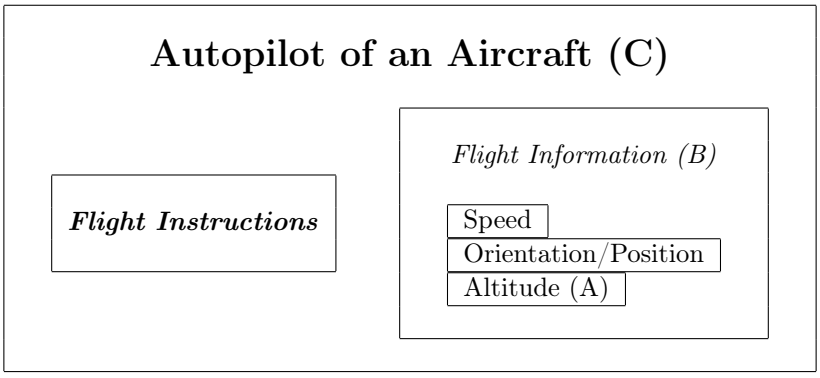
16-124-836
Marcel ZAUDER

1.2 Describing Dependable Systems

We will consider the distributed system embedded in an autopilot of an aircraft:



The autopilot of an aircraft (C) can be easily described as a big system which has two major subparts embedded in it: One is responsible for the flight instructions and the other one is processing and interpreting the flight information which are coming from different sensors as the speed, orientation, and altitude measurements.
If one of these sensors have a malfunction (or domething similar), for example the altitude meter (A), sends wrong data to the processing part of the system which will therefore not work correctly, the autopilot will have a failure and will shut down completely.

A possible FAULT which can occur in the sensor for altitude measuring is that the tube for the pressure measurement is blocked. Therefore we have an ERROR state that the sensor is not working correctly and the FAILURE of outputting the wrong altitude will be the result. This wrong output will have an affect on the flight information processor (B). The FAULT here is that the data received from the sensor is faulty/false which leads to the ERROR that the system cannot process or falsely interpret those data. This has the effect on a false interpretation of where the aircraft currently is and what should be given to the autopilot system (FAILURE).
The autopilot (C) will get wrong information about the current altitude (FAULT) and can therefore not process which instructions should be executed (ERROR). Therefore the autopilot will stop working (FAILURE) and the pilot has to take control.