

Next generation architecture for flight control systems

Kristina Ahlström Jan Torin
Department of Computer engineering
Chalmers University of Technology

ABSTRACT

The development of fault tolerant embedded control systems such as flight control systems, FCS, are currently highly specialized and time consuming. We introduce a conceptual architecture for the next decade control system where all control and logic is distributed to a number of computer nodes locally linked to actuators and connected via a communication network. In this way we substantially decreases the lifecycle cost of such embedded systems and acquires scalable fault tolerance.

The study is based on a FCS for JAS 39 Gripen, a multirole combat aircraft that is statically unstable at subsonic speed. All actuator nodes in our architecture are similar, hardware as well as software wise. Standardizing actuator nodes will even further decrease development and maintenance cost.

INTRODUCTION

All fault tolerance is based on redundancy. Distributed fault tolerance makes it possible to tailor the redundancy according to reliability requirements and to implement the fault tolerance at the most suitable level. Our philosophy is to cover and reconfigure permanent faults with hardware replication and to handle error detection, error processing and, transient or temporal faults with software techniques. Since redundancy is considered in a scalable software architecture, where it is possible to better utilize system resources in the distributed network, the cost for hardware redundancy is minimized. This is achieved by allocating critical software to several nodes in the network in contrast to the traditional approach, in which the same type of redundancy is added locally, i.e. by duplicating or triplicating nodes. This later approach fulfills the dependability requirements, however it is an expensive approach.

Additionally we take advantage of systems intrinsic redundancy, more or less all aircraft, combat or commercial, have redundancy in the use of primary control surfaces i.e. it is possible to maneuver and land the aircraft by commanding a reduced number of primary control surfaces. For JAS 39 Gripen this is used in the design of control laws such that one primary control surface can be failing as long as it fails in a safe way i.e. the FCS must know when and which control surface that fails and it shall fail by streamlining. (Most other embedded control systems for cars, trains etc have similar fail-safe conditions that can be used to reduce the hardware redundancy.)

DISTRIBUTED FCS

With a distributed system, there are several choices on where to put the computing power and the overall control laws and logic. Most mechanical control systems are not particularly computer processing demanding, e.g. all data processing in the flight control system of JAS 39 Gripen is handled by a single computer today. Consequently, in a distributed control system the computational capacity in the nodes

is not considered a limiting factor. Thus it is not mandatory to allocate the tasks according to processing load balance. A future FCS system should be based on distributed control in which the task allocation is optimized according a criterion of minimum bandwidth requirements on the communication system and additionally, allocated to achieve more fault tolerance and low maintenance cost.

ASSUMPTIONS

The computational capacity of microprocessors will increase over the years giving more processing power at a lower cost. Future sensor and actuator elements will be integrated either on the same silicon die or in the same package as the associated micro controller. Hence, wherever there is electronics i.e. a sensor or actuator, there is a node with processing power since the extra cost for data processing is negligible in comparison to cost of hardware devices.

The nodes are fail-silent in the temporal domain, connected through a broadcast bus, the protocol supports for membership agreement. Transient faults must be tolerated with high coverage (0.999).

SYSTEM ARCHITECTURE

Necessary nodes as well as their physical location is given by the elements connected for functionality; sensors, cockpit, nose wheel, engine, control surfaces. The critical sensor nodes and the bus are duplicated. The actuator nodes, one by each primary control surface, are simplex. This is possible since the aircraft is still controllable and able to perform safe landing with six of seven primary control surfaces. The duplicated sensors, the duplicated bus, and the simplex actuators forms the minimum hardware configuration that fulfills the two safety requirements a) less probability of critical failure than $0.5 \cdot 10^{-6}$ per flight hour and b) no single point of failure.

Sensor data available globally give the least traffic on the communication network, hence the minimum bandwidth criterion gives that tasks should be allocated to actuator nodes. We allocate critical tasks redundantly to similar actuator nodes. This gives a high degree of hardware fault detection and fault tolerance for both permanent and transient faults without cost of extra hardware. The computational overhead for doing this is negligible for the studied flight control systems.

With sensor data available globally (broadcast at the communication bus) and replicated actuator nodes with redundant calculations, the system hardware is best utilized. Additionally, the complexity as well as the development cost is reduced. Furthermore, maintainability is improved with a high degree of fault detection and the possibility of identical spare parts.

Note that the developed software of today's centralized FCS with over 10 000 flight hours can be re-used in this future distributed FCS. Hence, design fault and the discussion of N-version programs, which most certainly could be an option with seven control nodes, is not considered in our study.

The National Aerospace Program in Sweden supported this work, NFFP project no 349.