Software engineering 1a (4 marks) p2q16 RJA

You are building a flight-control system for which a convincing safety case must be made. Would you assign the tasks of safety requirements engineering, test case development and assurance documentation to a separate team, or distribute them among your developers? Justify your answer briefly.

Model answer: I would not use a separate team, except perhaps in the case where the safety functionality could be built into a small, separate, component (which does not hold for flight control). The lessons learned from the near-collapse of IBM, as discussed in the guest lecture, apply here. IBM had separate people doing development and testing, so programmers had every incentive to produce masses of buggy code and throw it over the wall for the other team to fix. That's the last thing you want in a safety-critical system