A FAULT-TOLERANT MULTI-MICROPROCESSOR ARCHITECTURE FOR SARGOS

Y. DESWARTE — Projet Pilote SURF, 7, avenue du Colonel Roche, F - 31400 TOULOUSE

J.L. BOSSEBOFUF — E.N.S.I.C.A., 49, avenue Léon Blum, F - 31056 TOULOUSE CEDEX

P. COHEN — Université Paul Sabatier, 118, route de Narbonne, F - 31077 TOULOUSE CEDEX

N. GARGIR & J. LEROUGE — C.E.I.S.- Espace, avenue de Larrieu, F - 31094 TOULOUSE CEDEX

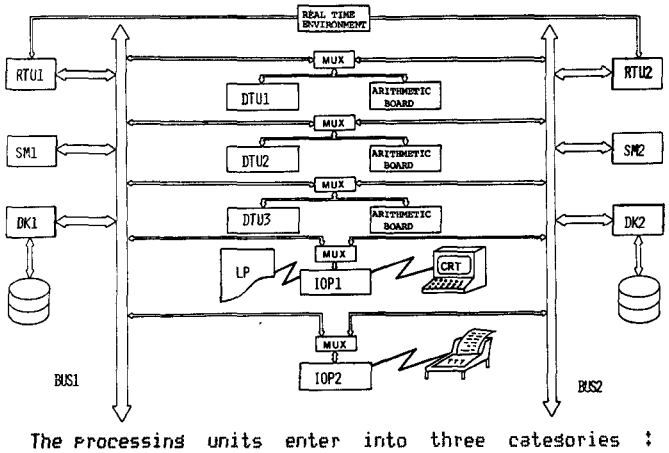
Introduction : System Requirements

The SARGOS system intends to identify and locate distress beacons by satellite. This paper presents the architecture of the data processing unit of the SARGOS Ground Stations. This data processing unit has been specifically designed to achieve the 99 % availability requirement with a long mean time to repair (MTTR about 100 h.) imposed by the fact that this kind of stations may be situated anywhere in the world.

Other requirements are :

- Since the ground station is to operate under human supervision, some simple manual reconfiguration can be contemplated.
- The loss of telemetry being considered as serious, data acquisition and antenna control must be carried out even if a failure has occured.
- Peripheral devices must have collective redundancy (teletypewriter and CRT keyboards, printer and teletype paper output).

Outlines of the Architecture



The processing units enter into three categories :

- Real-time units (RTUs)
- Differed-time units (DTUs)
- Input-output processors (IOPs)

Every one of those processing units is composed of a standard Intel 86/12 board. Each processing unit is connected to a standard Intel Multibus, but its local memory is large enough to carry out most of the processings with no interaction with other units. Consequently, in most cases, the processing unit can be isolated by means of software and/or hardware. This isolation is a way to avoid fast error propagation amongs the various units.

This study is supported by the Projet Pilote SURF under Grant No.80073.

Real-time processing units are doubled (RTU1 and RTU2). Throughout the transit of the satellite, each of these RTUs takes in charge the acquisition of the telemetry and the output of antenna control orders. Orders issued by both RTUs are compared by an external device. In the event of disagreement, the operator is alerted and a selection is automatically made between the two RTUs, the operator having the facility to change this selection manually. Throughout the transit, RTU software isolation from other units is secured.

At the end of the transit, data are saved on the two disks (DK1 and DK2) via the two multibus BUS1 and BUS2. These data are then processed in differed-time by non-doubled units (DTUs) : orbitography, beacons location, forecast of satellites transits, computation of control tables for the next transit, etc... During most of these processings, every DTU is isolated from the other units by its multiplexer (MUX). These processings involving mainly numerical computations, acceptance testing of the results and periodical testing of the processor hardware should set a satisfactory "coverage". Moreover, the DTUs check the consistency and identity of data issuing from the two shared memories (SM1 and SM2) as well as from the two disks. Then, permanent failures of one DTU will bring about throughput degradation but without any noticeable disturbance in the station.

Specific input-output processors (IOPs) are in charge of peripheral devices. Like the DTUs, IOPs have access to the shared memories and the two disks and use the same kind of testing.

Processors are not adressable, in order to get hardware modularity transparency for the software and to permit the isolation of the processors. Task creations and data exchange between units are done through the shared memories. A task is created by inserting a descriptor of this task in a queue associated with the set of material processors able to execute this task. Each idle material processor periodically consults the queue with which it is associated, and assumes the first elisible task.

Several detection means are provided :

- Run-time test program,
- Comparison between left and right copies,
- Max-times on tasks and locks,
- Watch-dogs on tasks,
- Acceptance tests by OS or application programs.

Automatic and manual rollbacks and reconfigurations can be carried on with no interference with application programs.

References :

J.L.BOSSEBOEUF, P.COHEN, Y.DESWARTE, N.GARGIR, J.LEROUGE "Une Architecture Multi-Microprocesseur Sûre de Fonctionnement pour SARGOS" (in French) Journées SURF 1981, 15-16 Janvier 1981, Paris, 18 pages