DESIGN CONCEPTS FOR A HIGHLY RELIABLE MULTIMICROPROCESSOR SYSTEM FOR COMMUNICATION SATELLITES

Francois PLISSON
Digital System Department
MATRA S.A. (FRANCE)

Summary. - Over past years, the microprocessors have been used widely and efficiently for many applications. Some of them have become industrial standards, and the question arised how to use them most efficiently for space applications. The paper describes the design concepts which have directed the study and the breadboarding of a trimicroprocessor system and its monitoring software. These concepts have been traded off for reaching a high system overall availability and flexibility. The multiprocessor is organized around C-MOS microprocessors and a time shared/common bus, designed for reliable operations. The monitoring software is especially developed to yield a triple redundancy for critical (i.e. mission success dependent) software functions and to assure the mutual failure independency of the application programs.

On board telecommunication satellites, the multiprocessor structure have been found better suited for reliability, probability of mission interruptions and its capability of degraded operation when it was compared to a classical stand by redundant monoprocessor array. At the end of the year, the triprocessor system will be integrated into a satellite attitude control simulator for a system closed-loop test with an air bearing table and actual satellite equipments.

Introduction. - The availability of large integrated digital circuits is changing the mind of design conceptors for satellite control systems. While the communication satellites become bigger and more sophisticated their critical functions must rely on complex but high reliable control hardware. Structures which have been only used in the past for large ground computing systems, are now foreseen for on board applications. Their intrinsic qualities offer a good approach for reaching overall system reliability and decrease probability of mission interruptions. These concepts have been implemented, using three CMOS microprocessors, connected in a multiprocessor structure. The hardware and software structures have been designed simultaneously for yielding a triple redundancy for critical system functions. For purpose of faults detection and to avoid faults propagation, the concept structurizes the software programs and the hardware detection devices. The goal was to assure the mutual failure independency of the application programs.

The multiprocessor hardware have been breadboarded and the monitor software programs have been developed and tested. In parallel the global reliability and disponibility of the system have been estimated and trade off were performed. Part of a continuous effort for developing new satellite attitude control structures, this multiprocessor is tested with attitude control laws for communication satellite station keeping.

1) **Design goals -** For meeting the space requirements, the on-board control system must offer at least the following characteristics

- a high degree of overall system availability/reliability
- be flexible for user's needs adequation and graceful degraded operations
- use of proven technologies for space applications
- be easy to program and provide a large range of development aids for minimization of design errors.

The trade off we made for the definition of the best suited system led us to a multi-microprocessor structure. We shall describe it latter on so let us first discuss the four design leading keypoints we have already set up.

1.1.1. Any high availability system design is based on four concepts

- analysis and recoverability : ability to detect errors and to minimize their impact into the system
- modularity : provisions for isolatable and assignable elements
- configurability : reconfiguration or exchange of modules in face of detected errors
- continuity of operations : smooth reconfigurations quickly performed.

1.1.2. The flexibility of a space system may be understood as a design concept which assures its perinnity, but also as a feature which allows an easy reconfiguration and graceful degraded operations.

Both concepts are complementary : the system can be modular and reconfigurable.

Modular : as the number of models built for a given space application is generally limited and the requirements vary from one project to the next one.

Adaptable : the modularity can be exerciced during flight.

1.1.3. The requirements for proven technologies are well known in space business.

They stem from all the experiences accumulated during the past decade on parts and materials. These technological data are used for building up a reliability model from which one can derive the expected time life of the system, with some degree of confidence.

1.1.4. The reliability of a system depends directly from the methodologies followed during its development. The sophistication of the tools used by the designer have a direct impact on the development time but also on the formalism and the structurization which help for avoiding bugs. The architecture of the system itself impacts the development tools, by providing inner test facilities or easy test interface. These statements are particularly applicable to software programs writing and integration.

2) **The core structure -** The core structure is built around three microprocessors which are in active redundancy. But the concept can accomodate more processors, when operational constraints require it.

The processors share the computing load between them. They are organized around a time shared/common bus. The bus is especially designed for reliable operation. It allows the connexion of various kinds of units and it provides for them timing and exchange procedures. The system expansion or the modifications for user's needs adequation are easy to achieve.

Connected to the bus are :

- three identical microprocessors with local memory, real time clock and bus interface control
- the system memory for storage of system level data
- up to six user's memories block of 4K x 12 bits words
- input/output couplers for interface with system devices
- external interrupts input registers.

The three processors work simultaneously. The memory access time being four times shorter than a microprocessor elementary sequence, the processors work almost as if they were alone with the memory.

The software tasks are not dedicated to any processor. The processors are symmetrical. Every processor can be equally effective in executing the tasks.

The instruction codes are located both in the local memory and in the user's common memories. The system programs which are the most often run (scheduling sequence, interrupt monitor or general purpose subroutines) are stored in the local memories. The user’s program (which are mission dependent) are located in the user’s memories.

For a reliable software, the programs are functionnally structurized and implemented. The design goal has been to split the user’s tasks into independent sections which do not rely on other non redundant tasks. The structure handles software parallel processing chains, in a way similar to conventional dedicated hardware chains.

The failure of one or two processors degrades gracefully the performances but it does not affect the completion of the mission functions. The failure of one memory chip involves only the user’s program stored in it, i.e. only one or a few functions (if they are not elsewhere redunded) are lost but the overall system is still operative. Reconfigurations are performed through software error recovery sequences.

It has been made a maximum use of the processors to control the peripheral devices. The saving in hardware parts is significant and it will increase the overall system availability.

3) **The performances** - The performances must be analysed in terms of efficiency and availability.

The efficiency depends on

3.1. Computing power

- average instruction time 2,3 µS
- instruction set of the PdP8
- memory capacity up to 32K words of 12 bits.

3.2. Flexibility : user’s needs adequation

- modular interfaces : parallel I/O, serial I/O, DMA, interrupts, CAD, CDA, teletype writer, real time clock, etc...
- powerful I/O instructions (I/O status skip ...)
- very low power consumption (CMOS parts)
- full military temperature range
- adaptable computing power, regard to mission phases by powering off one or two processors and memory blocks
- powerful and versatile operating system.

3.3. Development aids

- structurized software for true modular programming
- use of PdP8 basis software
- automatic test of software module chain by Petri net algorithms
- development tools from Intersil : the intercept integrated in the test rack
- cross assembler on host computer with disk system

3.4. Maintenance

- modular design
- standard connection to the common data bus of the memory blocks and I/O units
- structurized software offers software modules independence
- a picture of the system status is located in the system memory and can be transmitted on demand
- the bus access and the system memory are controlled by watch dogs and semaphores, system data are monitored for min and max values
- self test programs are periodically run and when the processors are idle
- after failure detection, test and recovery programs analyse the defective sequence and look for reconfiguration
- the test bench provides full test capability for the processors.

3.5. Availability

- space qualified or potentially qualified highly reliable parts
- the system structure has been designed for high availability
    - critical hardware units are redunded
    - failure detection has been carefully studied
    - reconfiguration and isolation of the defective units
    - structurized software for independence of tasks and easy reconfigurations and tests
    - the supervisor and critical programs are duplicated in the three processor local memories
    - the failure of one processor degrades gracefully the system performances
    - provisions are made to avoid software error propagations.
- low probability of mission interruption after failure
    - recovery time minimized
    - degraded modes of operation.

4) **Availability estimates for a telecommunication satellite** - The estimates have been computed for a 7 years mission duration. The reliability figures, which were not available from test life results were taken off the European Space Agency Specification QRA 14-ECS Issue I.

Parallel evaluations were performed on both a standard single microprocessor system with cold and global redundancy and the trimicroprocessor system with internal redundancies. The user's program memory was assumed to be 4K words in both systems.

The main results are about the reliability over seven years and the mission interruptions for a geostationnary satellite.

4.1. Reliability estimates

The summary figures are quoted for three multiprocessor configurations, i.e. three processors, two or one processor available at the end of the mission.

- multiprocessor	3/3	0.485
	2/3	0.910
	1/3	0.988
- single processor with stand by redundancy		0.946

4.2. Mission interruption estimates

The mission interruption is defined as the elapsed time between the going out of the specifications at the event of a failure and the service re-establishment into the mission specifications.

The same philosophy have been kept for comparison between both single and triprocessor systems

- on failure detection, the microprocessor is halted
- the hardware reconfiguration (add on of idle units) is telecommanded from the ground.

At a failure accurence, the trimicroprocessor system is still available but with gracefull degraded performances. In the contrary, the switching into the halt state of the processor of a single processor system induces a mission interruption.

The probability estimates for having one or several mission interruptions over seven years are the following ones

triprocessor : 0,116
single processor, stand by unit : 0,307.

Conclusion. - A multiprocessor system offers the following advantages for a telecommunication satellite :

- a better reliability (0,987 versus 0,946) although the cross trap effects between memories is under evaluated for the multiprocessor due to the small retained memory configuration
- a better availability due to : the low probability (11,6 % versus 30 %) of mission interruption
- a gracefull degradation of the processing performances at the accurance of failures
- the possible adaptation of a multiprocessor system to the availability requirements of various missions
- a good safety ; it remains at least a processor (up to three processor failures) for controlling the system.

References

1/. J.E. Julinssen and F.J. Mowle, Multiple microprocessors with common main and control memories, IEEE Trans Comp, vol C22, Nov 1973, pp 999-1007

2/. J.L. Baer, Multiprocessing Systems, IEEE Trans Comp, vol C25, Dec 1976 pp 1271-1277

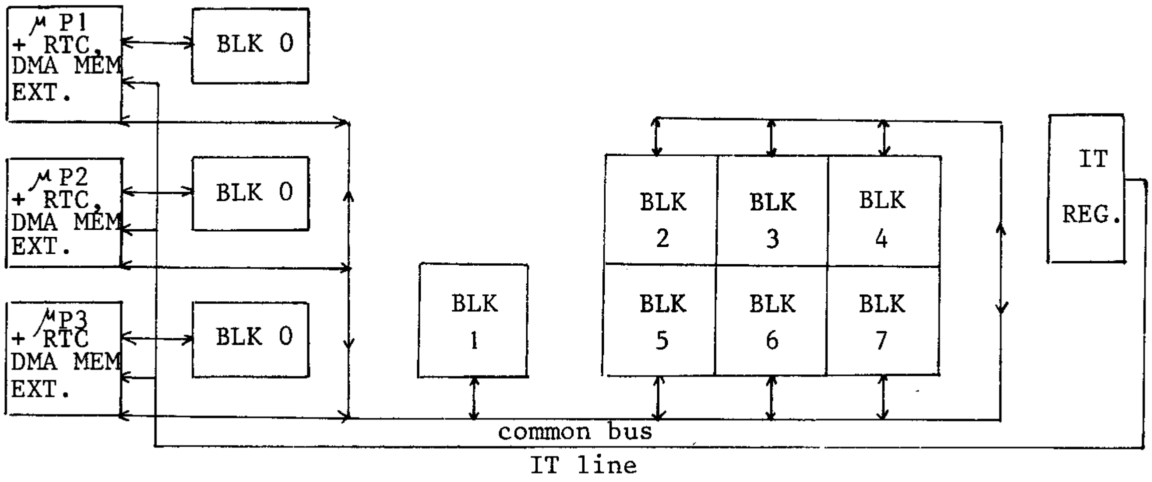
3/. A. Avizienis, Fault Tolerant Systems, IEEE Trans Comp, vol C25, Dec 1976, pp 1304-1311

4/. A.E. Cooper and W.T. Chow, Development of on board space computer systems, IBM J Res Develop, vol 20, pp 5-19, Janv 1976

5/. Philip H. Enslew Jr Editor, Multiprocessor and Parallel processing, Comtre Corporation

6/. Alan J. Weissberger, Analysis of Multiple Microprocessor system architectures, Computer Design, June 1977, pp 151-163

7/. D.P. Siewiorek, Multiprocessors : Reliability Modeling and Graceful Degradation, Infotech state of the art report, Berkshire (England), June 1977.

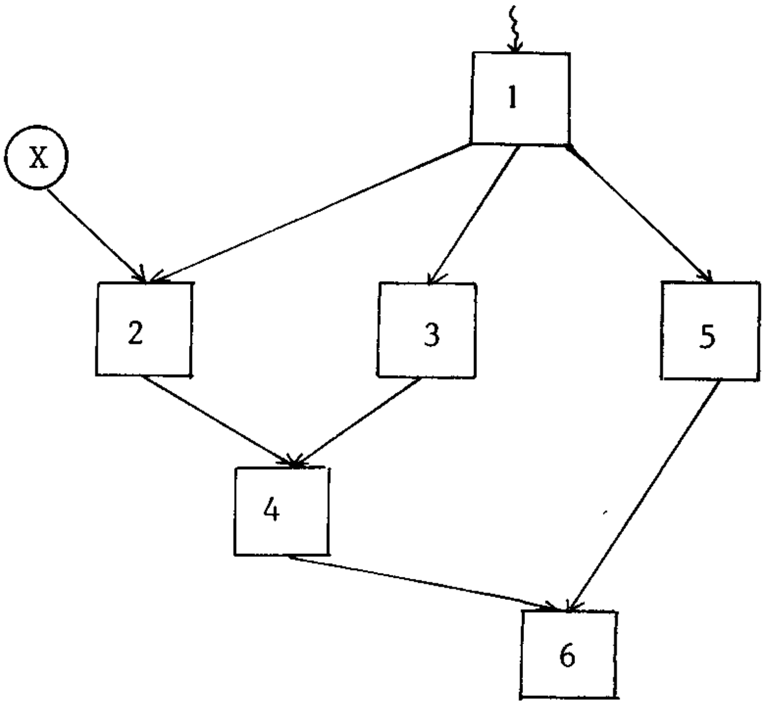


<u>Memory blocks function</u>:

block 0 : local - 3 identical blocks (ROM + RAM)
contains :
- supervisor programs
- general purpose routines (*, /..)
- local data

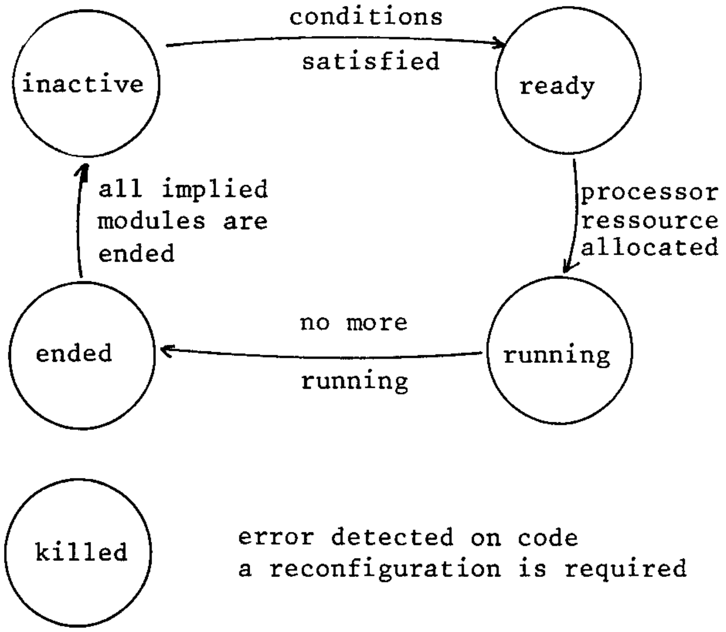
block 1 : common - RAM + PROM
contains :
- supervisor tables
- user's data
- initial values

blocks 2 to 7 : common - only PROM
contains :
- user's programs (these programs use block 0 RAM as temporary storage).



User’s tasks are organized in chains.
A chain is made of modules.
It is activated on an external event (interrupt, cyclic order).
“1” implies modules 2,3,5.
“2” depends on module “1” completion and data “X” ready.
A module can be run only when all its dependence conditions are satisfied.

A module can be :


inactive
conditions
satisfied
ready
processor
ressource
allocated
running
no more
running
ended
all implied
modules are
ended
killed
error detected on code
a reconfiguration is required