AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

account for conditions, acts, or chain of events that can result in a hazard. The ground safety analysis must account for the possible failure of any control or monitoring circuitry within hardware systems that can cause a hazard.

(i) A ground safety analysis must identify the hazard controls to be established by a launch operator for each hazard cause identified in paragraph (h) of this section. A launch operator's hazard controls include the use of engineering controls for the containment of hazards within defined areas and the control of public access to those areas.

(j) A launch operator must verify all information in a ground safety analysis, including design margins, fault tolerance and successful completion of tests. A launch operator must:

(1) Trace any identified hardware to an engineering drawing or other document that describes hardware configuration;

(2) Trace any test or analysis used in developing the ground safety analysis to a report or memorandum that describes how the test or analysis was performed;

(3) Ensure the accuracy of the test or analysis and the associated results;

(4) Trace any procedural hazard control identified to a written procedure, and approved by the person designated under §417.103(b)(2) or the person's designee, with the paragraph or step number of the procedure specified;

(5) Identify a verifiable hazard control for each hazard; if a hazard control is not verifiable, a launch operator may include it as an informational note on the hazard analysis form;

(6) For each hazard control, reference a released drawing, report, procedure or other document that verifies the existence of the hazard control; and

(7) Maintain records, as required by §417.15, of the documentation that verifies the information in the ground safety analysis.

(k) A launch operator must ensure the continuing accuracy of its ground safety analysis. The analysis of systems and operations must not end upon submission of a ground safety analysis report to the FAA during the license application process. A launch operator must analyze each new or modified system or operation for potential hazards that can affect the public. A launch operator must ensure that each existing system and operation is subject to continual scrutiny and that the information in a ground safety analysis report is kept current.

§417.407 Hazard control implementation.

(a) *General*. A launch operator must establish and maintain the hazard controls identified by the ground safety analysis including:

(1) System hazard controls that satisfy §417.409;

(2) Safety clear zones for hazardous operations that satisfy §417.411;

(3) Hazard areas and controls for allowing public access that satisfy §417.413;

(4) Hazard controls after launch or an attempt to launch that satisfy §417.415; and

(5) Controls for propellant and explosive hazards that satisfy §417.417.

(b) *Hazard control verification*. A launch operator must establish a hazard tracking process to ensure that each identified hazard has a verifiable hazard control. Verification status must remain ''open'' for an individual hazard control until the hazard control is verified to exist in a released drawing, report, procedure, or similar document.

(c) *Hazard control configuration control*. A launch operator must establish and maintain a configuration control process for safety critical hardware. Procedural steps to verify hazard controls, and their associated documentation, cannot be changed without coordination with the person designated in §417.103(b)(2).

(d) *Inspections*. When a potential hazard exists, a launch operator must conduct periodic inspections of related hardware, software, and facilities. A launch operator must ensure qualified and certified personnel, as required by §417.105, conduct the inspection. A launch operator must demonstrate that the time interval between inspections is sufficient to ensure satisfaction of this subpart. A launch operator must ensure safety devices and other hazard controls must remain in place for that hazard, and that safety devices

and other hazard controls must remain in working order so that no unsafe conditions exist.

(e) *Procedures.* A launch operator must conduct each launch processing or post-launch operation involving a public hazard or a launch location hazard pursuant to written procedures that incorporate the hazard controls identified by a launch operator's ground safety analysis and as required by this subpart. The person designated in § 417.103(b)(2) must approve the procedures. A launch operator must maintain an ''as-run'' copy of each procedure. The ''as-run'' procedure copy must include changes, start and stop dates, and times that each procedure was performed and observations made during the operations.

(f) *Hazardous materials.* A launch operator must establish procedures for the receipt, storage, handling, use, and disposal of hazardous materials, including toxic substances and sources of ionizing radiation. A launch operator must establish procedures for responding to hazardous material emergencies and protecting the public that complies with the accident investigation plan as defined in § 417.111(h)(2). These procedures must include:

(1) Identification of each hazard and its effects;

(2) Actions to be taken in response to release of a hazardous material;

(3) Identification of protective gear and other safety equipment that must be available in order to respond to a release;

(4) Evacuation and rescue procedures;

(5) Chain of command; and

(6) Communication both on-site and off-site to surrounding communities and local authorities.

(g) *Toxic release hazard notifications and evacuations.* A launch operator must perform a toxic release hazard analysis for launch processing performed at the launch site that satisfies section I417.7 of this part. A launch operator must apply toxic plume modeling techniques that satisfy section I417.7 of this part and ensure that notifications and evacuations are accomplished to protect the public from potential toxic release.

§ 417.409 System hazard controls.

(a) *General.* A launch operator must establish and maintain hazard controls for each system that presents a public hazard as identified by the ground safety analysis and satisfy the requirements of this section. A launch operator must:

(1) Ensure a system be at least single fault tolerant to creating a public hazard unless other hazard control criteria are specified for the system by the requirements of this part. A system capable of creating a catastrophic public hazard must be at least dual fault tolerant. Dual fault tolerant system hazard controls include: Switches, valves, or similar components that prevent an unwanted transfer or release of energy or hazardous materials;

(2) Ensure each hazard control used to provide fault tolerance is independent from other hazard controls so that no single action or event can remove more than one inhibit. A launch operator must prevent inadvertent activation of hazard control devices such as switches and valves;

(3) Provide at least two fully redundant safety devices if a safety device must function in order to control a public hazard. A single action or event must not be capable of disabling both safety devices; and

(4) Ensure computing systems and software used to control a public hazard satisfy the requirements of § 417.123.

(b) *Structures and material handling equipment.* A launch operator must ensure safety factors applied in the design of a structure or material handling equipment account for static and dynamic loads, environmental stresses, expected wear, and duty cycles. A launch operator must:

(1) Inspect structures and material handling equipment to verify workmanship, proper operations, and maintenance;

(2) Prepare plans to ensure proper operations and maintenance of structures and material handling equipment;

(3) Assess structures and material handling equipment for potential single point failure;

(4) Eliminate single point failures from structures and material handling equipment or subject the structures