From Minor Exam:

You've been asked to design the next-generation air traffic control system (ATCS). The ATCS is a complex hardware-software system, with many different sub-systems. The ATCS must work with different types of aeroplanes (speed, size etc.), sensing infrastructure (Radar, lidar, sonar etc), manage communication with pilots, inter alia. Sub-systems could be responsible for
(i) managing landings and take-offs;
(ii) another ground traffic management, etc.

We focussed on managing air traffic landing.

Two critical functional requirements are communication and "early detection warning" capability.

Recall, non-functional properties that you must consider include:
(1) high-availability (> 99.9999% up time);
(2) High-performance (i.e., must support up to 1000 landings per hour)
(3) Fault tolerance (i.e. successfully respond to hardware failure, or incorrect radar readings).
Identify at least one more?

You've created a Use Case, architecture and state diagram.

Now provide answers to the following: (2 points each)

1. Suggest at least two sociotechnical elements that must be took into account when designing ATCS
2. Suggest an architecture that would support fault detection and removal.
3. Identify the major potential hazards as part of the certification process of ATCS.
4. Discuss failure recognition, resistance, recovery, and reinstatement for ATCS. [resilience]
5. Discuss a design for ATCS that enable software reusability. [reusability]

For 1 extra points each:

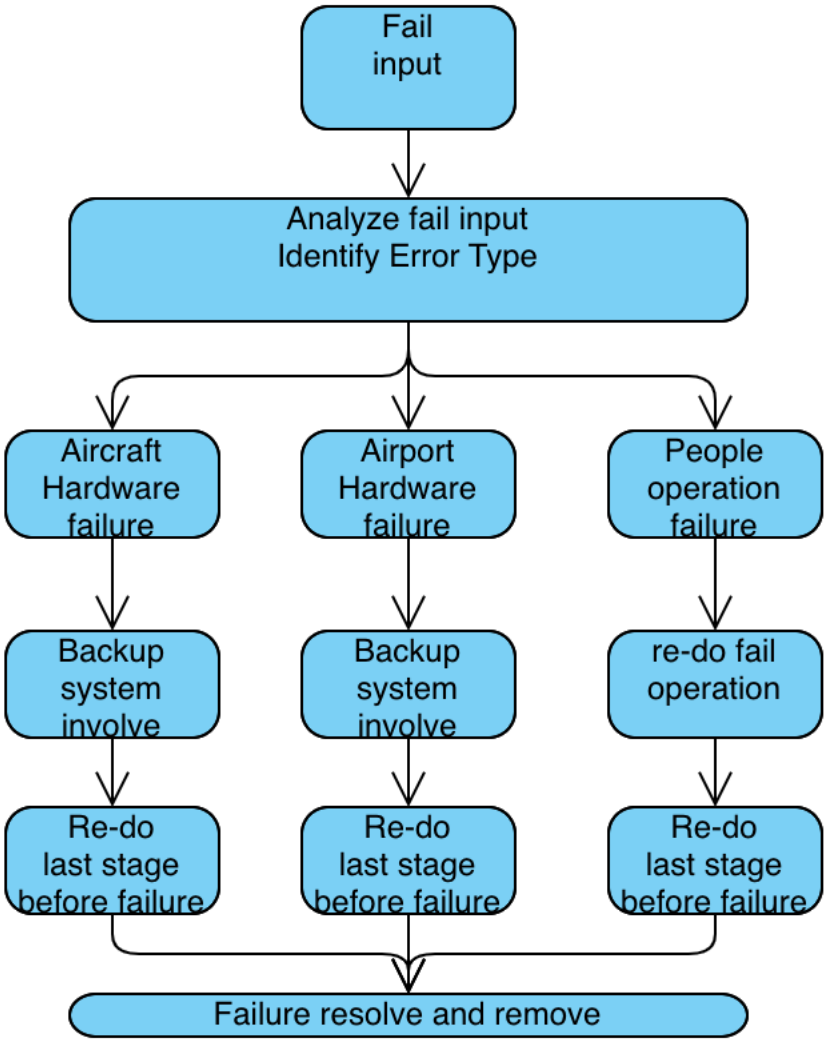
6. Discuss pros and cons of a service-oriented architecture for ATCS. [service-oriented eng]
7. Describe the sociotechnical system that includes ATC. [system of systems]

Answer:

1. Suggest at least two sociotechnical elements that must be took into account when designing ATCS

    1. Company policies changes: When company policies change the original workflow might have to change to adopt new company policies.
    2. Process changes: When the implementation of a new system (failure detection system for example), employees might need to change the way they work. It is essential to take this element in account when design ATCS.

2. Suggest an architecture that would support fault detection and removal



3. Identify the major potential hazards as part of the certification process of ATCS.

    1. Power failure: One of the most critical hazards which threat to ATCS. Power failure means that's no aircraft can land or take off and the polit cannot see the airport.
    2. Aircraft monitoring system fail: If this hazard happens. ATCS cannot monitor aircrafts which causes the airport cannot operate.

4. Discuss failure recognition, resistance, recovery, and reinstatement for ATCS. [resilience]

    1. Failure recognition: Possible failure should be recognized before it occurs. For ATCS, it requires 99% higher fault tolerance. It is directly related to the safety issue of passengers.
    2. Failure resistance: Even though ACTS has fault tolerance ability, but there is no guarantee that the system is 100% safe. ACTS should have failure resistance ability to reduce the damage after failure occurs. For example, emergency power system to supply power when power failure occurs.
    3. Failure recovery: The strategy helps system to recover after system failure happen. For instance, if the weather observe system is unavailable, this strategy should have other source to obtain weather information to keep airport operation.
    4. Failure reinstatement: After this stage, all sub-system of ACTS should be restored and work perfectly.

5. Discuss a design for ATCS that enable software reusability. [reusability]
   Like many automotive vehicle systems or any public transportation systems, the development of ATCS must includes many sub-systems that were used. Safety related systems usually have long development time and long verification stage. For ATCS, GPS system, navigation system, ground light control system.