U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: ANOMALY REPORTING AND CORRECTIVE ACTION FOR A REUSABLE SUBORBITAL ROCKET OPERATING UNDER AN EXPERIMENTAL PERMIT

Date: April 20, 2007 **AC No:** 437.73-1
Initiated by: AST-1 **Change:**

1.0 PURPOSE

a. This Advisory Circular (AC) provides guidance for reporting anomalies occurring in reusable suborbital rockets operating under an experimental permit issued by the Federal Aviation Administration (FAA). This AC also provides guidance for implementing an anomaly reporting and corrective action system for reusable suborbital rockets operating under an FAA-issued experimental permit. An acceptable approach to an anomaly reporting and corrective action methodology is described here. Other approaches that fulfill regulatory objectives may be acceptable to the FAA.

b. This AC is not, in itself, mandatory and does not constitute a regulation. It is issued to describe an acceptable means, but not the only means, for demonstrating compliance with certain requirements associated with the launch or reentry of a reusable suborbital rocket.

c. This AC affects any entity that intends to obtain an experimental permit to launch or reenter a reusable suborbital rocket.

2.0 APPLICABLE REGULATIONS AND RELATED DOCUMENTS

a. Regulations

14 CFR III

Part 401, Organization and Definitions

Part 437, Experimental Permits for Reusable Suborbital Rockets

b. FAA Advisory Circulars and Guidance Documents (available through the FAA web site, www.faa.gov)

AC 23.1309-1C, Equipment, Systems, and Installations in Part 23 Airplanes, March 12, 1999.

AC 431.35-2A, Reusable Launch and Reentry Vehicle System Safety Process, July 20, 2005.

Guide to Reusable Launch Vehicle Safety Validation and Verification Planning, Version 1.0, September 2003.

Guide to Reusable Launch and Reentry Vehicle Reliability Analysis, Version 1.0, April 2005.

c. Industry Documents

Goldberg, et al., *System Engineering "Toolbox" for Design-Oriented Engineers*, NASA Reference Publication 1358, December 1994.

3.0 DEFINITIONS

a. **Anomaly.** A problem that occurs during verification or operation of a system, subsystem, process, facility, or support equipment.

b. **Cause and effect diagram.** An analysis that graphically represents the relationships between a problem and its possible causes. This technique is also known as a fishbone or Ishikawa diagram.

c. **Contributing cause.** A reason that an anomaly occurred. A contributing cause indirectly affects the outcome or occurrence but on its own may not create the problem.

d. **Control chart.** A graphical display of a variable in a process used to determine whether that process is within acceptable limits.

e. **Corrective action.** An action taken to eliminate the root cause of an existing anomaly in order to prevent it from happening again.

f. **Energy flow/barrier analysis.** System safety analysis that identifies hazards from energy sources, what could be harmed, and the mitigation measures for those energy sources.

g. **Event sequence diagram.** Qualitative graphical technique that analyzes the order of events likely to occur given that an initiating event has occurred.

h. **Event tree analysis.** System analysis that explores responses to an initiating event and enables assessment of the probabilities of unfavorable or favorable outcomes.

i. **Failure Modes and Effects Analysis (FMEA).** System analysis by which each potential failure in a system is analyzed to determine the effects on the system and to classify each potential failure according to its severity and likelihood.

j. **Fault tree analysis.** Deductive system reliability analysis that provides qualitative and quantitative measures of the probability of an event occurring or of failure of a system, subsystem, or process. A fault tree analysis estimates the probability that a consequence will occur, identifies systematically possible causes leading to that event, and documents the results of the analytic process to provide a baseline for future studies of alternate designs.

k. **Flowchart analysis.** An analysis that uses a pictorial representation of the steps of the process to identify potential sources of problems.

l. **Hazard.** Equipment, system, operation, or condition with an existing or potential condition that may result in loss or harm.

m. **Histogram.** A bar chart that shows a dispersion of data over a specified range.

n. **Initiating events.** Triggering events in sequences of events that ultimately lead to either success or failure.

o. **Key flight-safety event.** A permitted flight activity that has an increased likelihood of causing a launch accident compared with other portions of flight.

p. **Pareto analysis.** A problem solving analysis in which potential problem areas or sources of variation are ranked from the most frequent to the least frequent. A Pareto chart is a type of a histogram.

q. **Preliminary hazard analysis (PHA).** Examination of a system or subsystem to identify and classify each potential hazard according to its severity and likelihood of occurrence and to develop mitigation measures to those hazards.

r. **Preventive action.** An action taken to prevent an anomaly from occurring.

s. **Proximate cause.** The immediate event that sets off a series of events to cause an anomaly. Also known as the direct cause. (See the example on page 6.)

t. **Regression analysis.** An analysis that produces a mathematical model describing the relationship between a variable and the factors that influence it.

u. **Risk.** Measure that takes into consideration the likelihood of occurrence and the consequence of a hazard to people or property.

v. **Risk mitigation.** Process of reducing the likelihood of occurrence, severity of consequences, or both the likelihood and severity of a hazard to people or property.

w. **Root cause.** The fundamental reason that an anomaly occurred.

x. **Root cause analysis.** A systematic investigation of the circumstances and factors leading to an anomaly for purposes of finding the fundamental reason for that anomaly.

y. **Safety critical.** Essential to safe performance or operation. A safety-critical system, subsystem, condition, event, operation, process, or item is one whose proper recognition, control, performance, or tolerance is essential to system operation such that it does not jeopardize public safety.

z. **Scatter plot.** A graphical representation showing how two variables are related and that is used to test for cause and effect relationships.

aa. **Validation.** An evaluation to determine whether each safety measure derived from a system safety process is correct, complete, consistent, unambiguous, verifiable, and technically feasible. Validation is the process that ensures that the implemented safety measure is right.

bb. **Verification.** An evaluation to determine whether safety measures derived from a system safety process are effective and have been properly implemented. Verification provides measurable evidence that a safety measure reduces risk to acceptable levels.

4.0 BACKGROUND

The FAA Office of Commercial Space Transportation (AST) regulates commercial space transportation operations to the extent necessary to protect public health and safety and the safety of property. To fulfill its responsibilities, the FAA issues licenses for the launch or reentry of a launch vehicle or for the operation of a launch or reentry site. In addition, the Commercial Space Launch Amendments Act of 2004 provided FAA with the alternative of issuing experimental permits for the launch or reentry of developmental reusable suborbital rockets.

In reviewing the history of launch vehicle failures, analyses often show that clues existed before the mishap occurred. Such clues frequently take the form of anomalies observed during the life cycle of a project. Anomaly reporting and corrective action, therefore, play an important role in protecting public safety during launch or reentry. Analysis of anomalies can

- help warn of impending mishaps;
- provide risk analysis data, including potential consequences and likelihood of the hazard and the conditions that need to be controlled to mitigate public risk;
- help identify risk mitigation approaches;
- assist in the validation and verification of risk mitigation measures; and
- assist in establishing new structured processes and improving existing processes.

Corrective and preventive actions can prevent a mishap from occurring by eliminating the root cause of the problem or mitigating the effect of the anomaly.

As required by 14 CFR §437.73, an applicant must record each anomaly that affects a safety-critical system, subsystem, process, facility, or support equipment, identify all root causes of each anomaly, and implement all corrective actions for each anomaly. The FAA is not interested in all anomalies, but rather is only concerned about anomalies of systems, subsystems, processes, facilities, and support equipment that are essential for safe performance or operation. For example, an operator must report to the FAA any anomaly to those systems and processes associated with confining the operating area; restricting the location of key flight-safety events; and mitigating measures resulting from a hazard analysis. The operator must report to the FAA any anomaly for these systems or processes that occurs during verification (including ground test and inspection) or flight. Reporting of these anomalies will allow the FAA to analyze and evaluate operations under permits and verify that the operator is making informed safety decisions while operating under a permit.

5.0 ANOMALY REPORTING AND CORRECTIVE ACTION PROCESS

The FAA recommends that an operator implement an anomaly reporting process before vehicle testing begins. Figure 1 shows the steps in the anomaly reporting and corrective action process.

a. Anomaly Reporting

After an anomaly occurs, the suborbital rocket operator should identify that anomaly, verify the anomaly to assure that the problem has been properly identified, evaluate the anomaly for its potential impact, and analyze the anomaly

to determine root cause and corrective action. The operator should prepare a report documenting what happened and why. The report should include the root cause and corrective and preventive actions taken. Paragraph 5b discusses root cause analysis, and paragraph 5c discusses corrective and preventive actions.

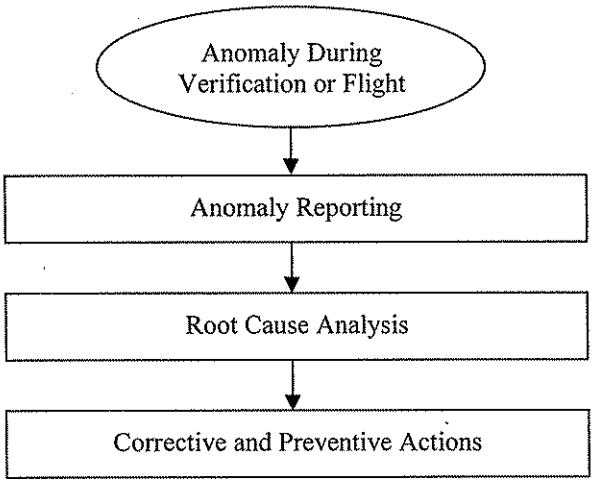


Figure 1. Anomaly reporting and corrective action process.

At a minimum, an anomaly report should include the following:

- A narrative description of the anomaly,
- The date and time of the anomaly,
- The affected component, system, subsystem, or software,
- The operation being performed when the anomaly occurred,
- The program phase during which the anomaly occurred,
- The number of times the anomaly occurred,
- Whether the anomaly could be verified,
- The potential hazards associated with the anomaly,
- The root cause of the anomaly,
- The method used to determine the root cause,
- The corrective and preventive actions taken, and
- The steps to validate and verify the effectiveness of the corrective and preventive actions.

The narrative description should include the conditions and equipment configuration at the time the problem occurred. Activities leading up to the problem, including an event sequence or timeline, should also be included. As part of the reporting process, operators should not underestimate the importance of collecting data on the anomaly. During the program phase, for example, did the anomaly occur in ground tests or in flight? Note the number of times the anomaly occurred. Was this the first time the anomaly occurred, or is it a recurring problem?

If feasible, the operator should verify the anomaly to confirm the problem before action is taken. This helps to ensure that the correct problem is being solved and assists in determining root cause and corrective action. An example of verifying a problem might be to rerun a test that resulted in a software anomaly. To determine the magnitude of the problem, the operator should identify the potential hazards associated with the anomaly. These hazards may have already been identified from an operator's hazard analysis or system safety process; therefore, the operator should reference applicable hazard analyses.

Obtaining information about an anomaly immediately after the occurrence of the problem is important; timeliness helps to avoid lost, distorted, or incomplete data. If, for example, too much time lapses before recording the information, the test article configuration could change or be relocated, personnel could forget critical details or remember information incorrectly, and documentation could be misplaced or destroyed.

To assist in determining root cause and corrective actions, the FAA recommends collecting and retaining data related to the anomaly. These data can include, but are not limited to, the following:

- Vehicle telemetry,
- Voice recordings,
- Operating and work logs,
- Correspondence,
- Inspection records,
- Maintenance records,
- Equipment history logs,
- Test results,
- Vendor manuals,
- Procedures and work orders,
- Drawings and specifications,
- Design information,
- Change documents,
- Sample analysis and results,
- Environmental factors, such as weather conditions, and
- Notes from interviews with test personnel.

Where appropriate, the suborbital rocket operator should retain physical evidence, such as a failed component, for later investigation. Photographic evidence can also assist in later analysis of anomalies.

Note that the operator must provide anomaly reports to the FAA only for those systems that could have public safety implications. For an experimental permit, the operator would only report anomalies for the systems related to containment in the operating area, location of key flight-safety events, and safety measures derived from a hazard analysis.

An operator may have an existing failure or nonconformance reporting system. The operator could use that system to meet the reporting requirements as long as it incorporates the reporting elements described here.

b. Root Cause Analysis

The anomaly report should describe the root causes of the problem and the approaches taken to determine those root causes. Before implementing any corrective actions, an operator should determine the root cause of an anomaly to ensure that the problem is understood. A root cause is the fundamental reason that an anomaly occurred. If the root cause, or underlying source of the problem, were eliminated, then the undesired outcome, that is the anomaly, would not have occurred. This underlying source differs from the proximate or direct cause, which is the immediate cause of the problem. For example, a circuit breaker tripping and leading to a loss of electricity would be the proximate cause of the loss of a home's lighting. However, a short circuit in the wiring would be a root cause of the problem.

Root cause analysis looks beyond the direct cause of the problem to find the underlying cause and prevent its reoccurrence. Many problems have multiple root causes leading to an undesirable outcome. In addition, multiple factors, known as contributing causes, can contribute to an anomaly. Causes include, but are not limited to, the following:

- Component, subsystem, or system failures, faults, and inherent process variability;

- Software and computing system errors;
- Environmental factors, such as weather conditions;
- Human error, including incorrect decisions, improperly followed procedures, and misunderstood procedures;
- Fatigue or lack of crew rest, which may cause or aggravate human error;
- Organizational factors, such as poor scheduling, inadequate or non-existent training, inadequate communications, or inadequate resources;
- Design inadequacies; and
- Inadequate or non-existent procedures and documentation.

Root cause analysis is necessary to identify the circumstances and factors leading to an anomaly. This analysis also eliminates potential causes not supported by the data and helps select causes that need further verification. This analysis allows the launch operator to learn from past problems, failures, and mishaps and assists in determining corrective actions. Without root cause analysis, the likelihood that only the proximate cause of the problem will be fixed increases, so the problem reoccurs. In the wiring example, a root cause may have been that wiring maintenance had not been performed as scheduled, thereby leading not only to a short circuit but possibly to other problems. Contributing causes could include maintenance budget cuts and personnel changes.

A variety of tools exist which can assist in root cause analysis. Some of these tools are listed below.

- Cause and effect diagrams present a graphical display of the relationship between a problem and possible root causes and facilitate brainstorming.
- Energy flow/barrier analysis identifies potential breakdowns in barriers that may have prevented or mitigated the problem.
- Event sequence diagrams allow an analysis of a sequence of events that led to a problem.
- Event tree analysis allows scrutiny of both favorable and unfavorable outcomes to events or challenges to the system.
- Failure Modes and Effects Analysis (FMEA) identifies possible failure modes of individual components, systems, subsystems, or processes.
- Fault Tree Analysis (FTA) maps anomalies with candidate root causes through multiple failure mechanisms.
- Flowchart analysis graphically represents the steps in a process or sequence of events to determine how a process works or how a problem occurred.

The technique used depends on the complexity of the problem, and some problems may not require detailed analysis. Regardless of the approach used, a root cause analysis should ultimately determine what happened and why it happened.

Details on Event Tree Analysis, FMEA, and FTA can be found in the FAA/AST *Guide to Reusable Launch and Reentry Vehicle Reliability Analysis*. NASA's *System Engineering "Toolbox" for Design-Oriented Engineers* provides examples of Cause and Effect Diagrams, Energy Flow/Barrier Analysis, Event Sequence Diagrams, and Flowchart Analysis.

c. Corrective and Preventive Actions

The anomaly report should describe the corrective and preventive actions and the steps taken to validate and verify those corrective and preventive actions. Once the root causes of an anomaly have been identified, corrective and preventive actions may be necessary to prevent reoccurrence of old problems and avoid occurrence of new problems. These actions may also mitigate the consequences of hazards identified in the hazard analysis process required by 14 CFR 437.29. For example, if a fire occurred in the propulsion system during testing, the operator may decide to install a firewall on the vehicle to isolate the propulsion system from the pilot. A corrective action is a reactive process taken to address a problem that has already occurred. A preventive action is a proactive process taken to stop a potential problem from occurring. Key elements of corrective and preventive action include the following:

- Validating that the proposed corrective or preventive actions are correct, complete, and feasible.
- Implementing the proposed corrective and preventive actions.
- Verifying that the corrective and preventive actions have been properly implemented and are effective. Typical verification approaches include analysis, test, demonstration, or inspection, as described in the FAA/AST *Guide to Reusable Launch Vehicle Safety Validation and Verification Planning*.

It is important that both validation and verification be performed. In case of the wiring example, one could verify that the wiring had been installed correctly. However, it would also be important to validate that the correct wiring had been specified in the first place.

Often several alternative corrective actions are available for each root cause. In the case of a fire in the propulsion system, in addition to installing a firewall, the operator's options include installing a fire detection system, constructing a fire extinguishing system, or implementing abort procedures. Selection of the corrective or preventive action will typically depend on a number of factors, including the effectiveness of the approach, type of operation, and impact on system performance or maintenance. Whether the selected action introduces new hazards or changes existing hazards should always be taken into account.

6.0 TREND ANALYSIS

The FAA recommends that the suborbital rocket operator use trend analyses, where appropriate, to identify patterns that may emerge from the anomaly reports. Trends in empirical data can be used to identify potentially hazardous conditions. This analysis evaluates variations of data to find patterns, with the ultimate objective of assessing current status and forecasting future events. Trend analysis can be reactive, to uncover the cause of a previous problem, or proactive, to detect adverse conditions. NASA's *System Engineering "Toolbox" for Design-Oriented Engineers* provides examples of these analyses. Examples of trend analysis include, but are not limited to, the following items:

- Control charts,
- Histograms,
- Pareto Analysis,
- Regression Analysis, and
- Scatter plots

7.0 SOFTWARE TOOLS

Software tools can assist in conducting anomaly reporting and corrective action. Descriptions and manufacturer information for such tools can be found through various professional organizations and societies. Examples include:

- Institute of Electrical and Electronics Engineers -- Reliability Society (http://www.ieee.org),
- Reliability Analysis Center (http://src.alionscience.com),
- American Society for Quality -- Reliability Division (http://www.asq.org), and
- Society of Automotive Engineers -- Reliability, Maintainability, Supportability, and Logistics Division (http://www.sae.org)

8.0 RELATIONSHIP OF ANOMALY REPORTING TO HAZARD ANALYSIS

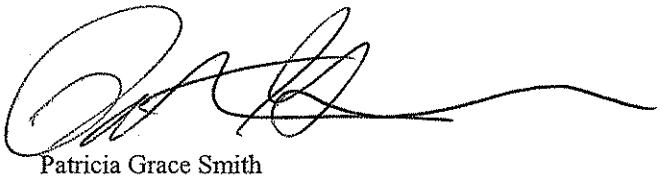
Hazard analyses are performed to identify system hazards and risks, to influence system design and operation, and to prevent mishaps. Hazard analyses are most effective when performed early in the vehicle design phase. At this point, making design and operational changes is easier and less costly. However, a hazard analysis is usually a forward-looking effort, and few hazard analyses can forecast and mitigate all potential anomalies. Anomaly reporting represents the "real world" experience of actual failures and problems observed during verification and operation. The anomaly reporting and corrective action system benefits the hazard analysis process by providing information that can be used to verify existing hazard and risk information and to provide information on new hazards not postulated in the original analysis. Therefore, the anomaly reporting, corrective action, and hazard analysis process should be closely linked to ensure that the analytical processes in the hazard analysis agree with real world experience reflected by anomalies. As part of this analysis, a suborbital rocket operator should identify the approaches and data needed to detect anomalies in order to improve those analyses (for example, temperature

measurements on a thrust chamber to detect excessively high temperatures). Additional information on hazard analyses and system safety can be found in AC 431.35-2A, Reusable Launch and Reentry Vehicle System Safety Process.

9.0 FOR FURTHER INFORMATION

For more information on the guidance contained in this AC contact the Office of Commercial Space Transportation, Federal Aviation Administration, 800 Independence Ave. S.W., Washington, DC 20591. Telephone: 202-267-7793.

Issued in Washington, DC, on April 20, 2007.



Patricia Grace Smith
Associated Administrator for Commercial Space Transportation