(2) *Federal launch range.* This provision applies to all sections of this subpart. The FAA will accept a flight safety system used or approved on a Federal launch range without need for further demonstration of compliance to the FAA if:

(i) A launch operator has contracted with a Federal launch range for the provision of flight safety system property and services; and

(ii) The FAA has assessed the Federal launch range, through its launch site safety assessment, and found that the Federal launch range's flight safety system property and services satisfy the requirements of this subpart. In this case, the FAA will treat the Federal launch range's flight safety system property and services as that of a launch operator.

§ 417.303   Command control system requirements.

(a) *General.* When initiated by a flight safety official, a command control system must transmit a command signal that has the radio frequency characteristics and power needed for receipt of the signal by the onboard vehicle flight termination system. A command control system must include all of the following:

(1) All flight termination system activation switches;

(2) All intermediate equipment, linkages, and software;

(3) Any auxiliary stations;

(4) Each command transmitter and transmitting antenna; and

(5) All support equipment that is critical for reliable operation, such as power, communications, and air conditioning systems.

(b) *Performance specifications.* A command control system and each subsystem, component, and part that can affect the reliability of a component must have written performance specifications that demonstrate, and contain the details of, how each satisfies the requirements of this section.

(c) *Reliability prediction.* A command control system must have a predicted reliability of 0.999 at the 95 percent confidence level when operating, starting with completion of the preflight testing and system verification of § 417.305(c) through initiation of flight and until the planned safe flight state for each launch. Any demonstration of the system's predicted reliability must satisfy § 417.309(b).

(d) *Fault tolerance.* A command control system must not contain any single-failure-point that, upon failure, would inhibit the required functioning of the system or cause the transmission of an undesired flight termination message. A command control system's design must ensure that the probability of transmitting an undesired or inadvertent command during flight is less than 1×10^{-7}.

(e) *Configuration control.* A command control system must undergo configuration control to ensure its reliability and compatibility with the flight termination system used for each launch.

(f) *Electromagnetic interference.* Each command control system component must function within the electromagnetic environment to which it is exposed. A command control system must include protection to prevent interference from inhibiting the required functioning of the system or causing the transmission of an undesired or inadvertent flight termination command. Any susceptible remote control data processing or transmitting system that is part of the command control system must prevent electromagnetic interference.

(g) *Command transmitter failover.* A command control system must include independent, redundant transmitter systems that automatically switch, or "fail-over," from a primary transmitter to a secondary transmitter when a condition exists that indicates potential failure of the primary transmitter. The switch must be automatic and provide all the same command control system capabilities through the secondary transmitter system. The secondary transmitter system must respond to any transmitter system configuration and radio message orders established for the launch. The fail-over criteria that trigger automatic switching from the primary transmitter to the secondary transmitter must account for each of the following transmitter performance parameters and failure indicators:

(1) Low transmitter power;

(2) Center frequency shift;

(3) Out of tolerance tone frequency;

(4) Out of tolerance message timing;

(5) Loss of communication between central control and transmitter site;

(6) Central control commanded status and site status disagree;

(7) Transmitter site fails to respond to a configuration or radiation order within a specified period of time; and

(8) For a tone-based system, tone deviation and tone imbalance.

(h) *Switching between transmitter systems.* Any manual or automatic switching between transmitter systems, including fail-over, must not result in the radio carrier being off the air long enough for any command destruct system to be captured by an unauthorized transmitter. The time the radio carrier is off the air must account for any loss of carrier and any simultaneous multiple radio carrier transmissions from two transmitter sites during switching.

(i) *Radio carrier.* For each launch, a command control system must provide all of the following:

(1) The radio frequency signal and radiated power density that each command destruct system needs to activate during flight;

(2) The 12-dB power density margin required by section D417.9(d) of appendix D of this part under nominal conditions; and

(3) A 6-dB power density margin under worst-case conditions.

(j) *Command control system monitoring and control.* A command control system must provide for monitoring and control of the system from the flight safety system displays and controls required by § 417.307(g), including real-time selection of a transmitter, transmitter site, communication circuits, and antenna configuration.

(k) *Command transmitter system.* For each launch, a command transmitter system must:

(1) Transmit signals that are compatible with any command destruct system's radio frequency receiving system of section D417.25 and command receiver decoder of section D417.29 of appendix D of this part;

(2) Ensure that all arm and destruct commands transmitted to a flight termination system have priority over any other commands transmitted;

(3) Employ an authorized radio carrier frequency and bandwidth with a guard band that provides the radio frequency separation needed to ensure that the system does not interfere with any other flight safety system that is required to operate at the same time;

(4) Transmit an output bandwidth that is consistent with the signal spectrum power used in the link analysis of § 417.309(f); and

(5) Not transmit other frequencies that could degrade the airborne flight termination system's performance.

(l) *Command control system antennas.* A command control system antenna or antenna system must satisfy all of the following:

(1) The antenna system must provide two or more command signals to any command destruct system throughout normal flight and in the event of a launch vehicle failure regardless of launch vehicle orientation;

(2) Each antenna beam-width must:

(i) Allow for complete transmission of the command destruct sequence of signal tones before a malfunctioning launch vehicle can exit the 3-dB point of the antenna pattern;

(ii) When the vehicle is centered in the antenna pattern at the beginning of the malfunction, account for the launch vehicle's malfunction turn capability determined by the analysis of § 417.209, the data loss flight times of § 417.219, and the time delay of § 417.221.

(iii) Encompass the boundaries of normal flight for the portion of flight that the antenna is scheduled to support; and

(iv) Account for any error associated with launch vehicle tracking and pointing of the antenna;

(3) The location of each antenna must provide for an unobstructed line of site between the antenna and the launch vehicle;

(4) The antenna system must provide a continuous omni-directional radio carrier pattern that covers the launch vehicle's flight from the launch point to no less than an altitude of 50,000 feet above sea level, unless the system uses a steerable antenna that satisfies paragraphs (l)(1) and (2) of this section for the worst-case launch vehicle malfunction that could occur during that portion of flight;

(5) An antenna must radiate circularly polarized radio waves that are compatible with the flight termination system antennas on the launch vehicle; and

(6) Any steerable antenna must allow for control of the antenna manually at the antenna site or by remote slaving data from a launch vehicle tracking source. A steerable antenna's positioning lag, accuracy, and slew rates must allow for tracking a nominally performing launch vehicle within one half of the antenna's beam-width and for tracking a malfunctioning launch vehicle to satisfy paragraph (l)(2) of this section.

§ 417.305 Command control system testing.

(a) *General.* (1) A command control system, including its subsystems and components must undergo the acceptance testing of paragraph (b) of this section when new or modified. For each launch, a command control system must undergo the preflight testing of paragraph (c) of this section.

(2) Each acceptance and preflight test must follow a written test plan that specifies the procedures and test parameters for the test and the testing sequence. A test plan must include instructions on how to handle procedural deviations and how to react to test failures.

(3) If hardware or software is redesigned or replaced with a different hardware or software that is not identical to the original, the system must undergo all acceptance testing and analysis with the new hardware or software and all preflight testing for each launch with the new hardware or software.

(4) After a command control system passes all acceptance tests, if a component is replaced with an identical component, the system must undergo testing to ensure that the new component is installed properly and is operational.

(b) *Acceptance testing.* (1) All new or modified command control system hardware and software must undergo acceptance testing to verify that the system satisfies the requirements of § 417.303.

(2) Acceptance testing must include functional testing, system interface validation testing, and integrated system-wide validation testing.

(3) Each acceptance test must measure the performance parameters that demonstrate whether the requirements of § 417.303 are satisfied.

(4) Any computing system, software, or firmware that performs a software safety critical function must undergo validation testing and satisfy § 417.123. If command control system hardware interfaces with software, the interface must undergo validation testing.

(c) *Preflight testing*—(1) *General.* For each launch, a command control system must undergo preflight testing to verify that the system satisfies the requirements of § 417.303 for the launch.

(1) *General.* For each launch, a command control system must undergo preflight testing to verify that the system satisfies the requirements of § 417.303 for the launch.

(2) *Coordinated command control system and flight termination system testing.* For each launch, a command control system must undergo preflight testing during the preflight testing of the associated flight termination system under section E417.41 of appendix E of this part.

(3) *Command transmitter system carrier switching tests.* A command transmitter system must undergo a test of its carrier switching system no earlier than 24 hours before a scheduled flight. The test must satisfy all of the following:

(i) *Automatic carrier switching.* For any automatic carrier switching system, the test must verify that the switching algorithm selects and enables the proper transmitter site for each portion of the planned flight; and

(ii) *Manual carrier switching.* For any manual carrier switching, the test must verify that the flight safety system crew can select and enable each transmitter site planned to support the launch.

(4) *Independent radio frequency open loop verification tests.* A command control system must undergo an open loop end-to-end verification test for each launch as close to the planned flight as operationally feasible and after any modification to the system or break in the system configuration. The test must: