TWELFTH EUROPEAN ROTORCRAFT FORUM

Paper No. 93

EMI-FAULT PREVENTION AND SELF RECOVERY OF DIGITAL FLIGHT CONTROL SYSTEMS

Michael Stock

MESSERSCHMITT-BÖLKOW-BLOHM GmbH

Munich, F.R. Germany

September 22 - 25, 1986

Garmisch-Partenkirchen

Federal Republic of Germany

Deutsche Gesellschaft für Luft- und Raumfahrt e.V. (DGLR)
Godesberger Allee 70, D-5300 Bonn 2, F.R.G.

EMI-FAULT PREVENTION AND SELF RECOVERY

OF DIGITAL FLIGHT CONTROL SYSTEMS

Abstract

The task of helicopter flight control is more and more reliant on digital control systems. The microcomputer systems normally used for flight control can be forced to produce undeterminable results by electromagnetic interference. Despite redundancy, these malfunctions may become hazardous to the rotorcraft and must therefore be taken into account from the very beginning of system design.

It is the aim of this paper to show ways to achieve system reliability and survivability for microcomputers in complex flight critical applications. Microcomputer systems failures caused by EMI and their impact on flight control systems shall be addressed. Also addressed are ways to maintain system reliability in electromagnetic contaminated environment and ways to ensure self recovery after EMI caused faults.

In conclusion, a digital flight control system, designed with respect to EMI problems and flight tested on a BK 117, is presented.

1. Microcomputer system failures caused by EMI and their impact on flight control systems

Normally, an electronic system which is exposed to electromagnetic radiation does not suffer hardware damage. Analog systems will continue proper operation after the radiation has decreased. A microcomputer system, however, is very likely to run out of normal program execution after radiation has decreased.

It is totally undeterminable, with regards, what an unprotected microprocessor, which has run out of its program, will do. If no preventive measures are taken, the following possibilities have to be considered:

- the microprocessor can alter memory and its own register contents randomly;
- the microprocessor can jump to some undefined address space, find executable code and run over its own program counter;
- the microprocessor can jump into an endless loop and execute the code in-between for an indefinite time;
- the microprocessor can perform random signal outputs through I/O-devices.

Normally, a combination of these possible failures will occur. The last item could cause the whole control system to fail. As long as a control unit simply loses function, the situation can be handled quite easily. However, if the system starts to produce random signals, it becomes hazardous to all other systems it communicates with. For example in a simplex, limited authority stability augmentation system, the actuator could start to oscillate or pulse. In a redundant flight control system, the confused processor could try to move output signals to the actuators despite being acknowledged as being faulty by the other processors. It might also broadcast confusing information to the redundant processors, forcing them to separate this data from correct data. As these examples point out, preventing false outputs may in some cases be an absolute requirement, but will in every case be a support to maintain safety and stability of digital flight control systems.

A working microcomputer system, having been thrown out of normal program execution by transient electromagnetic radiation would be useless for the rest of the flight if it ended up in an endless loop. Unfortunately, this will happen without proper preparation.

In conclusion, in digital flight control systems the prevention and handling of EMI-faults is even more important than in analog systems. In flight critical applications, methods for faultless operation will be indispensable in making a system reliable.

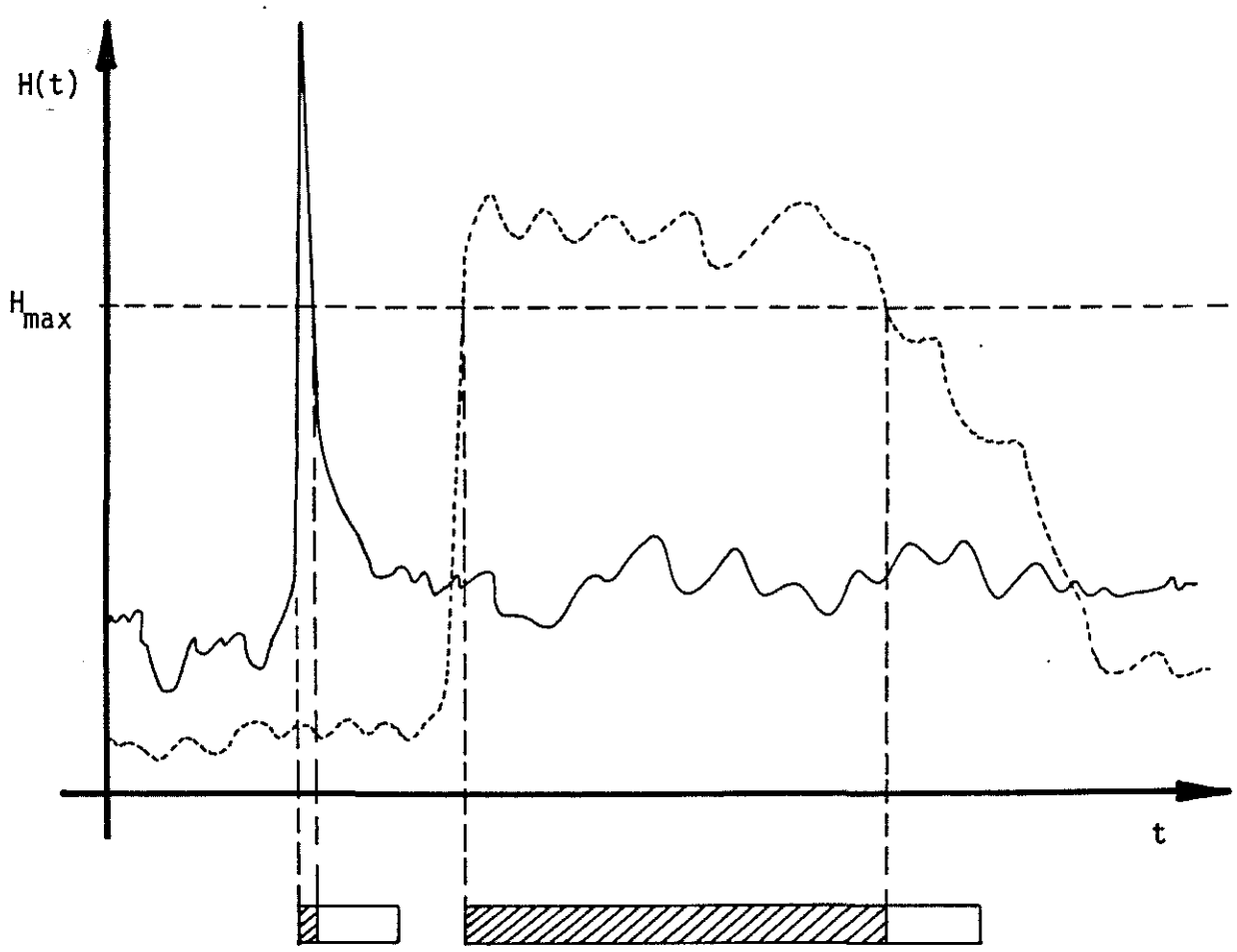
It can be seen that the trend in rotorcraft guidance and control is moving towards triplex or quadruplex redundant digital flight control systems without mechanical back-up. In rotorcraft, due to limited space, the redundant computers cannot be separated very far from each other. Normally they are very likely to be exposed to the same amount of electromagnetic radiation. Therefore, malfunctions caused by EMI will occur in all redundant channels simultaneously. - The logical consequence is that the pilot loses control of the helicopter.

The impact of single failures, occuring one after the other is simply insufficient to determine the safety margin of a redundant flight critical system. The possibility of simultaneous faults must be considered.

2. Ways to achieve system reliability of microcomputers in electromagnetic contaminated environment

Trying to maintain system reliability under EMI conditions is difficult. Every unhoused microcomputer system will have a certain point at which the amount of induced energy falsifies the system bus data and makes proper bus transactions impossible. This point is dependant upon the preventive measures taken and on the type of radiation. Amplitude-modulated signals with suppressed carrier waves will be most dangerous to a microcomputer system bus. This is because electromagnetic induction is proportional to the rate of the electromagnetic field. Therefore the more variable a field is, the more energy will be induced into a bus line.

The duration, for which electromagnetic radiation is present, influences the impact on a flight control system to a high degree. If the amount of radiation lasts for a very short period of time as in the case of lightning, self recovery after the fault can take place fast enough to keep the rotorcraft under control. Longer lasting distortion like in the case of a transmitting AM radio station will block the system until the radiation has decreased below Hmax plus the time needed for self recovery (picture 1). Therefore component irradiation must be prevented by the means of electromagnetic shielding, system bus insensitivity and EMI-resistant signal transfer to and from the microcomputer system.



Picture 1: Transient and continuous EMI

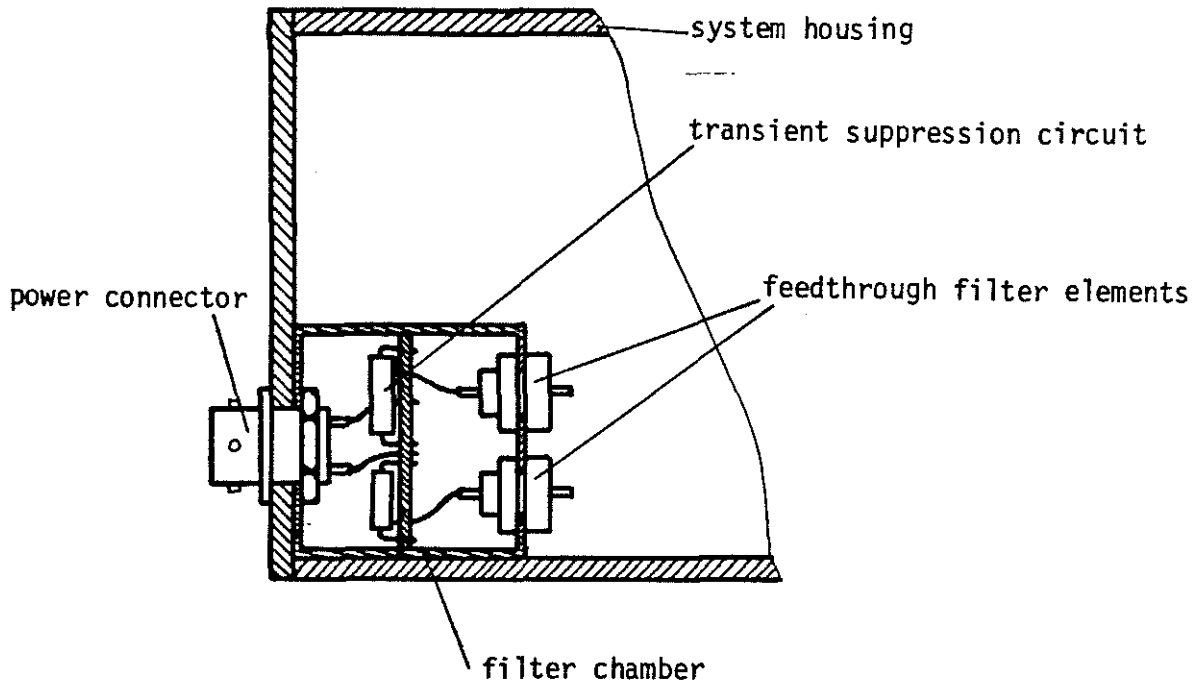
2.1 Electromagnetic shielding of microcomputer systems

If proper shielding of a digital flight control system is provided, electromagnetic radiation, reaching the inside of the microcomputer system, is much attenuated. The major components of the shield efficiency are the reflection attenuation and the absorption attenuation. These efficiencies are dependant on; the frequency of the radiation, the thickness of the walls and the specific conductance of the housing material. As attenuation increases with specific conductance, aluminium housings provide a good basis if the parts of the housing are low-resistance connected. This contact resistance, of course, is subject to aging by oxidation which has to be prevented to gain long-term attenuation, i.e. by conducting adhesive.

For low frequencies, the shielding efficiency of metal walls are close to infinity. The efficiency decreases very fast with growing frequency and increases again for high frequencies due to skin-effect. As a conclusion to this, the frequency range of 100 kHz to 1 GHz will be the critical frequency band. This is based on the assumption that no openings in the housing exist and necessary connectors are handled properly.

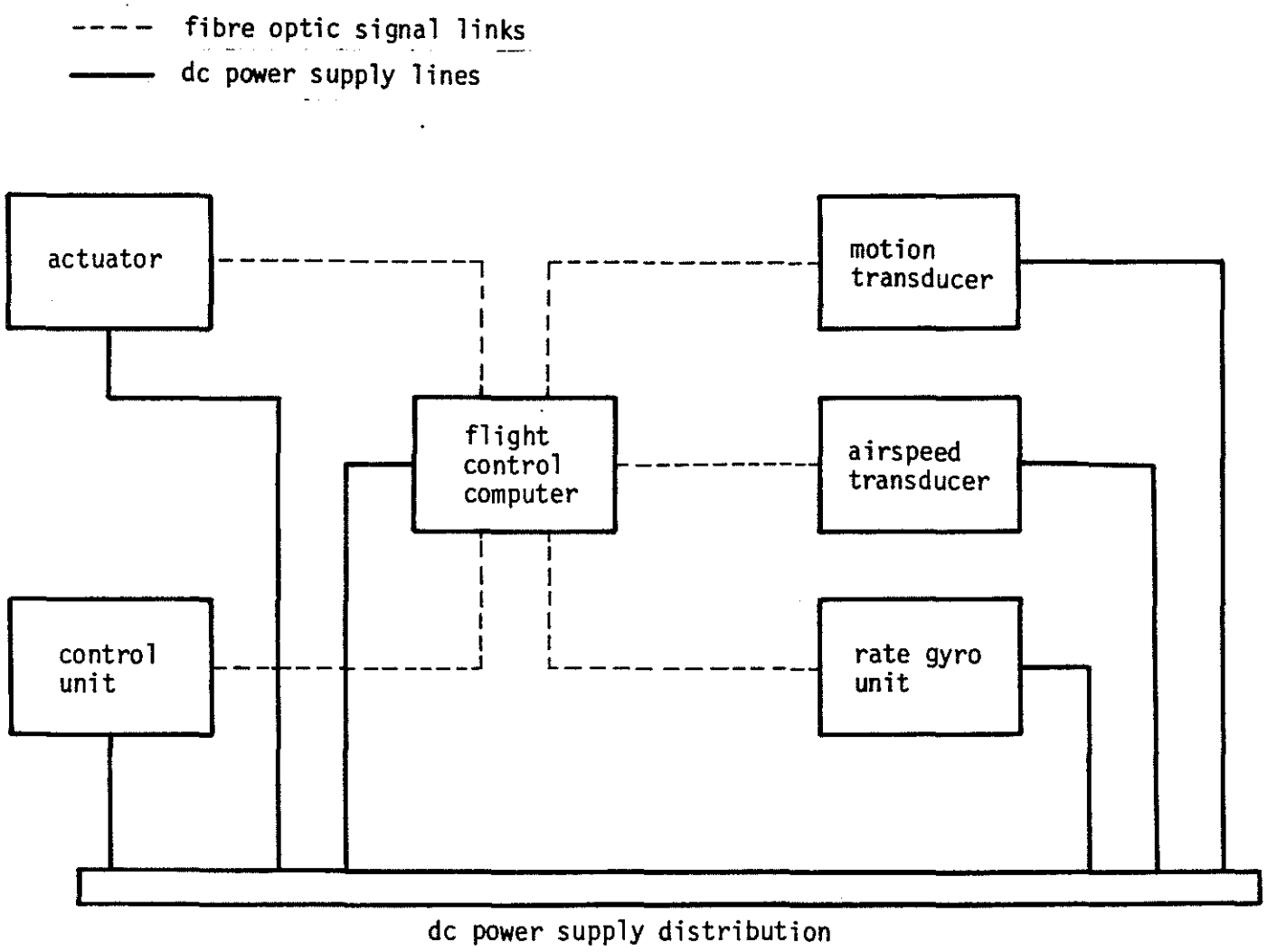
2.2 EMI-resistant signal transfer

There are two major categories of connections to flight control computers; dc power supply connections and control signal connections to sensors, actuators and control unit. All wires used for these purposes share the problem of working as an antenna for electromagnetic radiation exposure. Induced energy is transferred through the connectors to the inside of the microcomputer system. Power supply connections can be protected quite easily by letting them pass through a filter circuit of a very low cut-off-frequency, mounted within a filter chamber in the inside of the computer housing (picture 2).



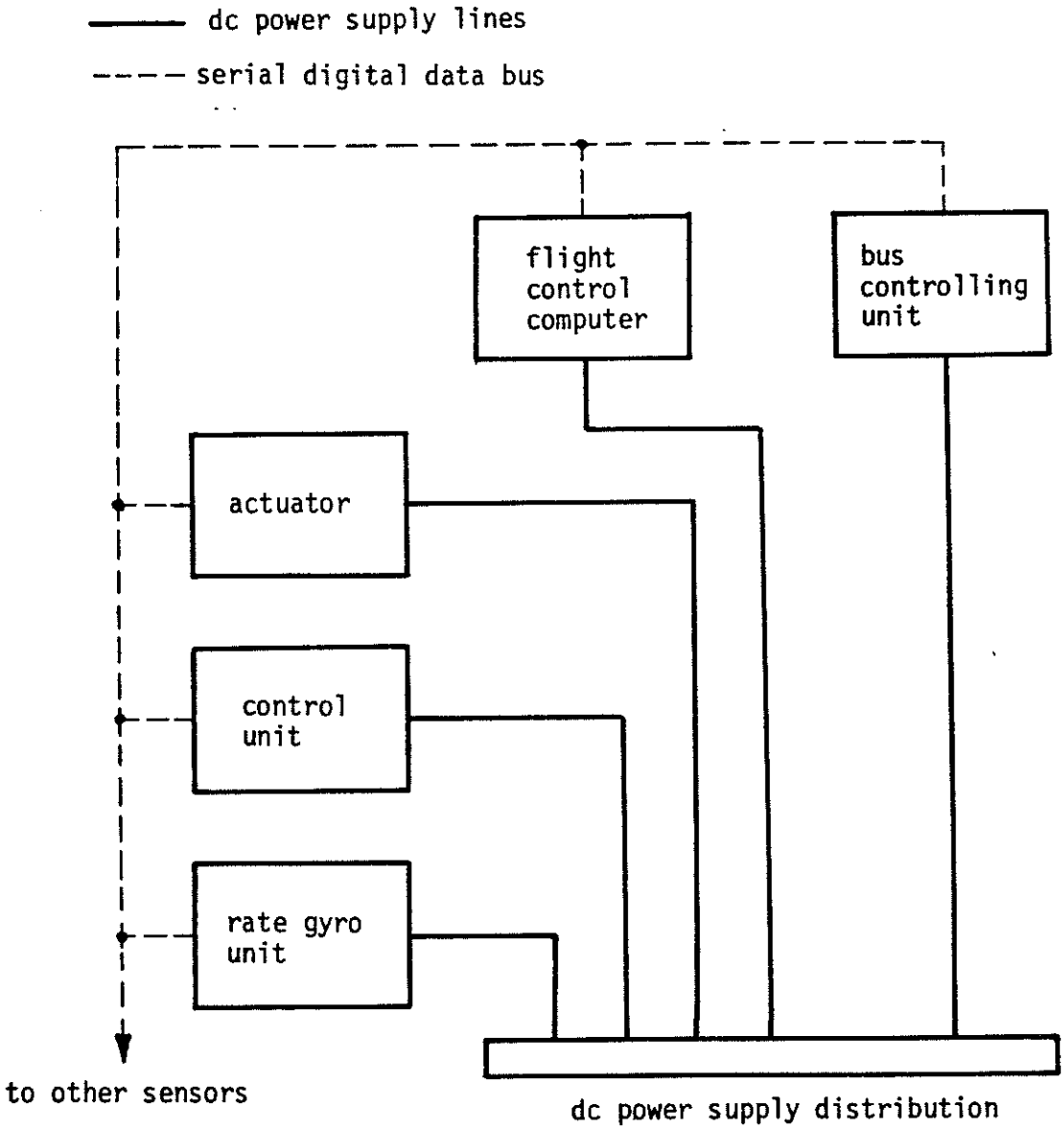
Picture 2: Filter chamber for dc power supply lines

Control signals are more difficult to treat. The difficulty is a result of the great number of signals, which are normally transferred by multi-way-connectors. These multi-way-connectors are available with reactor filter-inserts, but do normally have a high cut-off-frequency (> 1 MHz). These connectors go into saturation quite early, due to the small size of the reactors. The effect of this problem, however, can be reduced if the signal lines are shielded and the shields are properly coupled to low-resistance-mounted circular connectors. Despite that, the best way of control signal transfer with respect to the EMI-problems is the use of fibre optic links, which are completely insensitive to electromagnetic radiation. Unfortunately, one disadvantage comes along with this technology: In a fly-by-light control system, every sensor, actuator and control unit has to be an active component. This requires additional hardware and power supply (picture 3). In the future, this disadvantage will hopefully be overcome by all-light-transducers.



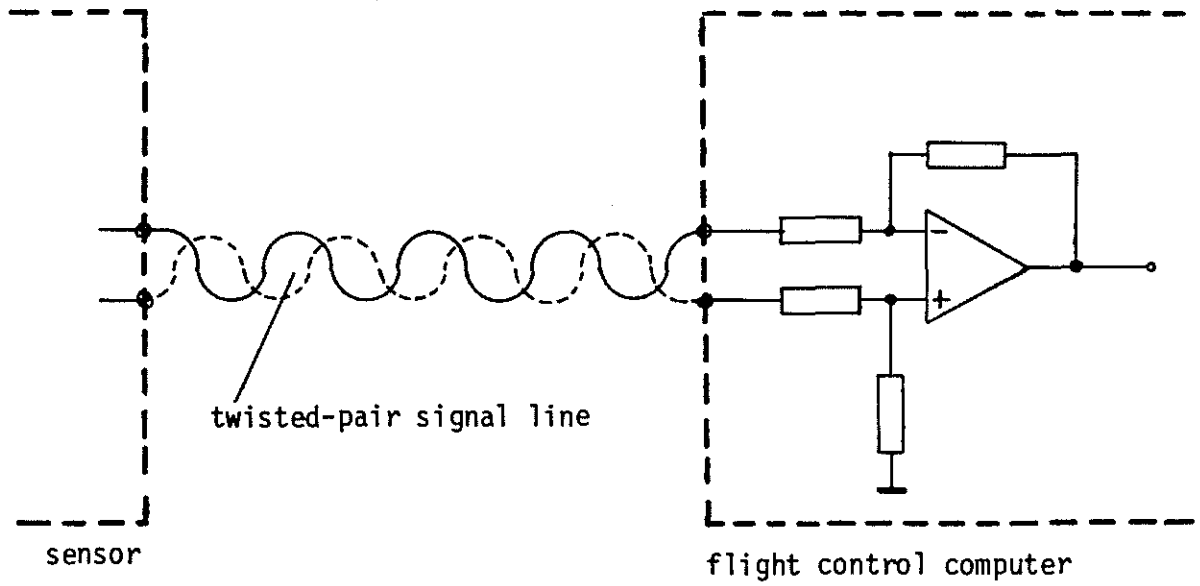
Picture 3: Fly-by-light flight control system

MIL-STD-1553 B bus systems (picture 4) provide good EMI-resistance too, assumed that shielded twisted-pair signal wiring and transformer coupling is used. Beside that, the signal-to-noise ratio of a digital signal can get close 50 % before the data becomes corrupted. Unfortunately, an additional bus controlling unit has to be added.



Picture 4: Flight control system with bus data transfer

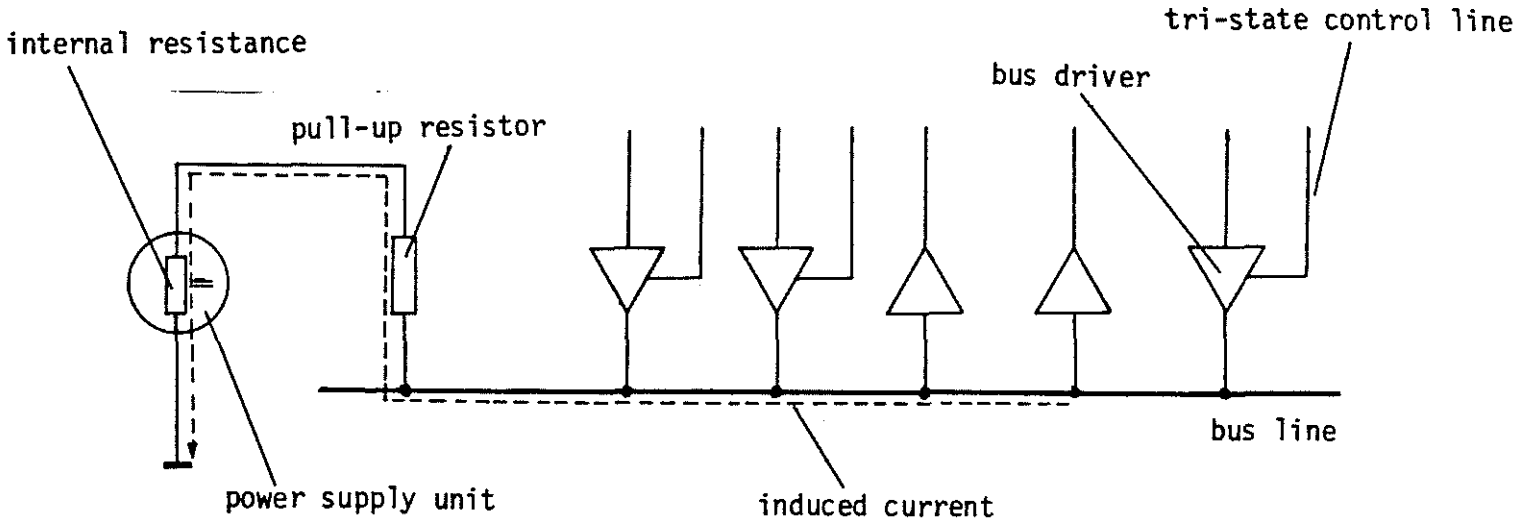
The classic way of analog signal transfer to digital flight control computers via twisted-pair lines and differential operational amplifier inputs (picture 5) involves a risk: any unsymmetry of the twisted-pair line will lead to EMI-induced currents, which will be rectified at the operational amplifier inputs and will produce an offset voltage at the output. Despite that, if the current induced by electromagnetic radiation does not receive sufficient attenuation by the filter connector, it will have direct impact on the microcomputer system. For this reason, this method of signal transfer has to be regarded as critical. Additional shielding has to be applied, if the more insensitive ways of signal transfer, as described above, are not applicable for any reason.



Picture 5: Analog signal transfer via twisted-pair lines

2.3 Gaining EMI-insensitivity of a microcomputer system bus

Normally, the bus lines of a microcomputer system are in a high impedance state, if no data access takes place. These high impedance bus lines, however, are very sensitive to electromagnetic induction and will transfer the induced energy to memory, timers, input/output-devices, etc. This energy is, as long as it is not short-circuited to ground, very likely to alter data and can throw the microprocessor out of program. Therefore, it is beneficial to pull up the system bus to the power supply by using minimum resistance (picture 6). The lower the value of the pull-up-resistors and the lower the value of the internal resistance of the power supply unit, the more energy can be shunt conducted to ground within the high impedance periods. This requires that all bus lines are being driven by powerful line-drivers to prevent reactions onto sources and to achieve low impedance during bus accesses.



picture 6: microcomputer system bus pull-up

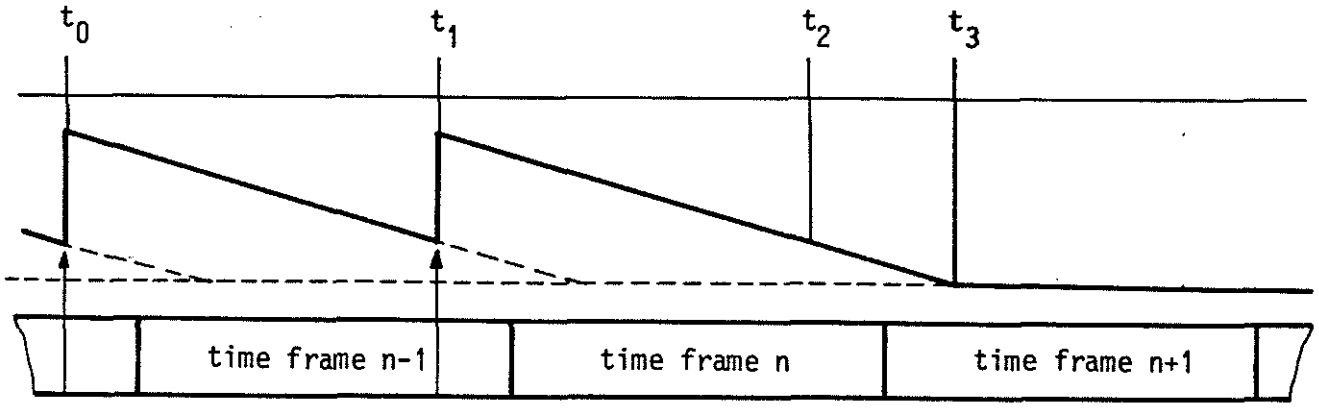
Another way of making the system bus more insensitive to electromagnetic radiation is to increase the shielding efficiency by covering the bus backplane with grounded surfaces on both sides. Together with pull-up-resistors, these measures will significantly increase the system bus reliability.

3. Ways to achieve self recovery of faulted microcomputers

Recovering from a software fault, caused by one of the events mentioned in the first chapter of this paper, requires the recognition of the faulty behaviour. The possibilities to achieve recognition differ widely, dependant on the in-circuit bus monitoring facilities of the chosen microprocessor. Many microprocessors available on the market lack such facilities and therefore rely on the system designer to provide means to get information about the system behaviour.

3.1 Self recovery hardware

A very basic, but also very important hardware bus monitor can be implemented by forcing the microprocessor to access a timing circuit in defined time units. If the microprocessor runs out an orderly program and fails to access, the time elapses and the circuit generates a hardware-reset or a non-mascable interrupt to reactivate the microprocessor system. This circuit must not depend on the system clock and must receive even more protection against electromagnetic radiation than the microcomputer itself. As digital flight control computers are mostly frame-synchronous, the internal timer has to run a little longer than the computer time frame itself (picture 7). It should, on the other hand, not exceed the frame too much, so that no time is lost to initiate self recovery. This presumes that the time frame leaves enough space to handle pending interrupts etc., so that the time-out event is well-defined. After the time has elapsed,



t_0: timer accessed t_1: timer accessed t_2: timer access failed

t_3: time elapsed, self recovery initiated

Picture 7: Hardware self recovery timing

the timing circuit has to generate reset- or interrupt-pulses periodically until it has been accessed again and therefore acknowledged the proper reactivation of the microcomputer system. The time between the pulses must be long enough for the self recovery procedure to execute plus some security. However, it must not be longer than that. This ensures short latency times in case that the electromagnetic field is still too strong to allow program execution.

The importance of this elementary self-recover-facility becomes clear if multiple-processor faults in redundant flight control systems are considered. In this case, the computers will, independently of each other, continuously try to reboot and therefore increase the probability to reclaim control of the helicopter.

3.2 Self recovery procedures

There are microprocessors with on-chip bus monitoring and microprocessors which lack that capability. For flight control computers based on CPU's which lack monitoring, self recovery can only be achieved by the hardware described under 3.1. The software supporting that hardware will be different in simplex and multiple redundant flight control systems, due to the fact that in non-redundant systems no information on previous values of variables can be obtained after a software crash. These values, however, are important for digital control algorithms to produce consistent outputs. The missing variables will force a non-redundant system to start in an idle state, where as a computer in a redundant system can ask the other computers to supply the necessary data and continue control algorithm processing without delay.

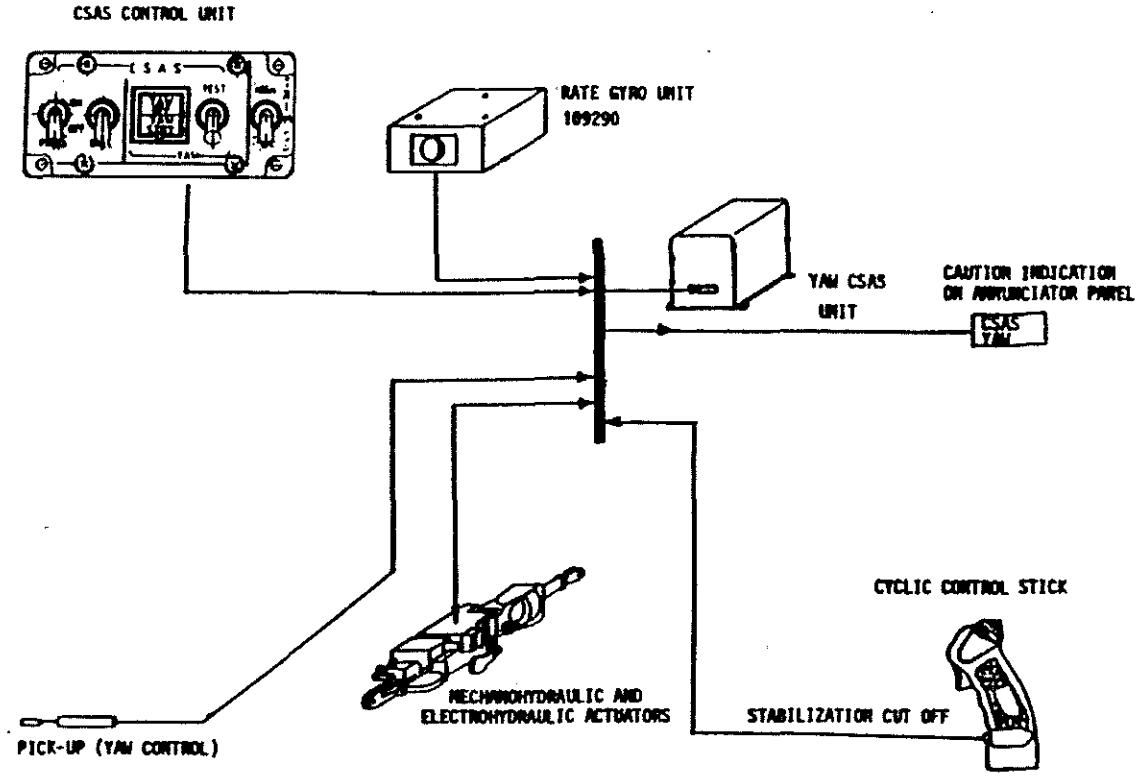
If a microprocessor is able to recognize the occurance of; not implemented instructions, accesses of non-existing devices and "wrong" interrupts, faults are very likely to be recognized earlier and self recovery can take place before the system has crashed totally. This, again, allows recovery within a short period of time, so that the impact on the flight control system is minimized. The major advantage of this "early warning system" is the possibility of preventing false outputs by recognizing the faulty behaviour fast enough.

To recover from such an early recognized EMI-caused fault, the microcomputer has to check if the variable values, located in random access memories or microprocessor registers, are still the same as they were before the event. This can be accomplished by supplying every value with a parity bit pattern which gives information about the validity of the variable. If no data corruption occured, the control program can be continued.

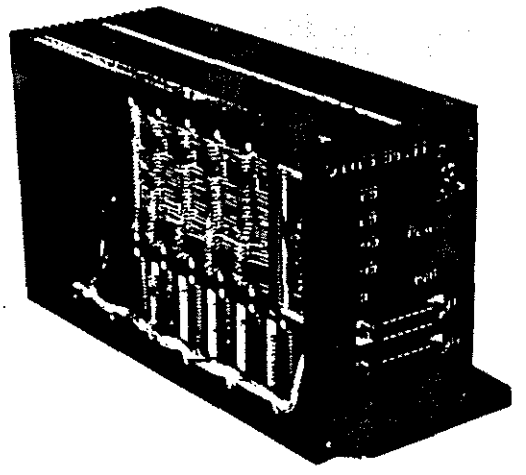
4. An EMI-resistant digital helicopter flight control system

A study was undertaken to develop a program to evaluate electromagnetic distortions of digital flight control systems in helicopters. The non-redundant yaw control stability augmentation system of the BK 117 helicopter (picture 8) was equipped with a digital flight control computer. The complete system, consisting of; the computer (yaw CSAS unit), the sensors (yaw control pick-up, rate gyro unit), the control unit and the actuator is shown in picture 9. The digital computer replacing the analog computer is based on a Motorola M 68000-microprocessing unit, working at 12.5 MHz clock frequency. It is installed in an 1/2 ATR short aluminium housing, which was treated so as to be sealed against electromagnetic radiation (picture 10). The analog signals are transferred to the computer via the simply shielded standard wiring of the helicopter and pi network filter element multi-way-connectors with a cut-off-frequency of 1.5 MHz. The microcomputer system bus is unshielded but properly pulled up as described under 2.3.

Picture 8: MBB BK 117 helicopter



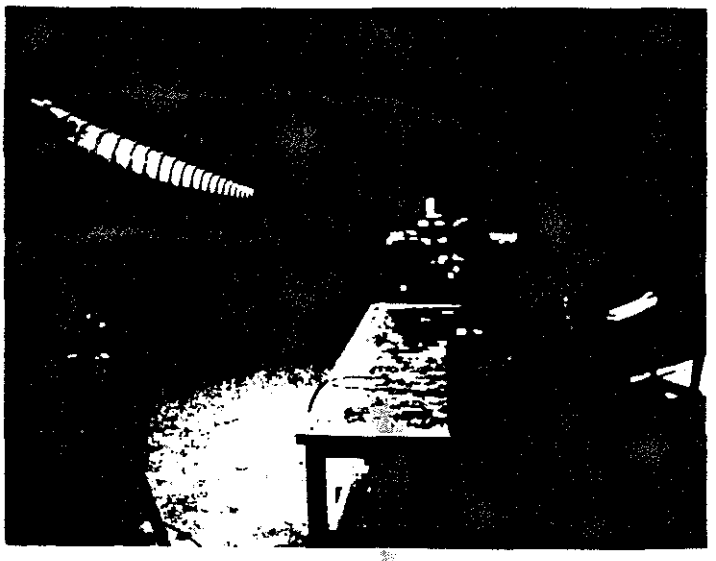
Picture 9: BK 117 yaw command stability augmentation system



Picture 10: Digital CSAS computer

The self recovery software of the CSAS computer uses the very complete bus monitoring of the 68000 microprocessor and starts exception processing on every as "insufficient acknowledged" bus transaction. The complete unused address space is given a defined value ($FFFF), which also leads to an exception if accessed by the CPU due to a jump. After these early recognized failures, the flight control computer will not access output devices until having checked all variables for validity, therefore preventing inconsistent outputs. During continuous distortion, which will cause multiple bus faults, the microprocessor responds by resuming execution and going into a halted state. This will automatically initiate self recovery as described under 3.1, generating a hardware reset.

In order to get useful information about the amount of radiation, which can be withstood by the digital CSAS computer due to its self recovery capability, the computer was exposed to defined electromagnetic radiation within the range of 100 kHz to 220 MHz in steps of 500 kHz (picture 11). The band between



picture 11: EMI impact test on the digital CSAS computer

2 - 30 MHz was given special consideration because it is in the region which is most often utilized by helicopter hf/ssb radios. During the tests (picture 12), the computer did enter the self recovery exception procedures, which was displayed with LED's. Testing which was conducted at the 2 - 30 MHz frequencies resulted in a sustained halted state of operation while the field intensity was at 90 m/V. When field strength was reduced between 70 - 90 V/m, operation was intermittant. At levels up to 70 V/m operation was continuous with intermittant activation of self recovery software. For frequencies other than 2 - 30 MHz operation was also continuous without activation of self recovery software.

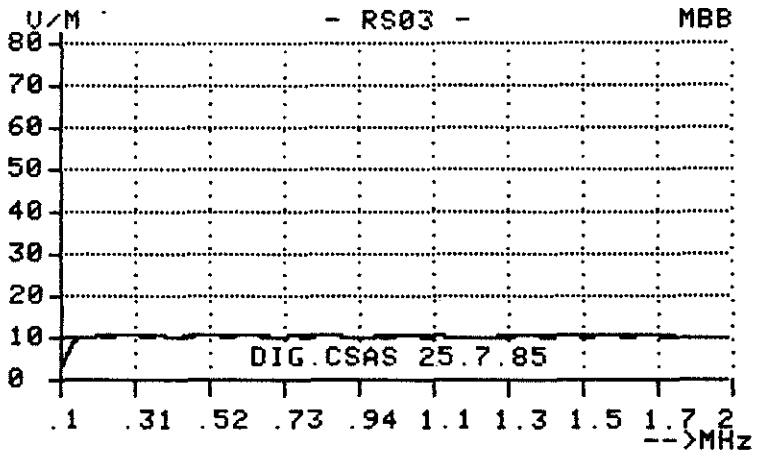
During the flight tests the digital CSAS computer operated without any problems in a fully-equipped BK 117 helicopter. In a next step, the system will be optimized with a shielded bus backplane and fibre optic digital signal transfer from the sensors (rate gyro, pedal pick-off) to the computer. It is projected that this will increase EMI-insensitivity beyond electromagnetic field intensities of 100 V/m.

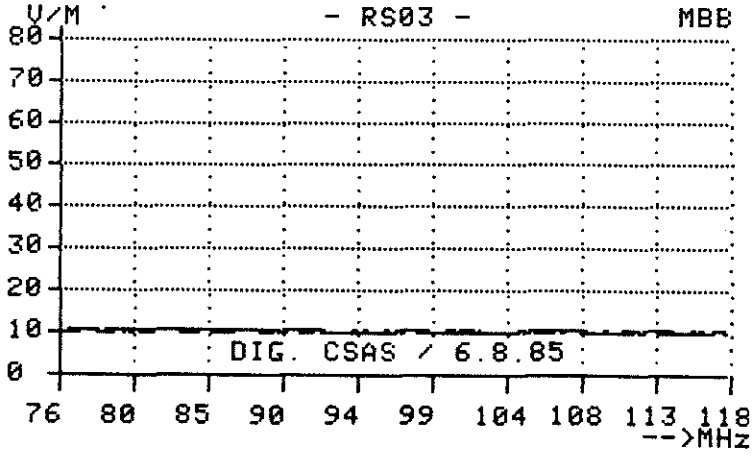
5. Summary

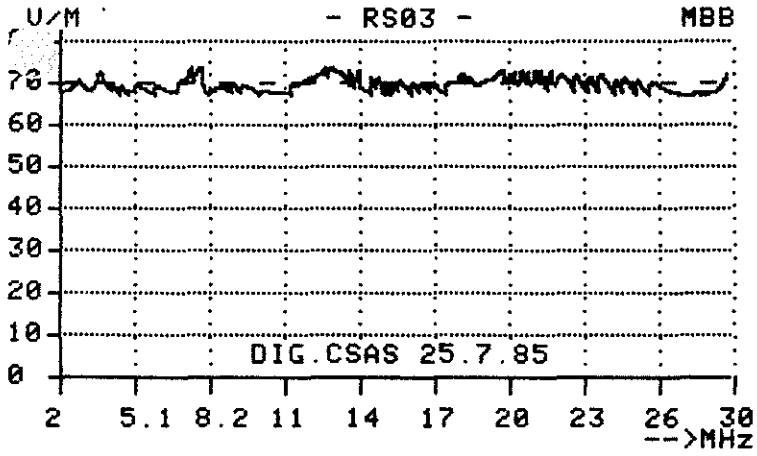
The results, which the EMI tests of the digital yaw CSAS computer offered, show that a high insensitivity of digital control systems against electromagnetic radiation can be achieved, if the system designer observes some rules to minimize the influence of the electromagnetic fields. It is important to be aware of the fact that a microcomputer system will only be able to execute a program as long as the electromagnetic field does not alter the data on the system bus and confuses transactions. In conclusion, the microcomputer must be shielded properly so that it only has to fight transient distortions, which can be handled by self recovery software. Longer lasting bus distortions will force the computer to wait until the electromagnetic field has decreased, before a restart can take place.

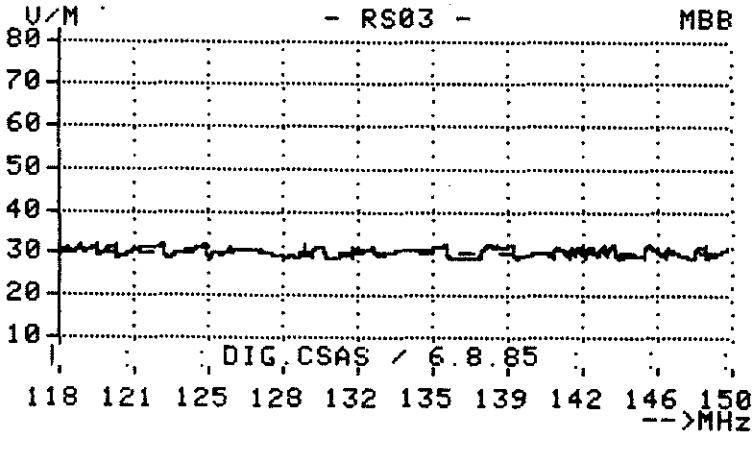
Concerning self recovery software, microprocessors with on-chip bus monitoring offer the best chances to recover from a EMI-caused fault, because failures are recognized before the system has crashed and destroyed register and memory contents.

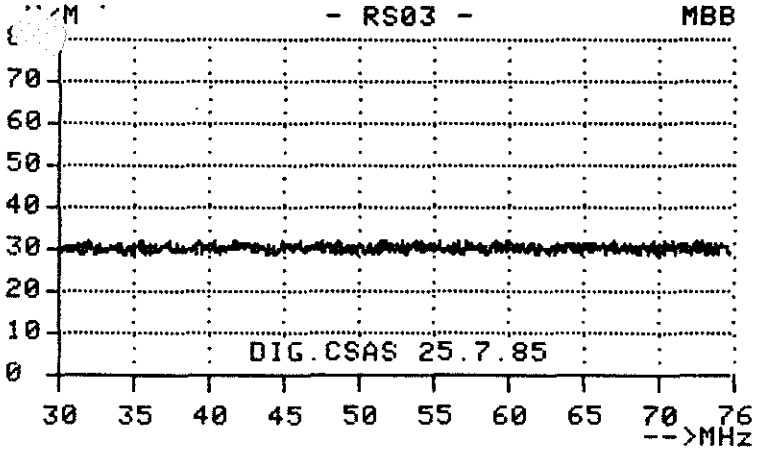
Many future helicopter flight control systems will demand extremely reliable flight control computers. The measures taken against electromagnetic interference are a definite "must" to gain this reliability.

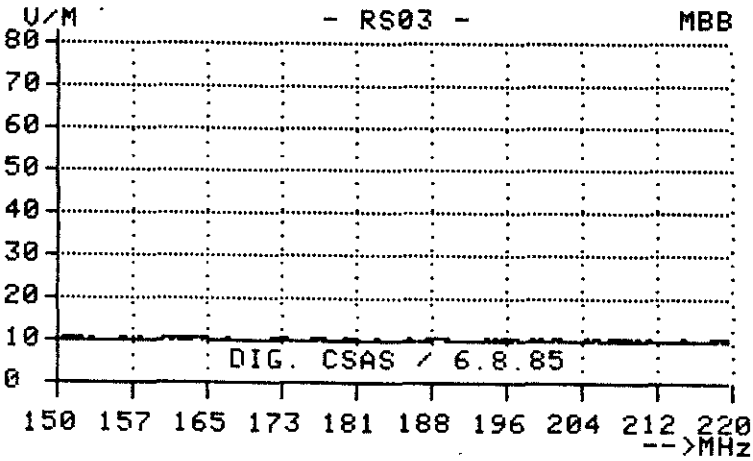












Picture 12: Electromagnetic impact test frequencies and field intensities