

U.S. Army Tank-automotive and Armaments Command
Armament Research, Development and Engineering Center
Quality Engineering Directorate

Policy No. 1-97 30 May 1997

(Revision 1D - 22 March, 2001)

AMSTA-AR-QA

SUBJECT: Safety Characteristics Policy

The following supplants AMCCOM Product Assurance and Test Directorate Policy No. 2, Subject: Critical Characteristics Policy, dated 03 February 1992, for all U.S. Army TACOM-ARDEC source selection and contract administration activities. In the event of a conflict between the text of this policy and references cited herein, the text of this policy takes precedence. Nothing in this policy, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

Definitions:

Safety characteristics are attributes of a system, item, assembly, subassembly, component or material that in the event of a nonconformance may result in hazardous or unsafe conditions for individuals using, maintaining or depending upon the product. Safety characteristics may be classified in specifications at two levels:

a. Critical Level I characteristics are those attributes that judgment and experience indicate must be met to avoid hazardous or unsafe conditions for individuals using, maintaining or depending upon the product. (Ref: MIL-STD-1916, DoD Preferred Methods for Acceptance of Product)

The following are examples of some characteristics that are considered Critical Level I characteristics:

1. A single point characteristic that failure to meet will result in a hazardous or unsafe condition.
2. A characteristic that failure to meet will remove or degrade a safety feature such as a fuze or safe and arm device.
3. A characteristic necessary to meet mandatory safety regulations, policies or standards.

b. Critical Level II characteristics are those attributes that judgment and experience indicate must be met to avoid hazardous or unsafe conditions for individuals using, maintaining or depending upon the product subject to the degree of divergence from requirements, and, or the presence of other nonconformances or

procedural errors. This term replaces the previous terminology for this characteristic which was "Special".

Background:

TACOM ARDEC considers the safety of all armament and munitions the paramount performance requirement strives to insure that all related systems provide high levels of safety to all DoD personnel throughout the system's life cycle. TACOM ARDEC classifies characteristic defects as critical when occurrence can result in a catastrophic event (death, permanent total disability or system loss) to the user.

When attempts to "design-out" such non-conformances has been exhausted, then the Quality Assurance Provisions are stated in a manner which keeps field occurrence "improbable". This number is intended to ensure that the event is indeed improbable, providing a high level of protection to the user. Based on this requirement, TACOM ARDEC associates a probability risk requirement of 'one in million' with critical characteristics.

This number is intended to ensure that the event is indeed improbable, providing a high level of protection to the user. Time has proven the less than 1 in a million number to be a reasonable and accepted Army and Military definition of "improbable". DARCOM-P 385-23 (page 6-5) made reference to this number and the current version of MIL-STD-882 also cites it. More importantly, the same line of reasoning has been used for decades in System Safety Risk Assessments, accepted and approved at the General Officer level. The definition has been the AMC promise to the soldier on what is safe.

Detail information on the 'one in a million' requirement can be found in the attached white paper or by request to AMSTA-AR-QAW-P.


ne in million final_.do

Policy:

1. Irrespective of any formal or informal partnering/teaming agreements, the safety of armament and munitions materiel and compliance to policies cited herein is the responsibility of TACOM-ARDEC. All TACOM-ARDEC personnel shall insure that safety characteristics are properly identified and documented for all associated development and production items/systems (whether the technical data be controlled by the government or supplier) and that suppliers use positive management, manufacturing and inspection controls to insure compliance to safety-related technical requirements.

2. Design and development - The preferred method of reducing the chance of manufacturing product with nonconforming safety characteristics shall be to eliminate them from the design. Design and development programs and associated contracts shall contain an objective that safety characteristics be designed out to the maximum practical extent and that producibility, inspectability and related life cycle safety risks be thoroughly considered for those safety characteristics which remain. Furthermore, program and associated contract objectives shall promote classification of safety characteristics based on analytical data and, whenever practical, supported by test data. Analytical techniques shall be performed through government-supplier partnerships as part of integrated product and process management.

Design and development integrated product teams (to include participants from both government and suppliers), with full consideration of all life cycle operational and tactical scenarios, shall perform system safety failure analyses (fault tree analysis, failure modes and effects criticality analysis, etc.) to identify all safety characteristics. Once identified, safety characteristics shall be classified as Critical, and annotated as Level I or Level II, as appropriate. These classifications shall appear on technical documents (drawings, specifications, purchase descriptions, etc.) and shall be used to insure proper development and deployment of associated manufacturing and inspection processes.

The following requirements shall apply when classifying characteristics:

a. Any characteristic, that in the event of a nonconformance will result in a hazardous or unsafe condition (often referred to as a single-point failure), shall be classified as "critical level I".

b. Any characteristic, that in the event of a nonconformance will remove or degrade a safety feature (such as those in a safe and arm device or fuzing system), shall be classified as "critical level I".

c. Any characteristic, that in the event of a nonconformance will result in violation of mandatory safety policies or standards, shall be classified as "critical level I".

d. Requirements cited in paragraphs 4 and 5 shall be mandatory for all critical level I characteristics.

e. With the exception of requiring suspension of production line, requirements cited in paragraphs 4 and 5 are mandatory for all critical level II characteristics.

f. Deviations from these requirements shall have written approval from the TACOM-ARDEC QED Associate Director.

3. Production Manufacturing - Manufacturing and inspection systems shall assure no more than one critical level I nonconformance per one million items produced and shall utilize preventative methods to preclude critical level II nonconformances. During fabrication of any materiel (either in design, development or production), supplier manufacturing and quality assurance systems shall assure compliance to material, component, subassembly, assembly and system safety requirements and the critical characteristic requirements of MIL-STD-1916, DoD Preferred Methods for Acceptance of Product.

As part of all proposals, suppliers shall be asked to describe policies, procedures and controls for all operations associated with safety characteristics, how they are documented and maintained under the supplier's integrated management system and how they serve to satisfy program safety requirements and this policy.

All production contracts shall contain requirements for handling critical defects. These requirements include those cited in MIL-STD-1916 and for critical level I characteristics include the stopping of production processes that produced the critical level I defect. The requirements cited in paragraphs 4 and 5 shall be mandatory for all critical level I characteristics and strongly recommended for critical level II characteristics.

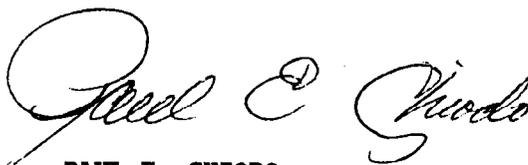
4. Critical characteristics - The following is required for all critical level I and critical level II characteristics:

- a. 100% inspection/test, obtaining variables data
- b. Use of non-operator dependent, repeatable, automatic decision making inspection equipment systems
- c. Government approval of all inspection and test procedures and equipment designs
- d. All processes affecting the characteristic under statistical process control (SPC)
- e. Government approval of SPC plans associated with critical level I and critical level II characteristics

5. Critical Level I and Critical Level II nonconformances - All requests regarding use of materiel with nonconforming critical characteristics shall be disapproved. Upon identification of a critical level I nonconformance (whether that characteristic is identified in government or supplier documents), a supplier shall suspend manufacturing, segregate suspect materiel and immediately notify the government. Upon identification of a critical level II nonconformance, the supplier shall be required to perform all the above actions except that suspension of manufacturing need not be required. Solicitations and contracts shall contain language alerting suppliers that TACOM-ARDEC reserves the right to refuse acceptance of any suspect materiel until the root cause of safety-related nonconformances has been identified, corrective action has been fully implemented and sufficient evidence is provided to exclude that materiel from the conforming population. Acceptance of previously suspect materiel shall require the written approval of the QED Associate Director.

6. Alternatives to policies and practices cited herein shall require written approval from the QED Associate Director.

Proponent: QED Engineering Policy Group, AMSTA-AR-QAW-P.

A handwritten signature in black ink, reading "Paul E. Chiodo". The signature is written in a cursive, flowing style with a large initial "P".

PAUL E. CHIODO
Director, Quality Engineering

DISTRIBUTION:

All Quality Engineering Directorate Employees

WHITE PAPER

The purpose of this paper is to explain the relationship between the Critical Defect Policy and the less than 1 in a million requirement.

As described in MIL-STD-1916 (see ref. 4), a critical defect (characteristic) is a defect that can lead to hazardous or unsafe conditions to the user and/or can cause the end item not to perform its intended mission. ARDEC classifies defects as critical when occurrence can result in a catastrophic event (death, permanent total disability or system loss) to the user. When attempts to "design-out" such non-conformances has been exhausted, then the Quality Assurance Provisions get stated in a manner which keeps field occurrence "improbable".

The connection between critical defects and the requirement for less than 1 in a million comes from risk management. Historically, in most cases, the highest risk that ARDEC has recommended for acceptance involving a possible catastrophic event is less than 1 in a million. This number is intended to ensure that the event is indeed improbable, providing a high level of protection to the user.

Time has proven the less than 1 in a million number to be a reasonable and accepted Army and Military definition of "improbable". DARCOM-P 385-23 (see ref.2, page 6-5) made reference to this number and the current version of MIL-STD-882 (see ref.1) also cites it. More importantly, the same line of reasoning has been used for decades in System Safety Risk Assessments, accepted and approved at the General Officer level. The definition has been the AMC promise to the soldier on what is safe.

MIL-STD 882 requires risk assessments be accomplished by characterizing hazards by hazard severity and hazard probability risks. The latest version of MIL-STD- 882 establishes suggested mishap probability levels. The mishap probability is the probability that the mishap will occur during the planned life expectancy of the system. The suggested mishap probability for Improbable, Level E, is described as "So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life". Tables from MIL-STD-882 for both the probability levels and the severity categories are shown below. DARCOM-P 385-23 also cites the same mishap probability levels and severity categories as the current revision of MIL-STD-882.

TABLE A-II Suggested mishap probability levels.

Description	Level	Specific Individual Item	Fleet or Inventory**
Frequent	A	Likely to occur often in the life of an item, with a probability of occurrence greater than 10^{-1} in that life.	Continuously experienced.
Probable	B	Will occur several times in the life of an item, with a probability of occurrence less than 10^{-1} but greater than 10^{-2} in that life.	Will occur frequently.
Occasional	C	Likely to occur some time in the life of an item, with a probability of occurrence less than 10^{-2} but greater than 10^{-3} in that life.	Will occur several times.
Remote	D	Unlikely but possible to occur in the life of an item, with a probability of occurrence less than 10^{-3} but greater than 10^{-6} in	Unlikely, but can reasonably be expected to occur.

		that life.	
Improbable	E	So unlikely, it can be assumed occurrence may not be experienced, with a probability of occurrence less than 10^{-6} in that life.	Unlikely to occur, but possible.

TABLE A-I. Suggested mishap severity categories.

Description	Category	Environmental, Safety, and Health Result Criteria
Catastrophic	I	Could result in death, permanent total disability, loss exceeding \$1M, or irreversible severe environmental damage that violates law or regulation.
Critical	II	Could result in permanent partial disability, injuries or occupational illness that may result in hospitalization of at least three personnel, loss exceeding \$200K but less than \$1M, or reversible environmental damage causing a violation of law or regulation.
Marginal	III	Could result in injury or occupational illness resulting in one or more lost work days(s), loss exceeding \$10K but less than \$200K, or mitigatable environmental damage without violation of law or regulation where restoration activities can be accomplished.
Negligible	IV	Could result in injury or illness not resulting in a lost work day, loss exceeding \$2K but less than \$10K, or minimal environmental damage not violating law or regulation.

The item or system ORD may specify the acceptable catastrophic rate to be less than one per million or more generally will just state that there shall be no hazards which will cause injury to personnel or damage to material.

During preparation of System Safety Risk Assessments (SSRA) the levels currently listed in MIL-STD-882 have been used as the guidance for assigning hazard probability levels. The communication of abnormally high risks to the soldier takes place via the SSRA. The AMC business process is to get user agreement to such instances. When an SSRA is not prepared and formally coordinated, then the communication, by default, is that the product poses no safety risk because occurrence is improbable.

Below are examples where SSRA's were generated and formally coordinated. These demonstrate the probability levels at which AMC considers it important to communicate the issue to the user, and to get explicit acceptance.

Table of Recent SSRA's

Item	Date of SSRA	Severity Level	Probability Level	Probability	Signature Level
M900	April 92	Catastrophic	Remote	1/303,075	Major General
MK66	March 95	Catastrophic	Occasional	1/56,988	General

Probability levels are controlled through a combination of design and inspection. The ARDEC specification practices take this into account. MIL-A-47078, MIL-STD-1316 and the QED Safety Characteristic Policy require critical defects be controlled to less than 10^{-6} . MIL-A-47078 specifically addresses fuzes but describes procedures for controlling the defect rate. MIL-STD-1316 addresses fuze design criteria, requiring fuze safety to be better than one per million. MIL-STD-1916 also requires a verification sample for all screening inspections of critical defects.

It is quite conceivable that failure in the manufacturing/inspection system results in an increased level of probability which the design cannot safely accommodate. The tire industry case is a recent, commercial example. In such cases, the risk management can no longer be handled purely in term of abstract probabilities, but based on actual indications of defect rates. If the actual indicators alter the originally stated/coordinated user's risk (SSRA or default), then it is suggested that user involvement in accepting the revised situation would be advisable.

Reference Documents

1. MIL-STD-882d; Standard Practice For System Safety; 10 Feb 2000
2. DARCOM-P 385-23; System Safety; 1 June 1977
3. MIL-A-48078A; Ammunition, Standard Quality Assurance Provisions, General Specification for; 16 Dec 1988
4. MIL-STD-1916; DOD Preferred Methods for Acceptance of Product
5. Report No: TR 90-4 Procedures for Risk Management in the Acquisition Process; System Safety Coordinating Panel Technical Subpanel Report; August 1990
6. QED Safety Characteristics Policy#1-97
7. MIL-STD-1316 Fuze Design, Safety Criteria for