a list of restrictions that must be observed to insure that the I 10 operation will be correctly interpreted:

1. Load Channel instructions are not permitted;

2. If a Reset and Load Channel is to be given in conjunction with a read or write select, it must be given immediately following the select instruction. The only exception to this rule is that up to 3 SPR, SPU, or NOP instructions may occur between the select and the RCH instructions;

3. Input-Output commands (except for those in the non-transmit mode) may not contain a word count greater than the 2's complement of the starting location since a larger count will allow writing of lower memory. For example, the command;

```
        IORT x,, -1
```

   would have to be replaced by;

```
        IORT x,, - x
```

4. No reference can be made to any I/O unit not assigned by TSS for the use of FMS. At present the following I/O units are available for use by FMS:

   I. Card reader, Printer, Punch channel A or B

   II. Tapes 1-7 channel A or B

The Interpreter checks all input sequences to insure that TSS is not overwritten. In the simple cases the Interpreter will simply check the starting address and the word count of the input command. Some command sequences however, cannot be checked, for example:

```
        IOCP   * -1,,1
        PZE    **,,**
```

If the channel operation is not completely defined in one command (e.g. IOCD, IORT, IOST, IOCT) the Interpreter executes the slect and the RCH instruction and goes into a Store Channel loop until the input operation is complete. In this Store Channel loop the contents of the channel address register are continuously checked for a memory protect violation and if this is discovered the channel is reset before any damage is done. If the channel is operating in the non-transmit mode, violations will be ignored. No attempt is made to check output command sequences.

MEMORY PROTECTION WITH 2 CORE MEMORIES (RPQ NO. E02120)

With the additional core memory, most existing systems can be run, without extensive modification, with the Time-Sharing System in place of the restricted FMS. This will be accomplished by running the existing system in core memory B and TSS, which will process all traps, in core memory A. TSS will simulate DATA Channel and Interval Timer traps for the system running in core memory B. Data Channel traps may be controlled by the B-core (Background) system with the use of the ENB and RCT instructions as described in the 7090 reference manual. Although the actual trap will occur in memory A, TSS will transfer control to the corresponding "Trap" location in memory B after processing. The Background system will now be able to reference every location in memory B.

The Background system must, however, be reassembled for the insertion of a bit in position 20 of all channel commands so that the Command Word and Data Word control indicators will be set for reference to memory B. Computation Center memo CC-202-1 contains a guide for modifying existing systems to run with the Time-Sharing System.