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

that it satisfies the required 12-dB margin for nominal system performance and 6-dB margin for worst-case system performance.

(2) When demonstrating the 12-dB margin, each link analysis must account for the following nominal system performance and attenuation factors:

(i) Path losses due to plume or flame attenuation;

(ii) Vehicle trajectory;

(iii) Ground system and airborne system radio frequency characteristics; and

(iv) The antenna gain value that ensures that the margin is satisfied over 95% of the antenna radiation sphere surrounding the launch vehicle.

(3) When demonstrating the 6-dB margin, each link analysis must account for the following worst-case system performance and attenuation factors:

(i) The system performance and attenuation factors of paragraph (f)(2) of this section;

(ii) The command transmitter failover criteria of §417.303(g) including the lowest output power provided by the transmitter system;

(iii) Worst-case power loss due to antenna pointing inaccuracies; and

(iv) Any other attenuation factors.

(g) *Sneak circuit.* Each electronic component that contains an electronic inhibit that could inhibit the functioning, or cause inadvertent functioning of a flight termination system or command control system, must undergo a sneak circuit analysis. The analysis must demonstrate that there are no latent paths of an unwanted command that could, when all components otherwise function properly, cause the occurrence of an undesired, unplanned, or inhibited function that could cause a system anomaly. The analysis must determine the probability of an anomaly occurring for input to the system reliability analysis of paragraph (b) of this section.

(h) *Software and firmware.* Any computing system, software, or firmware that performs a software safety critical function must undergo the analysis needed to ensure reliable operation and satisfy §417.123.

(i) *Battery capacity.* A flight termination system must undergo an analysis that demonstrates that each flight termination system battery has a total amp hour capacity of no less than 150% of the capacity needed during flight plus the capacity needed for load and activation checks, preflight and launch countdown checks, and any potential launch hold time. For a launch vehicle that uses any solid propellant, the analysis must demonstrate that the battery capacity allows for an additional 30-minute hang-fire hold time. The battery analysis must also demonstrate each flight termination system battery's ability to meet the charging temperature and current control requirements of appendix D of this part.

(j) *Survivability.* A flight termination system must undergo an analysis that demonstrates that each subsystem and component, including their location on the launch vehicle, provides for the flight termination system to complete all its required functions when exposed to:

(1) Breakup of the launch vehicle due to aerodynamic loading effects at high angle of attack trajectories during early stages of flight, including the effects of any automatic or inadvertent destruct system;

(2) An engine hard-over nozzle induced tumble during each phase of flight for each stage; or

(3) Launch vehicle staging, ignition, or any other normal or abnormal event that, when it occurs, could damage flight termination system hardware or inhibit the functionality of any subsystem or component, including any inadvertent separation destruct system.

§417.311 Flight safety crew roles and qualifications.

(a) A flight safety crew must operate the flight safety system hardware. A flight safety crew must document each flight safety crew position description and maintain documentation on individual crew qualifications, including education, experience, and training as part of the personnel certification program required by §417.105.

(b) A flight safety crew must be able to demonstrate the knowledge, skills, and abilities needed to operate the