(i) Verify the performance of each element of the system from the flight safety system displays and controls to each command transmitter site;

(ii) Measure all system performance parameters received and transmitted using measuring equipment that does not physically interface with any elements of the operational command control system;

(iii) Verify the performance of each flight safety system display and control and remote command transmitter site combination by repeating all measurements for each combination, for all strings and all operational configurations of cross-strapped equipment; and

(iv) Verify that all critical command control system performance parameters satisfy all their performance specifications. These parameters must include:

(A) Transmitter power output;

(B) Center frequency stability;

(C) Tone deviation;

(D) Tone frequency;

(E) Message timing;

(F) Status of each communication circuit between the flight safety system display and controls and any supporting command transmitter sites;

(G) Status agreement between the flight safety system display and controls and each and any supporting command transmitter sites;

(H) Fail-over conditions;

(I) Tone balance; and

(J) Time delay from initiation of a command at each flight safety system control to transmitter output of the command signal.

(d) *Test reports.* If a Federal launch range oversees the safety of a launch, the range's requirements are consistent with this subpart, and the range provides and tests the command control system, a launch operator need only obtain the range's verification that the system satisfies all the test requirements. For any other case a launch operator must prepare or obtain one or more written reports that:

(1) Verify that the command control system satisfies all the test requirements;

(2) Describe all command control system test results and test conditions;

(3) Describe any analysis performed instead of testing;

(4) Identify by serial number or other identification each test result that applies to each system or component;

(5) Describe any test failure or anomaly, including any variation from an established performance baseline, each corrective action taken, and all results of any additional tests; and

(6) Identify any test failure trends.

§417.307 Support systems.

(a) *General.* (1) A flight safety system must include the systems required by this section to support the functions of the flight safety system crew, including making a flight termination decision.

(2) Each support system and each subsystem, component, and part that can affect the reliability of the support system must have written performance specifications that demonstrate, and contain the details of, how each satisfies the requirements of this section.

(3) For each launch, each support system must undergo testing to ensure it functions according to its performance specifications.

(b) *Launch vehicle tracking.* (1) A flight safety system must include a launch vehicle tracking system that provides launch vehicle position and status data to the flight safety crew from the first data loss flight time until the planned safe flight state for the launch.

(2) The tracking system must consist of at least two sources of launch vehicle position data. The data sources must be independent of one another, and at least one source must be independent of any vehicle guidance system.

(3) All ground tracking systems and components must be compatible with any tracking system components onboard the launch vehicle.

(4) If a tracking system uses radar as one of the independent tracking sources, the system must:

(i) Include a tracking beacon onboard the launch vehicle; or

(ii) If the system relies on skin tracking, it must maintain a tracking margin of no less than 6 dB above noise throughout the period of flight that

the radar is used. The flight safety limits must account for the larger tracking errors associated with skin tracking.

(5) The tracking system must provide real-time data to the flight safety data processing, display, and recording system required by paragraph (e) of this section.

(6) For each launch, each tracking source must undergo validation of its accuracy. For each stage of flight that a launch vehicle guidance system is used as a tracking source, a tracking source that is independent of any system used to aid the guidance system must validate the guidance system data before the data is used in the flight termination decision process.

(7) The launch vehicle tracking error from all sources, including data latency and any possible gaps or dropouts in tracking coverage, must be consistent with the flight safety limits of § 417.213 and the flight safety system time delay of § 417.221.

(8) Any planned gap in tracking coverage must not occur at the same time as any planned switching of command transmitters.

(c) *Telemetry*. (1) A flight safety system must include a telemetry system that provides the flight safety crew with accurate flight safety data during preflight operations and during flight until the planned safe flight state.

(2) The onboard telemetry system must monitor and transmit the flight termination system monitoring data of section D417.17 and any launch vehicle tracking data used to satisfy paragraph (b) of this section.

(3) The telemetry receiving system must acquire, store, and provide real-time data to the flight safety data processing, display, and recording system required by paragraph (e) of this section.

(d) *Communications network*. A flight safety system must include a communications network that connects all flight safety functions with all launch control centers and any down-range tracking and command transmitter sites. The system must provide for recording all required data and all voice communications channels during launch countdown and flight.

(e) *Data processing, display, and recording*. A flight safety system must include one or more subsystems that process, display, and record flight safety data to support the flight safety crew's monitoring of the launch, including the data that the crew uses to make a flight termination decision. The system must:

(1) Satisfy § 417.123 for any computing system, software, or firmware that must operate properly to ensure the accuracy of the data;

(2) Receive vehicle status data from tracking and telemetry, evaluate the data for validity, and provide valid data for display and recording;

(3) Perform any reformatting of the data as appropriate and forward it to display and recording devices;

(4) Display real-time data against background displays of the nominal trajectory and flight safety limits established in accordance with the flight safety analysis required by subpart C of this part;

(5) Display and record raw input and processed data at a rate that maintains the validity of the data and at no less than 0.1-second intervals;

(6) Record the timing of when flight safety system commands are input by the flight safety crew; and

(7) Record all health and status parameters of the command control system, including the transmitter failover parameters, command outputs, check channel or pilot tone monitor, and status of communications.

(f) *Displays and controls*. (1) A flight safety system must include the displays of real-time data and controls that the flight safety crew needs to perform all its functions, such as to monitor and evaluate launch vehicle performance, communicate with other flight safety and launch personnel, and initiate flight termination.

(2) A flight safety system must present all data that the flight safety crew needs to ensure that all flight commit criteria are satisfied for each launch, such as hazard area surveillance, any aircraft and ship traffic information, meteorological conditions, and the flight termination system monitoring data of section D417.17.

(3) The real-time displays must include all data that the flight safety

crew needs to ensure the operational functionality of the flight safety system, including availability and quality, and that all flight termination rules are satisfied for each launch, such as:

(i) Launch vehicle tracking data, such as instantaneous vacuum impact point, drag corrected debris footprint, or present launch vehicle position and velocities as a function of time;

(ii) Vehicle status data from telemetry, including yaw, pitch, roll, and motor chamber pressure;

(iii) The flight termination system monitoring data of section D417.17;

(iv) Background displays of nominal trajectory, flight safety limits, data loss flight times, planned safe flight state, and any overflight gate through a flight safety limit all as determined by the flight safety analysis required by subpart C of this part; and

(v) Any video data when required by the flight safety crew to perform its functions, such as video from optical program and flight line cameras.

(4) The controls must allow the flight safety crew to turn a command transmitter on and off, manually switch from primary to backup transmitter antenna, and switch between each transmitter site. These functions may be accomplished through controls available to command transmitter support personnel and communications between those personnel and the flight safety crew.

(5) Each set of command transmitter system controls must include a means of identifying when it has primary control of the system.

(6) The displays must include a means of immediately notifying the flight safety system crew of any automatic fail-over of the system transmitters.

(7) All flight safety system controls must be dedicated to the flight safety system and must not rely on time or equipment shared with other systems.

(8) All data transmission links between any control, transmitter, or antenna must consist of two or more complete and independent duplex circuits. The routing of these circuits must ensure that they are physically separated from each other to eliminate any potential single failure point in the command control system in accordance with §417.303(d).

(9) The system must include hardware or procedural security provisions for controlling access to all controls and other related hardware. These security provisions must ensure that only the flight safety crew can initiate a flight safety system transmission.

(10) The system must include two independent means for the flight safety crew to initiate arm and destruct messages. The location and functioning of the controls must provide the crew easy access to the controls and prevent inadvertent activation.

(11) The system must include a digital countdown for use in implementing the flight termination rules of §417.113 that apply data loss flight times and the planned safe flight state. The system must also include a manual method of applying the data loss flight times in the event that the digital countdown malfunctions.

(g) *Support equipment calibration.* Each support system and any equipment used to test flight safety system components must undergo calibration to ensure that measurement and monitoring devices that support a launch provide accurate indications.

(h) *Destruct initiator simulator.* A flight safety system must include one or more destruct initiator simulators that simulate each destruct initiator during the flight termination system preflight tests. Each destruct initiator simulator must:

(1) Have electrical and operational characteristics matching those of the actual destruct initiator;

(2) Monitor the firing circuit output current, voltage, or energy, and indicate whether the firing output occurs. The indication that the output occurred must remain after the output is removed;

(3) Have the ability to remain connected throughout ground processing until the electrical connection of the actual initiators is accomplished;

(4) Include a capability that permits the issuance of destruct commands by test equipment only if the simulator is installed and connected to the firing lines; and

(5) For any low voltage initiator, provide a stray current monitoring device

in the firing line. The stray current monitoring device, such as a fuse or automatic recording system, must be capable of indicating a minimum of one-tenth of the maximum no-fire current.

(i) *Timing.* A flight safety system must include a timing system that is synchronized to a universal time coordinate. The system must:

(1) Initiate first motion signals;

(2) Synchronize flight safety system instrumentation, including countdown clocks; and

(3) Identify when, during countdown or flight, a data measurement or voice communication occurs.

§ 417.309 Flight safety system analysis.

(a) *General.* (1) Each flight termination system and command control system, including each of their components, must satisfy the analysis requirements of this section.

(2) Each analysis must follow an FAA approved system safety and reliability analysis methodology.

(b) *System reliability.* Each flight termination system and command control system must undergo an analysis that demonstrates the system's predicted reliability. Each analysis must:

(1) Account for the probability of a flight safety system anomaly occurring and all of its effects as determined by the single failure point analysis and the sneak circuit analysis required by paragraphs (c) and (g) of this section;

(2) Demonstrate that each system satisfies the predicted reliability requirement of 0.999 at the 95 percent confidence level;

(3) Use a reliability model that is statistically valid and accurately represents the system;

(4) Account for the actual or predicted reliability of all subsystems and components;

(5) Account for the effects of storage, transportation, handling, maintenance, and operating environments on component predicted reliability; and

(6) Account for the interface between the launch vehicle systems and the flight termination system.

(c) *Single failure point.* A command control system must undergo an analysis that demonstrates that the system satisfies the fault tolerance requirements of § 417.303(d). A flight termination system must undergo an analysis that demonstrates that the system satisfies the fault tolerance requirements of section D417.5(b). Each analysis must:

(1) Follow a standard industry methodology such as a fault tree analysis or a failure modes effects and criticality analysis;

(2) Identify all possible failure modes and undesired events, their probability of occurrence, and their effects on system performance;

(3) Identify single point failure modes;

(4) Identify areas of design where redundancy is required and account for any failure mode where a component and its backup could fail at the same time due to a single cause;

(5) Identify functions, including redundancy, which are not or cannot be tested;

(6) Account for any potential system failures due to hardware, software, test equipment, or procedural or human errors;

(7) Account for any single failure point on another system that could disable a command control system or flight termination system, such as any launch vehicle system that could trigger safing of a flight termination system; and

(8) Provide input to the reliability analysis of paragraph (b) of this section.

(d) *Fratricide.* A flight termination system must undergo an analysis that demonstrates that the flight termination of any stage, at any time during flight, will not sever interconnecting flight termination system circuitry or ordnance to other stages until flight termination on all the other stages has been initiated.

(e) *Bent pin.* Each component of a flight termination system and command control system must undergo an analysis that demonstrates that any single short circuit occurring as a result of a bent electrical connection pin will not result in inadvertent system activation or inhibiting the proper operation of the system.

(f) *Radio frequency link.* (1)The flight safety system must undergo a radio frequency link analysis to demonstrate