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.
§ 417.409 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