19

Setting Requirements

Cary R. Spitzer
AvioniCon, Inc.

19.1 Requirements-Setting for Avionics Systems

Proper requirements are the *sine qua non* for building an acceptable avionics system. It is inescapable: No avionics systems can perform as expected by the customer unless the customer requirements, along with requirements from other stakeholders and relevant regulations and standards, are completely documented and understood by the avionics manufacturer. Safety, mission, cost, and certification drive the requirements.

For all aircraft, safety of flight in all possible flight regimes is the prime requirement. All aircraft without the possibility of ejection in case of an emergency typically have a probability of catastrophic failure on the order 10^{-9} per flight hour. If the crew has the potential to eject in case of an emergency the probability of failure is somewhat less demanding, but still significant.

Second only to safety, the mission of the aircraft is the principal driver of requirements. Mission requirements may be in terms of aircraft performance, ground turnaround times, or maintenance practices. Virtually every mission requirement translates into an avionics requirement in some form.

Life cycle cost is of great importance in civil aircraft and is of increasing performance in military aircraft, more specifically the emerging Joint Strike Fighter. For a typical commercial transport aircraft the acquisition cost is approximately 20 to 25% of the total life cycle cost. In military aircraft, the acquisition cost is probably a smaller fraction of the life cycle cost. It is interesting to note that for the life cycle cost for civil avionics the acquisition cost rises to 60% of the total. Avionics life cycle cost, for example, will drive, the need for built-in testing, fault tolerance, and the ratio of mean time between unscheduled removals (MTBUR) and mean time between failure (MTBF.)

Finally, certification is a major factor in avionics design. As the complexity and criticality of avionics increases so does the need for extensive certification activities. Certification issues begin with the initial definition of requirements and last until the equipment is removed from the aircraft or the aircraft is retired.

It is important to note that the requirements definition, especially after the preliminary requirements are set, is very much an iterative process between the customer and the vendor, often under the purview of a Configuration Control Board. This configuration control process, which is sometimes viewed as an intrusion on the real work, is necessary to ensure that everyone is cognizant of proposed changes to requirements and can comment on them.

Aircraft functional requirements are at the top of the requirements hierarchy. The aircraft mission is broken into phases including preflight checkout, taxi out, take-off, cruise, descent, landing, rollout, taxi in, and postflight. Additional specialized mission phases such as weather diversions, cargo drop, electronic warfare, etc. also drive the aircraft performance requirements.

Typical aircraft functional requirements include ground steering and braking, passenger comfort, navigation, communication, and environmental conditioning. Figure 19.1 shows the breakdown (function decomposition) of requirements from the aircraft level to the avionics function level. Requirements

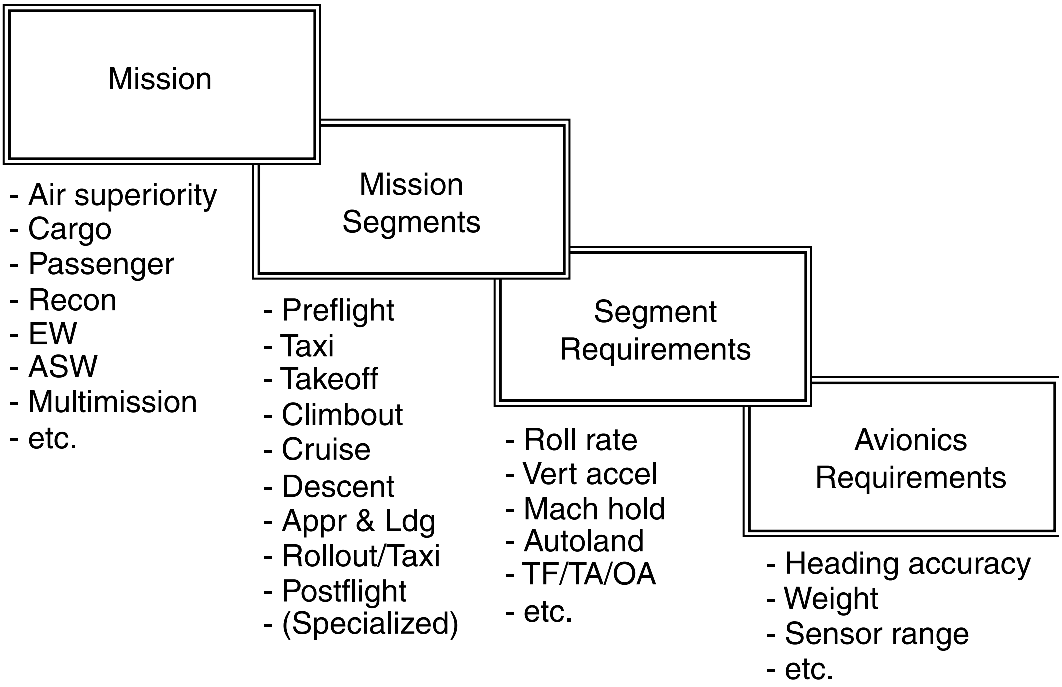

FIGURE 19.1 Function decomposition.

must be traceable and justified. In some cases every "shall" is numbered and then accounted for in test plans to demonstrate that it has been met.

An excellent example of military aircraft avionics top-level requirements is found in AFWAL-TR-1114 Architecture Specification for PAVE PILLAR Avionics. These requirements were postulated for a hypothetical high-performance fighter and guided the definition of the requirements for the F-22 Raptor (see Chapter 32). Typical PAVE PILLAR avionics requirements include:

- Two-level maintenance (flight line or depot)
- Combat turnaround time: ≤15 min
- Non-mission capable (for avionics): ≤1.2%
- Fault detection: 99% of all possible faults
- Fault isolation: 98% of all possible faults

Aerospace Recommended Practice (ARP) 4754 Certification Considerations for Highly-Integrated or Complex Aircraft Systems offers guidance on an aircraft-level Function Hazard Assessment (FHA) that addresses the effect on aircraft performance if a function is lost. The output of an FHA is function criticality and safety requirements, e.g., a "critical" function that must have a probability of failure of less than 10^{-9} per flight hour. This output, in turn, becomes an input to the system design and system-level FHAs. ARP 4761 System Safety Assessment, contains guidance on how to conduct the various analyses required by ARP 4754, including the well-known fault tree analysis and failure modes and effects analysis.

As requirements become more detailed the definition process becomes more amenable to automation. Computer-based processes enhance requirements traceability and validation, configuration control, and document generation. Examples of computer-based techniques include modeling and simulation (see Chapter 20), Systems Workshop, an Aerospatiale proprietary tool for use on Airbus Industrie products (see Chapter 30), and formal methods based on rigorous mathematical concepts (see Chapter 21).

DOD-HDBK-763 Human Engineering Procedures Guide is a valuable source of example techniques for determining requirements as they flow down and become more detailed. The emphasis in this handbook is, of course, on the human factors aspect, but there is a wealth of detailed general information on defining requirements.

Derived requirements are lower-level requirements that could not (or should not) be defined at the beginning of the avionics design process. Microprocessor selection is an example.

References

AFWAL-TR-87-1114, "Architecture Specification for PAVE PILLAR Avionics," January, 1987.

"Certification Considerations for Highly-Integrated or Complex Aircraft Systems," ARP 4754, SAE; 1996.

Palmer, Michael T., et al., "A Crew-Centered Flight Deck Design Philosophy for High Speed Civil Transport (HSCT) Aircraft," NASA Technical Memorandum 109171; January, 1995.

DOD-HDBK-763 Human Engineering Procedures Guide, 27 February, 1987.

"System Safety Assessment," ARP 4761, SAE; 1996.