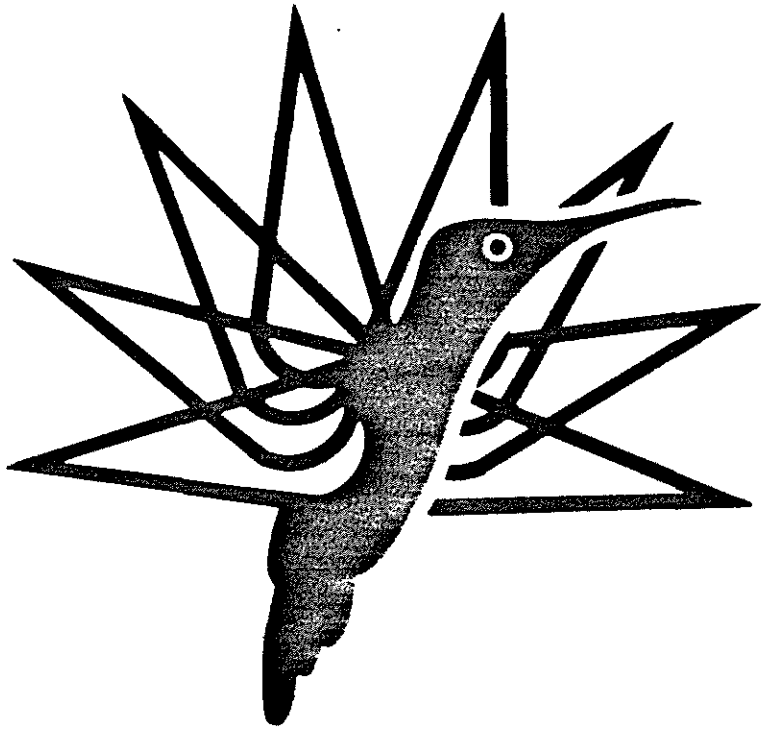
PAPER Nr. : 43



SAFETY ASPECTS IN STORES MANAGEMENT SYSTEMS

BY

F. CRISPOLTI and G. SCOTTI DI UCCIO

SELENIA Industrie Elettroniche Associate SPA
Avionic Systems
Pomezia - ITALY

TENTH EUROPEAN ROTORCRAFT FORUM
AUGUST 28 – 31, 1984 – THE HAGUE, THE NETHERLANDS

ABSTRACT

The operational requirements for a combact aircraft or rotorcraft, demand an high integrity system capable of managing and delivering weapons with the maximum efficiency, in terms of maximum success probability with the minimum crew workload. The introduction of complex Stores Management Systems (SMS) and complex weapons configurations pose safety problems that must be carefully considered in order to design systems whose main characteristics are reliability and safety.

This document outlines a general purpose SMS and defines the main reliability parameters. As a conclusion some system architectures are presented and discussed.

INDEX

1.0 INTRODUCTION TO SMS

2.0 SAFETY AND MISSION SUCCESS

3.0 SYSTEM ARCHITECTURE
3.1 Mono Channel System
3.2 Multi-Channel reconfigurable Systems
3.3 Communication Channels

4.0 CONCLUSIONS

1.0 Introduction to SMS

The most important role of a combact aircraft or of a rotorcraft is managing and delivering the carried weapons with the maximum efficiency, and, at the same time, assuring the highest safety grade.

With the production of more and more sophisticated aircraft and rotorcraft and the introduction of a great variety of complex weapons, the use of a Stores Managing System has become the only opportunity to ensure high success probability, without super work-load for the pilot, and no increase probability of generating events which could cause damage for the pilot, the aircraft or the friend theatre.

A typical SMS provides the selection, arming, release of the carried weapons and loads, (i.e. bombs, rockets, air to air missiles, air to ground missiles, torpedoes, sonobuoys, and so on) and provides the gun managing as well, if present. The system performs its functions by means of a control panel (multifunction or dedicated), under control of a computer (main or armament computer), that, generally, performs the weapon aiming calculations. However, the system is requested to have a reversionary capability in order to achieve its basical functions in case of failures of the computer or of its associated sensors.

The typical SMS provides also the jettison of loads, both in emergency (salvo) and selective jettison conditions.

The system provides the following facilities to the pilot or navigators:

- displaying the actual stores configurations;
- selecting, entering and recalling multiple attack packages;
- managing the delivery sequences, ensuring the balance requirements;

- managing the weapons, providing the correct firing sequences, with the right interlocks;
- presetting the defence weapons (air-to-air weapons) by mean of a single command (air-to-air override).

2.0 Safety and mission success

It is of paramount importance, for a weapon system, to achieve the safety and mission success demands. The following definitions must be considered in order to clarify the problem:

- DEFECT is any malfunction that must be corrected by scheduled or unscheduled maintenance;
- FAILURE is any defect which makes the equipment unable to perform its intended function;
- SAFETY CRITICAL FAILURE is any failure which gives rise to dangerous situations for crew, aircraft or rotorcraft, and friend theatre;
- FAILURE RATE is the number of failures of the equipment per unit of measure of its life;
- SAFETY RATE is the number of safety critical failures of the equipment per unit of measure of its life;
- DORMANT FAILURE is a failure that cannot be detected by Built - In Test Equipment (BITE).

The failure rate affects directly the mission success probability. Where no redundance is applied, failure rate equals defect rate. However, the safety rate, that is a part of failure rate, is composed, mainly, of:

- uninteded release firing rate
- failed jettison rate.

Every design effort, intended to reduce safety rate, increases failure rate and viceversa; this means that the design aim is the reduction of both figures at the same time. In the next sections this statement will be clarified.

The design requirements, in terms of reliability, are generally expressed by the following demands:

- no single fault shall cause an unintended release, jettison or fire of any store;
- no single fault shall prevent the jettison of stores during emergency jettison operation;
- wherever is possible, no single fault shall prevent release of any store, as selected, when intended.

Typical reliability figures required are:

- Failure rate: less than 10^{-4}
- Safety rate: less than 10^{-6}

These figures demand a designing approach for an high integrity system whose main characteristics are reliability and safety.

3.0 System Architecture

Essentially, an SMS can be considered functionally composed of: (see Fig. 1)

- Control panel;
- Control processor, with the jettison associated function;
- Output actuators, for the weapons power control.

The system, however, is physically composed of:

- One or more control panels, dedicated or multifunction;
- A central unit, with the store inventory panel, separated or not;
- Several peripheral units, dedicated to the stations or to various weapon types. The peripherals contain the output actuators and the logics dedicated to the loads.

3.1 Mono Channel System

The control panel and the central processor can be functionally considered as a Processor which controls, one power actuator supplying the relevant weapon. This configuration is depicted in Fig. 2A, where for FS is intended the Fire Supply voltage. This configuration does not allow to meet the reliability requirements for jettison success (that is a part of the safety rate). Two jettison blocks, separated from the main SMS function, must be provided, controlling two redundant output actuators in OR configuration. A multiplexer can switch the jettison blocks on the output lines. This configuration is depicted in Fig. 2B. This solution, that grants an higher successfull jettison probability, when intended, gives, however, an higher unintended release probability (that is a part of the safety rate also).

The natural growth of the single channel configuration gives the system depicted in Fig. 2C, where the output actuators are duplicated for each jettison channel.

The blocks "logics" allows a suitable decoding of the output information, providing that processor must use error detection encoding or a self correction encoding. This technique must be used in order to reduce the unintended release probability.

It is important to implement a good BITE, such as to be able to detect any safety critical failure and to act on with a suitable shut-down of the output interfaces.

Where redundancies are present (i.e. output actuators), it is also important to have a suitable BITE coverage providing that no dormant failure, that could affect the safety if a second failure accurs, is permitted.

3.2 Multi Channel Reconfigurable Systems

The mono channel system, although can be applicable for several applications, can give not suitable figures both for failure rate and safety rate, when system is operated in normal conditions. However, it is able to perform the jettison function, with the required reliability figures, because it has dual redundant jettison blocks.

The natural growth of such system is the Double Channel "OR" type, as depicted in Fig. 3A, which extends the previous cencept to the normal functions. This configuration gives a smaller failure rate but safety rate is increased, being both processors operative at the same time. This configuration requires a communication channel, being necessary some synchronization form between processors.

BITE requirements are the same as for mono channel system: it is requested to shut down fault channel if a safety critical failure is detected, and no dormant failure, that could affect the safety if a second failure accurs, is permitted.

A second solution, that privileges the safety, is the Double Channel "AND" type, as depicted in Fig. 3B. This configuration gives a smaller safety rate but failure rate is increased, being both processors necessary to the function achievements.

This configuration, as the "OR" type, requires a communication channel, being necessary a complete synchronization of both processors.

BITE requirements are not the same as the previous solution, because safety is intrinsically better and, however, every shut-down operation will cause the system the be unable to perform its function. However, as for previous solution, no dormant failure, that could affect the safety if a second failure occurs, is permitted.

A third solution, that has the same failure rate as the first one, but with smaller safety rate, is the Double Channel "HOT STAND-BY" type, as depicted in Fig. 3C. This configuration does not require synchronization of the processors, because one processor only, at any time, is operative on the outputs. However, the second processor (slave) is continuously updated about the operational situation, such as to be able to act on as "master" when a failure is detected in the first one.

Each channel has its own BITE, that can declare that its channel is fault. A simple common logics is able to decide which channel must be operative, depending upon fault declarations of two BITEs.

BITE the shall be able to switch the operative channel when a failure (not necessarely safety critical) is detected. Naturally, no dormant failure, that could affect the safety if a second failure occurs, is permitted.

The natural growth of the double channel configuration gives system depicted in Fig. 3D, where the advantages of solutions "AND" and "OR" previously seen are present at the same time. Infact, as first solution privileges the success probability (in war or jettison) and the second one privileges the safety (in peace or in training use), this solution allows a configuration switching (from OR to AND and viceversa) regarding to reliability figure to be privileged.
The reconfiguration facility can be handled:

- by Jettison command
- by Battle command
- by BITE

This configuration, as the second one, requires a communication channel, being both processors operative, and synchronized, at any time.

BITE must be able to distinguish if the detected failure is relevant to mission success (multiplexers in OR configuration) or to safety (multiplexers in AND configuration). Naturally, no dormant failure, that could affect the safety if a second failure occurs, is permitted.

The above discussed solutions can be implemented having in mind which reliability aspect must be privileged. Additionally, when the physical architecture is designed, it is possible to calculate the reliability figures for the main hardware/software blocks and, consequently, to decide, for each main block, if and which type of redundant solution is to be used.

A possible double channel solution based on the Selenia experience in the SMS technology conducted on military aircraft is shown in FIG. 4. This architecture is a Hot Stand-by Double Channel with AND-OR reconfigurable peripheral unit. Both the central unit processors recive information and elaborate it from the control panel but only one of them send information to the peripheral unit. Otherwise, both channels of the peripheral unit are operative at any time, receving the same command information. The power actuators, controlling the loads, are duplicated, in each channel, and every one of them can be controlled by both peripheral unit processors.

This configuration is suggested from the following considerations:

- Many peripheral units and many power actuators per unit ask an AND configuration of the unit for safety reason (unintended release or firing);
- the AND configuration of the peripheral unit must be switched to OR configuration, if requested (requirement for jettison and mission success);
- the multiplexed configuration of the communication channels from central units to peripheral units cover the jettison and mission success requirement allowing the crossing from each central unit channel to each peripheral unit channel;
- the hot stand-by configuration at central unit level requires no synchronization between processors;
- the control panel, due to its realiability figure, is connected to central unit in not multiplexed mode;

it is important to point out that the reliability models to be considered and evaluated, differ from each other as various mentioned realiability figures are considered (defect rate, failure rate, safety rate).

Other architectures can be considered (triple channel, quadruple redundant) but will not be described herein, due to their complexity.

3.3 Communication Channels

The reliability requirements discussed before, demand that SMS must be designed as an high integrity system, minimizing its functional dependency from external equipment. A dedicated communication network is generally preferred. SMS, essentially, requires three types of information exchange:

- discrete: from external controls (switches); to external indications (lamps); from weapons (i.e. ready, armed); to weapons (fire, release, preset);

- serial digital: from/to main or armament computer;
- analogal from/to some type of weapons (presetting and acquisition information).

In FIG. 5A a traditional networking is shown, where every information exchange inside SMS is implemented via a dedicated channel (one for each command, one for each return). A loss of one communication channel does not impact other peripheral units function. This is a star network, where every communication channel can be single or dual redundant according to single or double channel solution. Special attention must be paid designing the communication channel in term of:

- protocol (i.e. triple message must be received in an assigned time slot before its validation);
- information coding (i.e. self correcting codes);
- bit coding (i.e. pulse width modulation, self clocking);
- electric standard (i.e. CMOS levels on low impedence lines; common mode rejection by optical coupling);

in FIG. 5B a modern networking is shown, taking in account the MIL-STD-1760 SMS standardization networking requirements.

Multiplex data bus technology is now applied successfully in military aircraft to achieve as important goal efficient interconnection and flexible intergration of avionic subsystem.
Hyerarchical architectures are demostrated to provide the needed flexibility, on their simplistic top-down control mechanism make it possible to achieve the reliability with added redundancy and data transfer format.
In this figure a typical three level architecture based on dual redundant 1553B bus is used. A fourth higher level bus is the general avionic bus, not shown in figure.

- the armament bus: the dashed lines connecting the control panel to the bus are used if this is a multifunction panel, serving other armament systems also;
- the SMS bus, dedicated to Stores Management System
- the weapon bus, for smart weapons.

It is important to note, however, that there is insufficient error protection inherent in the 1553B bus to ensure reliable transfer of critical commands. To achieve better performance, a combination of protocols and information coding must be used.

4. Conclusions

Military aircraft of the 1980's 1990's and beyond will require Stores Management Systems which are reliable, flexible and efficient. In order to meet these goals both system architecture and utilization of the state-of-the-art hardware technology must be considered.

It is envisioned that the SMS must be so designed that no single hardware or software failure will result in a catastrophic failure or mission abortion.

Throught the analysis of system of architecture we have explored in top-down sequence the method to increase reliability figures adding redundancy and flexibility.

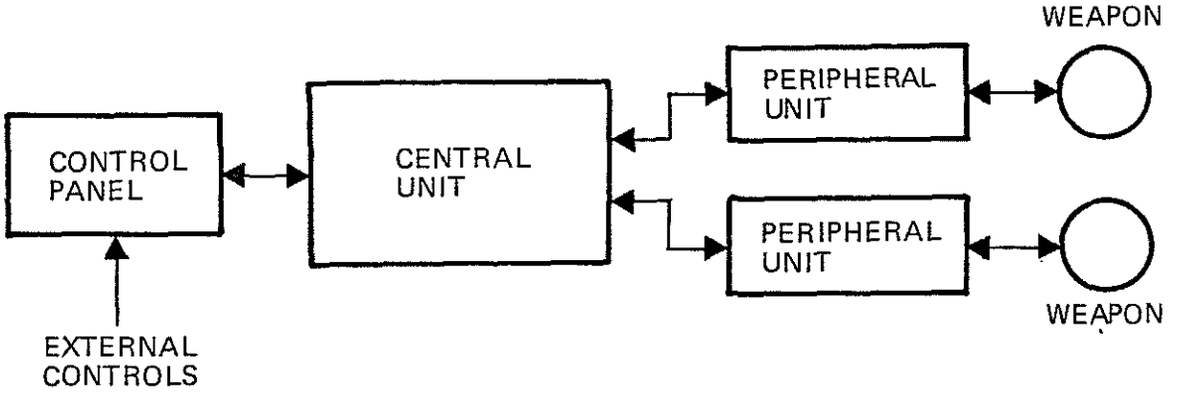


Fig. 1 - SYSTEM ARCHITECTURE

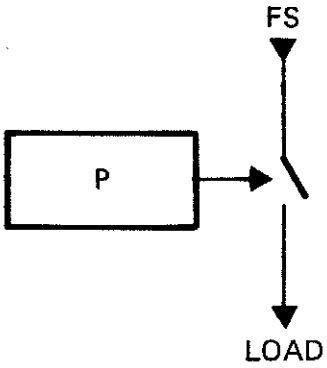


Fig. 2A

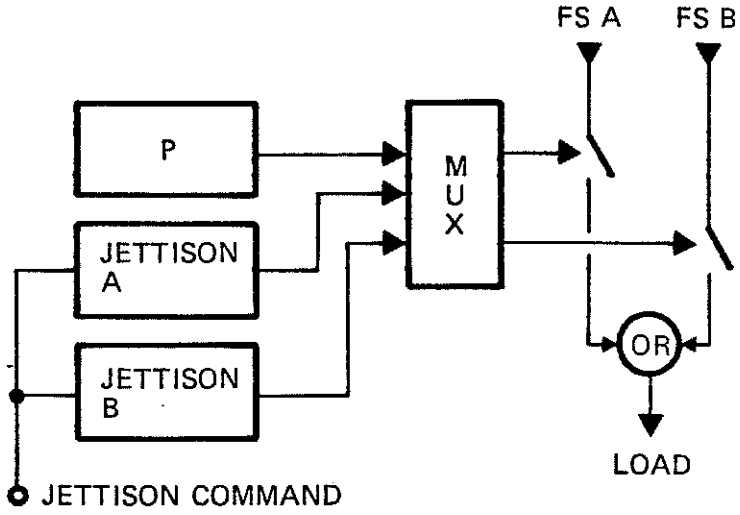


Fig. 2B

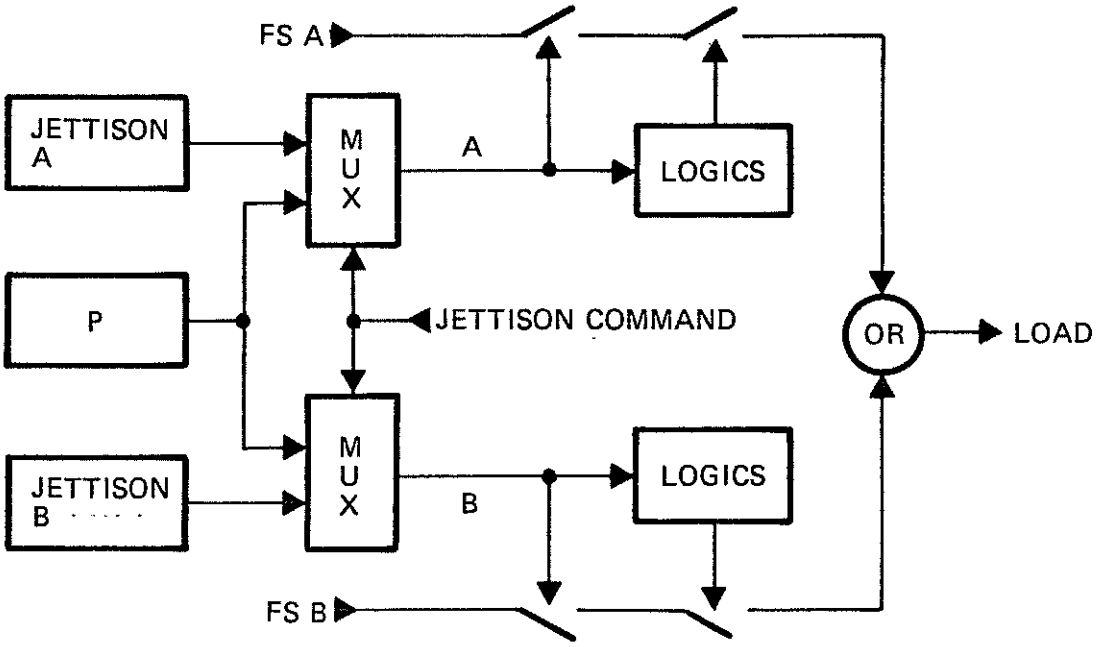


Fig. 2C

Fig. 2 - GROWTH OF A MONO CHANNEL SYSTEM

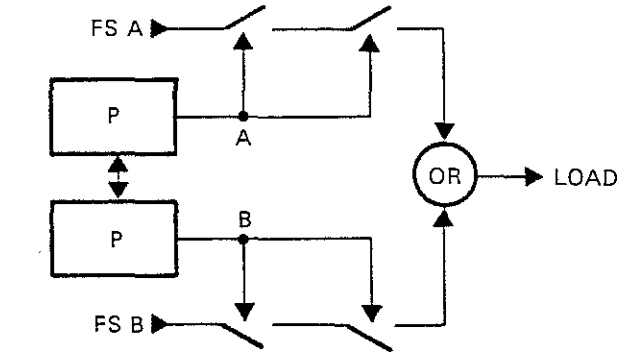


Fig. 3A – "OR" CONFIGURATION

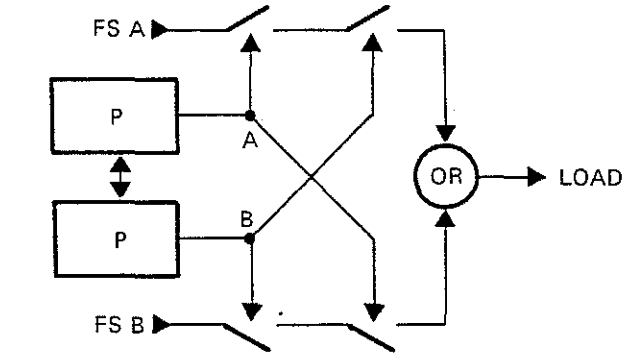


Fig. 3B – "AND" CONFIGURATION

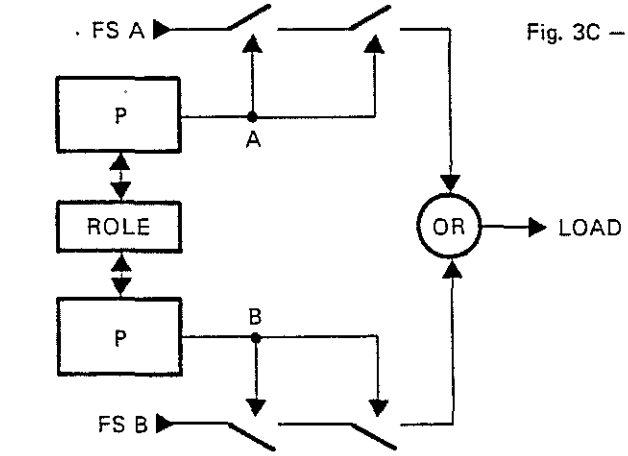


Fig. 3C – "OR HOT STAND-BY" CONFIGURATION

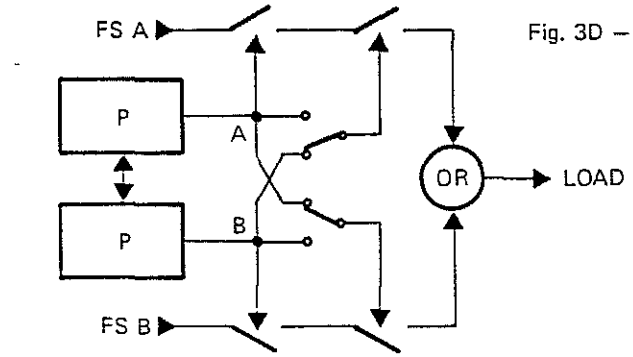


Fig. 3D – "AND/OR" RECONFIGURABLE SYSTEM

Fig. 3 - GROWTH OF A MULTICHANNEL SYSTEM

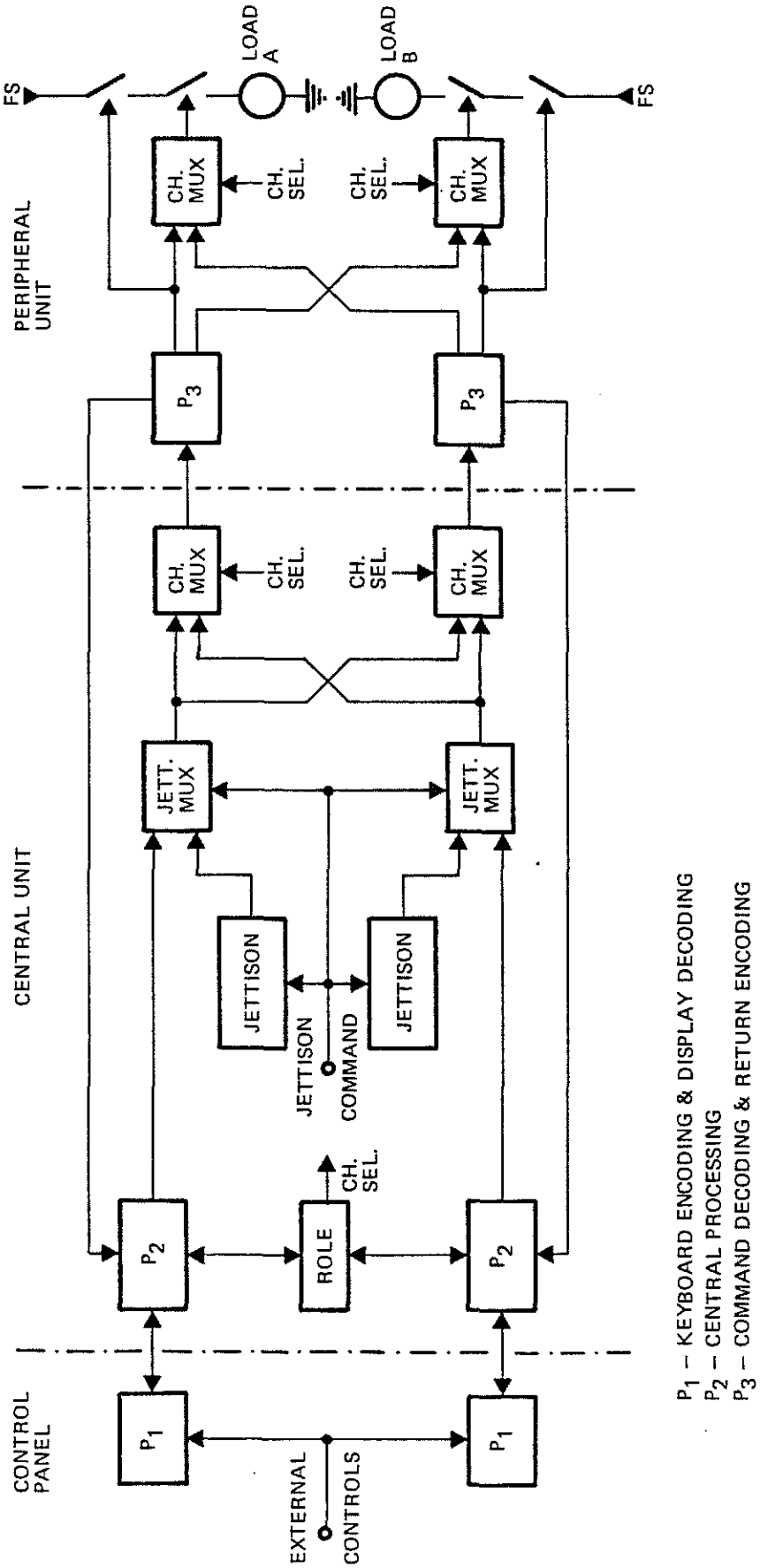


Fig. 4 - EXAMPLE OF DOUBLE CHANNEL CONFIGURATION

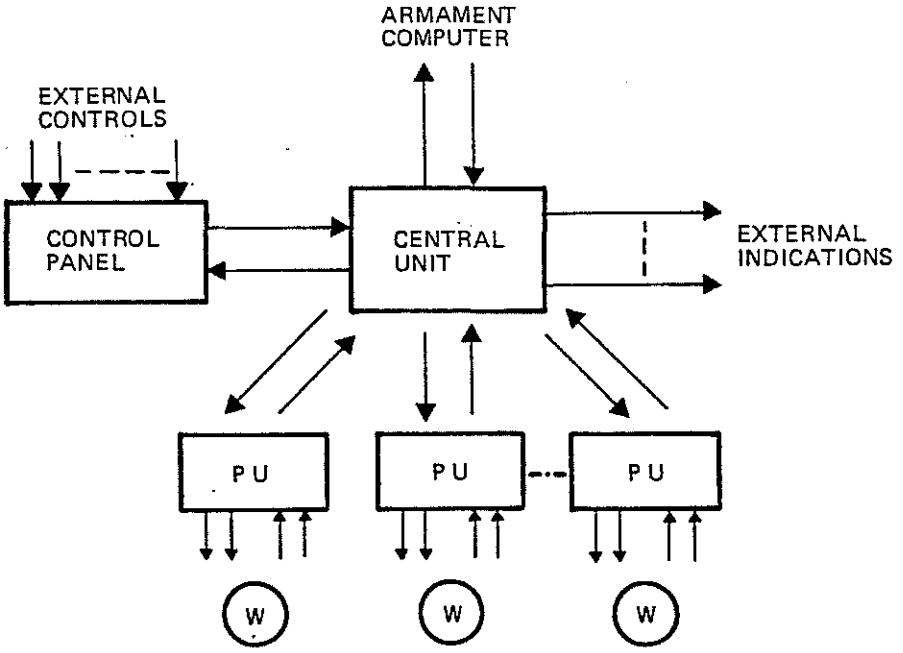


Fig. 5A – SMS STAR NETWORK

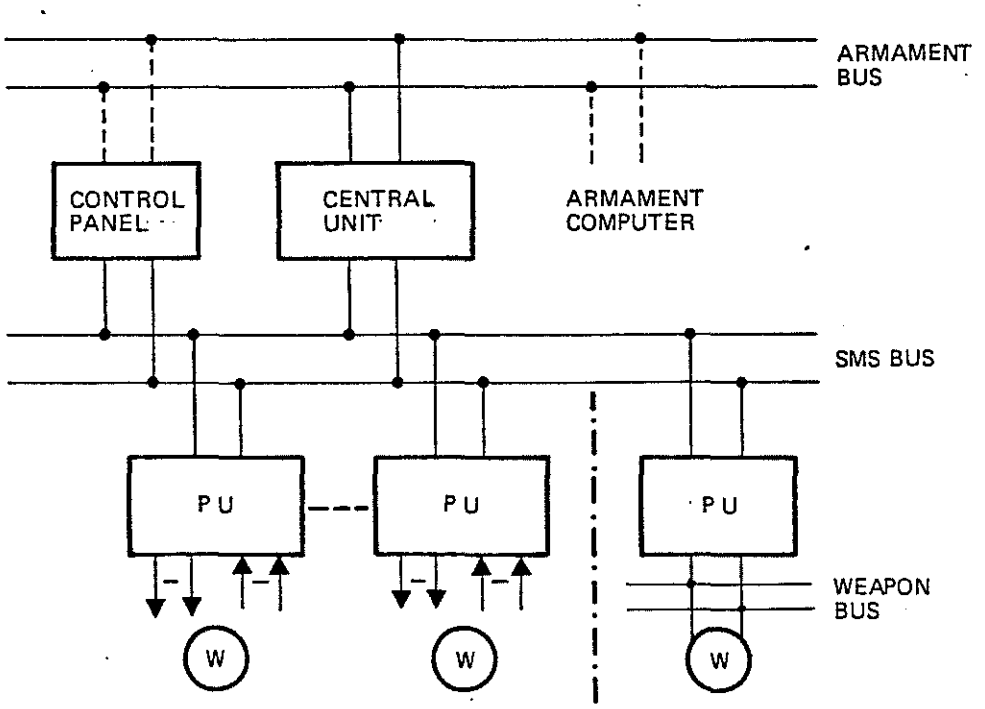


Fig. 5B – SMS BUS NETWORK

Fig. 5 - EXAMPLE OF SMS ARCHITECTURES